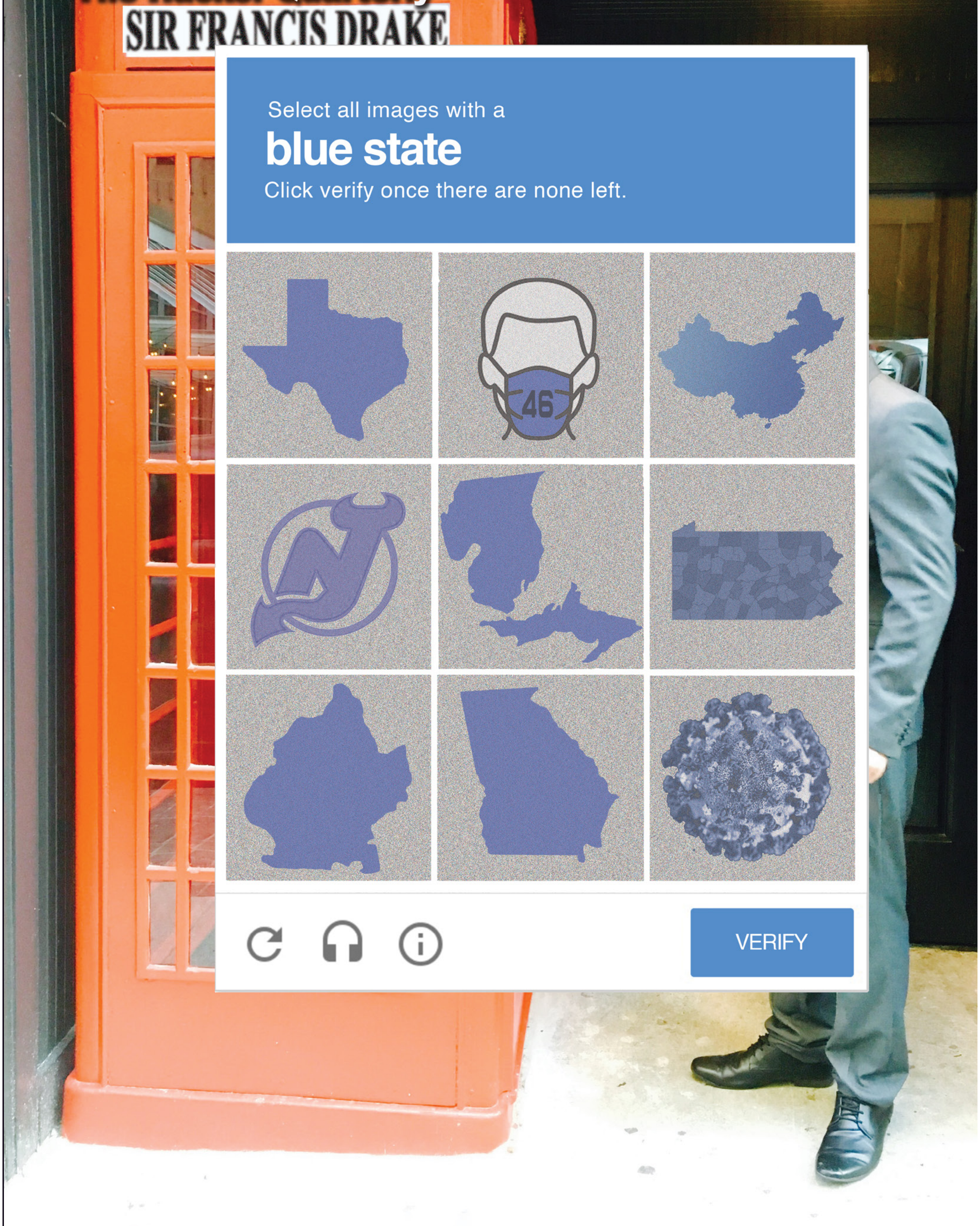
Volume Thirty-Seven, Number Three
DIGITAL EDITION

# 2600

## The Hacker Quarterly

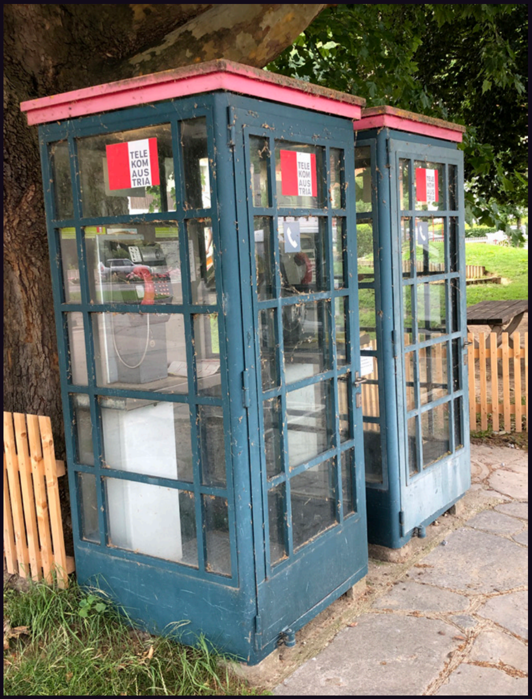


Select all images with a

**blue state**

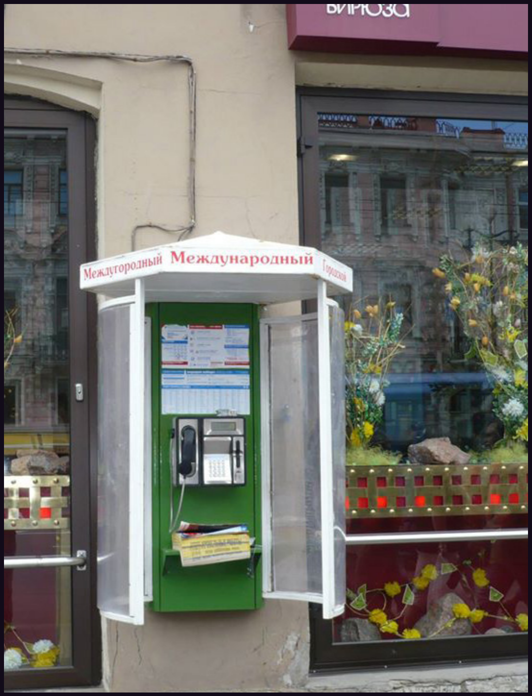
Click verify once there are none left.

# Distant Payphones



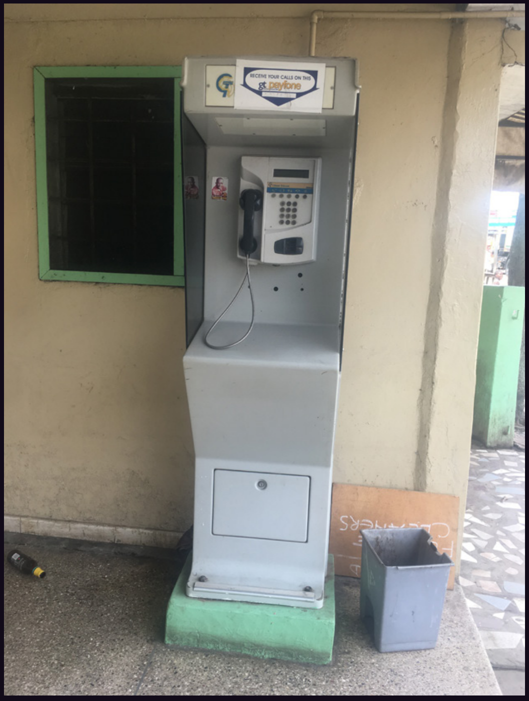
**Austria.** Seen in Spitz, this harkens back to the days when huge phone booths existed everywhere. While the booth may belong to Telekom Austria, the distinctive pink handsets indicate the phones **are** Magenta Telekom, a relative of T-Mobile.

***Photo by David Clark***



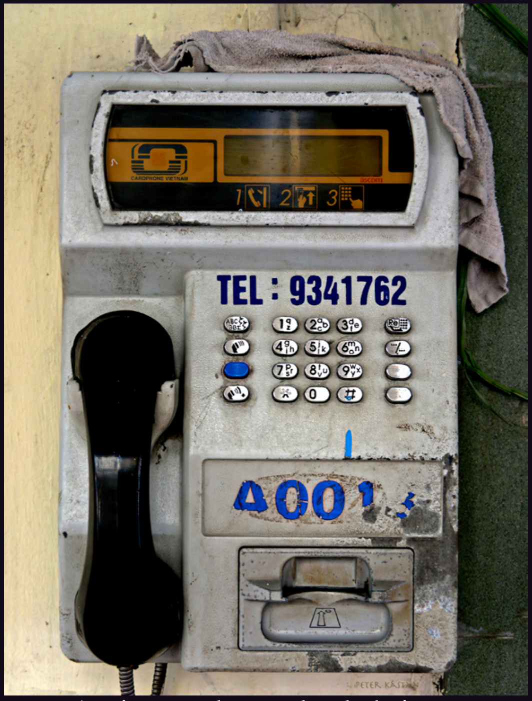
**Russia.** This distinguished looking model was found in St. Petersburg. It's proof that presentation is everything. The green background, colorful charts, phone book, and kiosk (including the font that says "international") make this a destination in itself.

***Photo by Pirho***



**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***

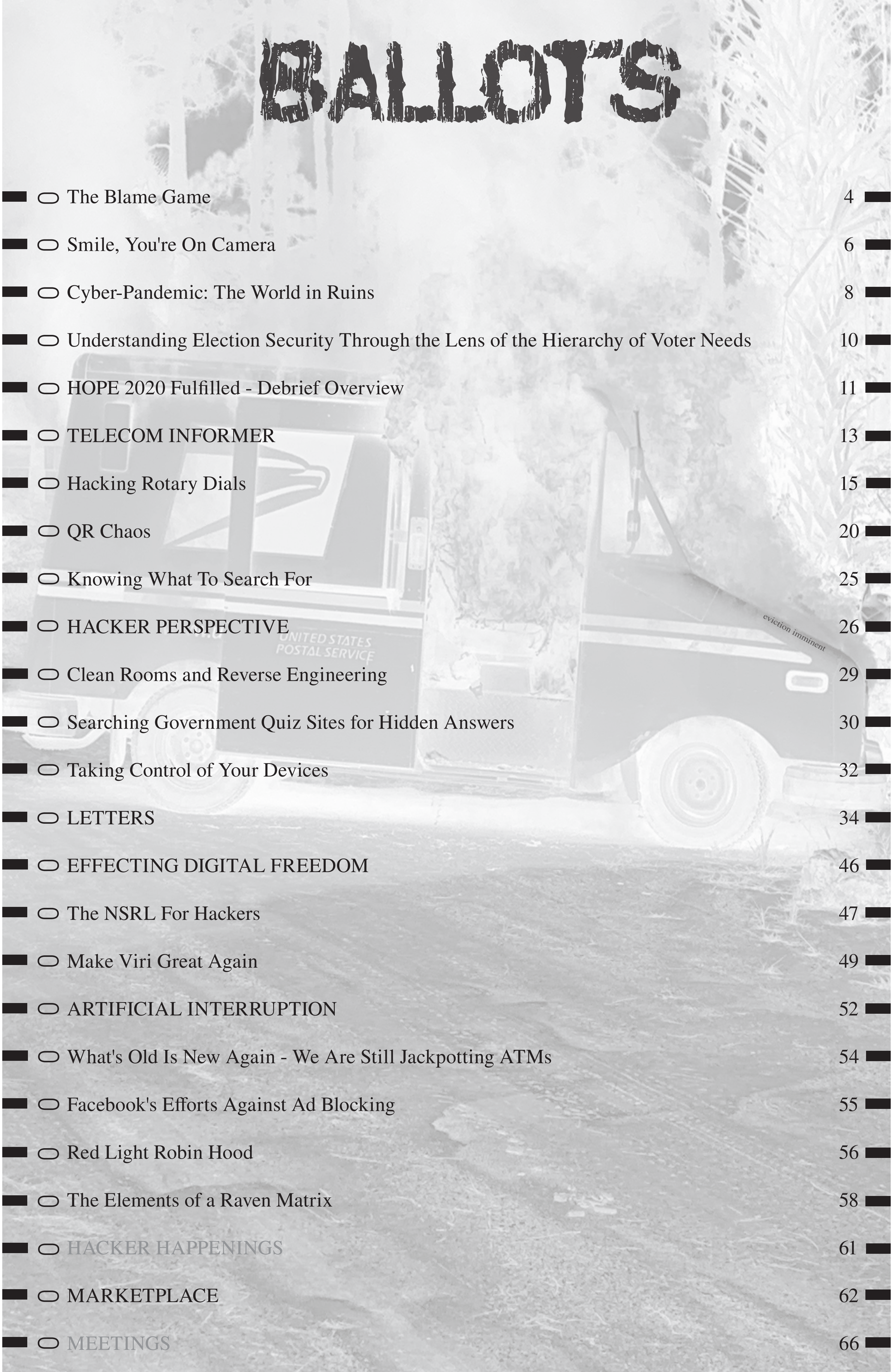


**Vietnam.** Again, people are clearly being encouraged to use this phone to receive calls, a concept that has become somewhat alien in America. Located in Hanoi, this card reading model looks fairly rugged.

***Photo by Peter Kastan***

Got foreign payphone photos for us? Email them to payphones@2600.com.
Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

# BALLOTS



# 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.

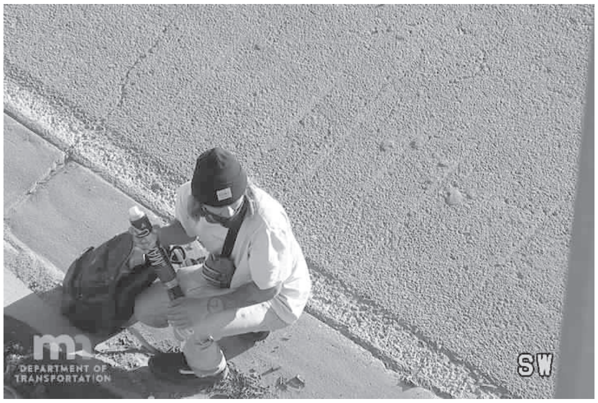
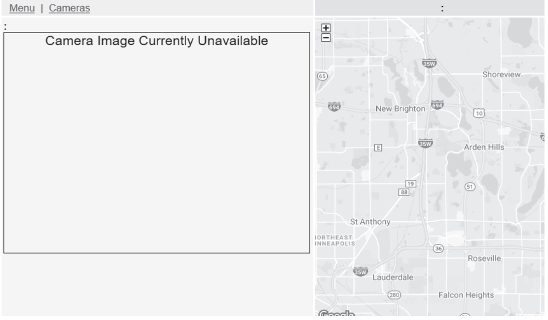


*Figure 1: The high resolution cameras were used to focus in on individuals, as seen here*

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.



Check out the new 511 site and leave us feedback!

Camera Image Currently Unavailable

*Figure 2: MN DOT webpage with missing camera feed*

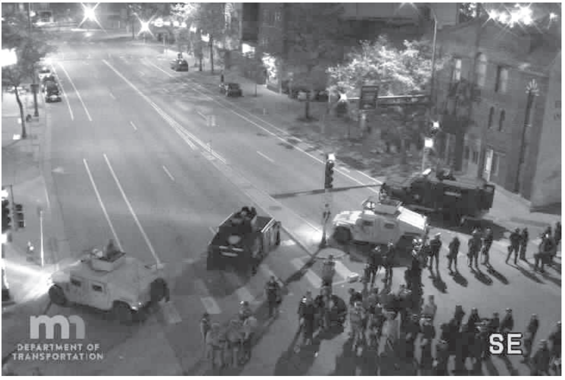


*Figure 3: Camera feed showing police activity*

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.

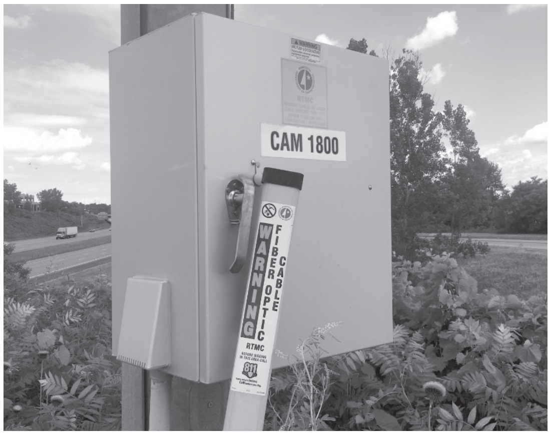


*Figure 4: The yellow ID labels on the cameras as seen from the road*

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.

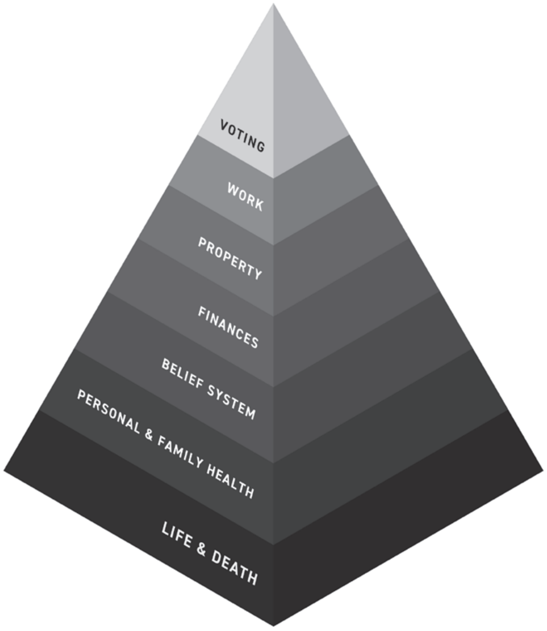
One thing is now clear. We have a lot of work and preparedness to do if we are to better deflect future attacks. We have a lot of things to seriously ponder, as a country, as individuals, and as a race of beings in general. We will have some big and critical decisions to make if we are to secure our 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*.

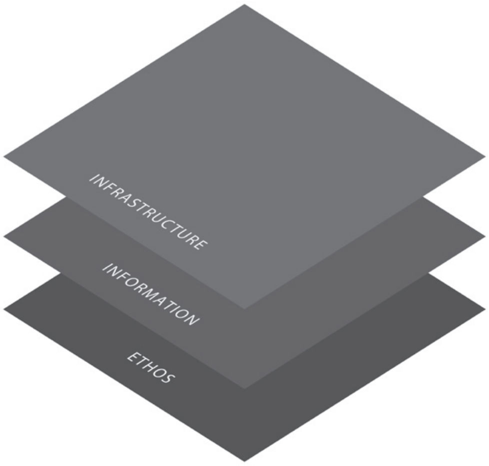
Each level of the Hierarchy of Voter Needs compounds on the other. For voters, events of life and death come before voting. When citizens are facing a natural disaster that threatens their lives, voting will not be their priority - getting to safety will be. Similarly, personal and family health, work 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.

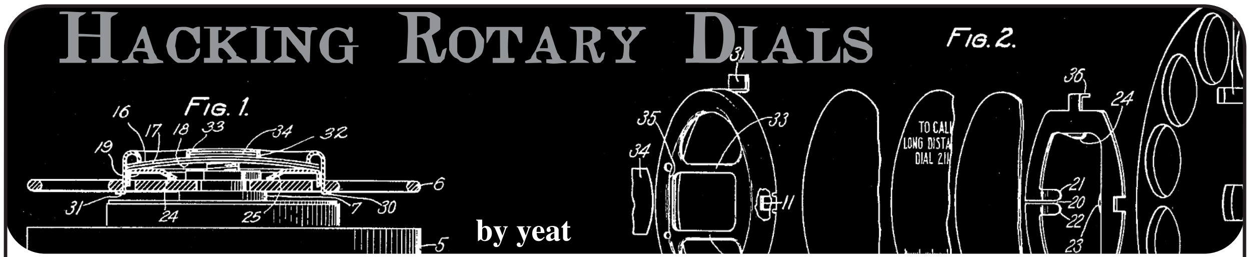
And with that, it's time to board up our windows. Our threat intelligence feed is warning of election-related violence, and corporate security has issued a directive. Granted, our windows are tiny, reinforced, and 30 feet up in the air, but I guess that's why we have a scissor lift. Try to stay safe 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`

# 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).

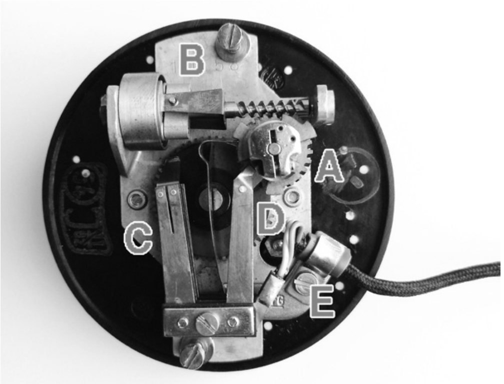
Even today, such old telephones can be used if connected, for instance, to an analog port of a DSL router. Most probably, receiving of calls would work without further effort. Only for outgoing calls, a pulse to DTMF converter may be required as most modern routers don't recognize dial pulses anymore.

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:

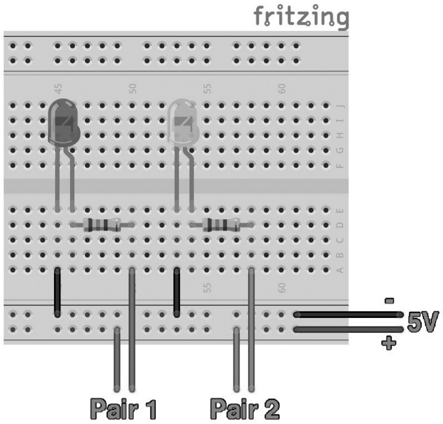
The dial on the front is attached to the large gear in the center on the rear side. This gear spins a rotor [A] which is adjusted to constant speed by a tiny centrifugal brake [B]. The center gear also toggles two switches at [C] - initially one is open and one is closed. There is an additional switch at [D] which is normally closed and opened in pulses by the spinning rotor [A].

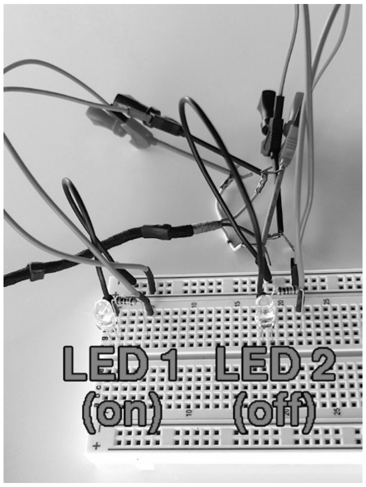
Last but not least, there is a cable attached at [E], forming the connection to the outside world. Its four wires were the focus of my further investigations.

### 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.

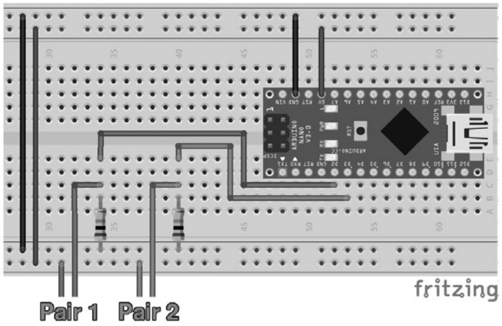
The pulses of LED 1 were fired rather quickly, but when slowing down the backward spin with my finger, I could observe that the number of pulses magically coincided with the number chosen on the dial! For instance, if number 5 was dialed, then LED 1 would shortly turn off five times, six times if number 6 was dialed, and so on.

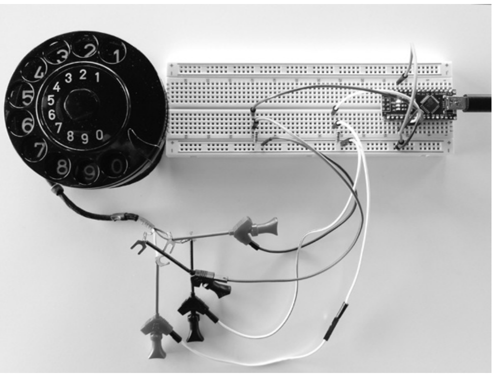
In other words, I had found one signal at Pair 2, indicating if the dial had been turned out of its resting position and another signal at Pair 1, revealing the number that had been dialed. That's definitely enough for a leap into the 21st century.

### 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?

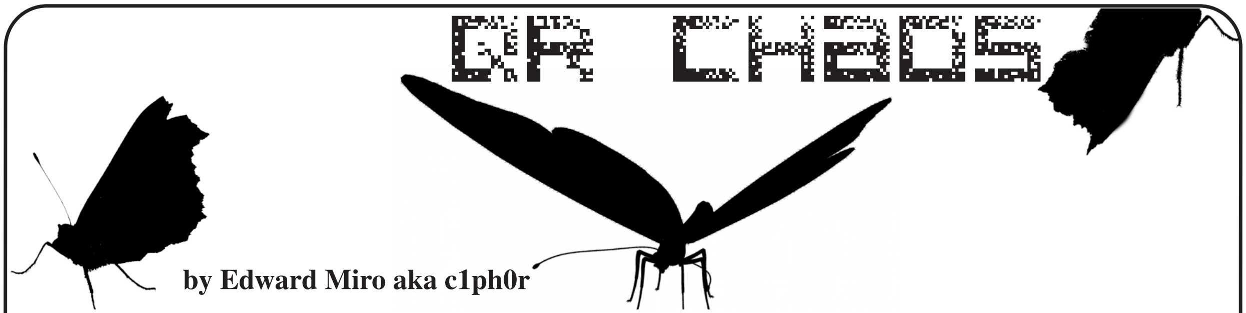
That's entirely up to you and your imagination! Apart from pushbuttons, potentiometers, keypads, and a myriad of other sensors, you are now capable of integrating a very cool vintage input device into your next project! I'm sure you will come up with countless marvelous ideas. And even if you don't, 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”);
?>
```

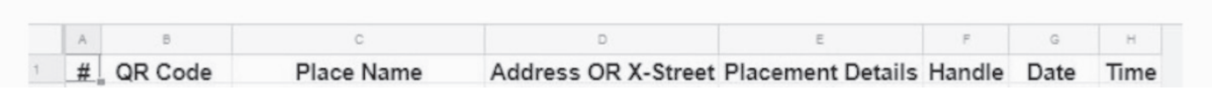
Nothing too crazy here. Just collecting the timestamp, device’s IP address, device’s browser, and the GET variable which is loc=(one of our random strings).

I pasted them into `https://➥qrexplore.com/generate/` and then printed them in sheets with the filename added:

R2BKINJHGn.png
tH93L16ZEU.png
Q2RMoetnUB.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.

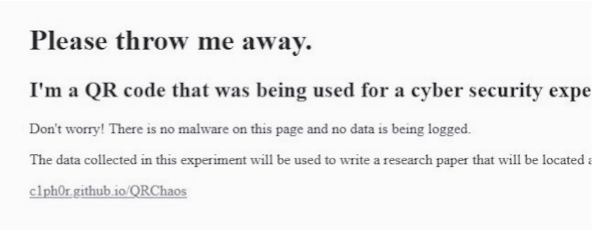
Of the remaining 70, only ten were logged on my sheet, and I found later on that I didn’t make the logging necessity and procedure as clear as I should have to many of my volunteers. If you repeat or expand this experiment with your students or cybersecurity club, I recommend walking all the participants 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=brpoOaYI0W)

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=brpoOaYI0W)

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

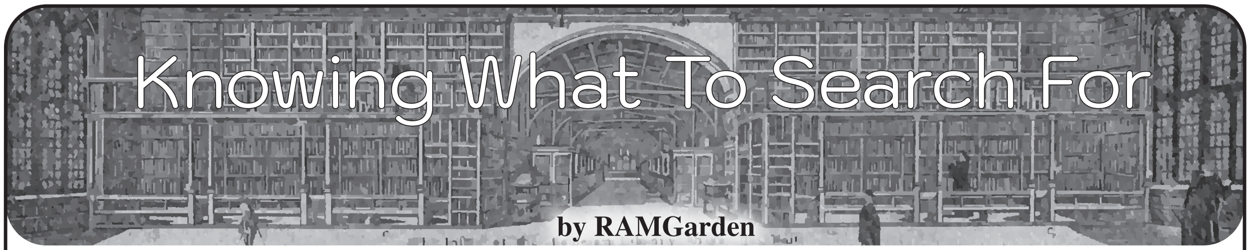
The QR code attack vector will require utilizing some of the same techniques used in detecting attacks such as phishing:

- 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!

# 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.

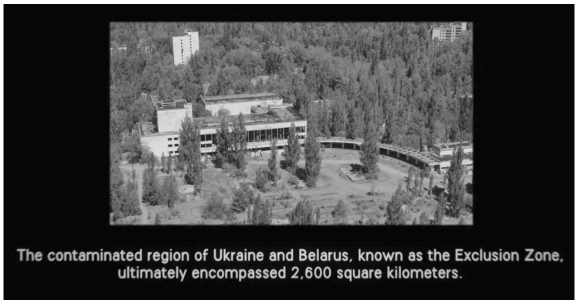
Not sure what you want to do with this info - I know you cannot possibly check every inmate's backstory that wants to run a personal in *2600*, but I imagine some of your readership might be a bit upset if they knew this.

**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.

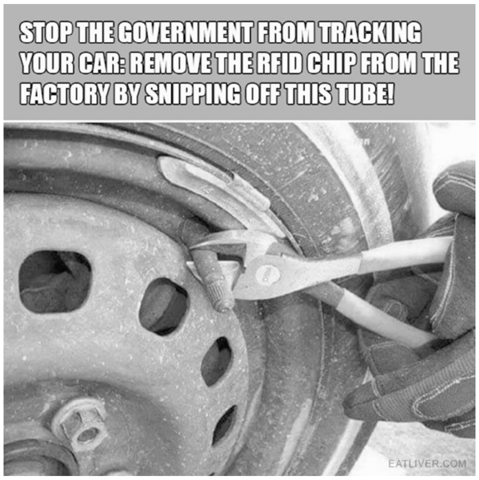
**A. C.**

*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!
EATLIVER.COM

**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.*

# 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 National Software Reference Library 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

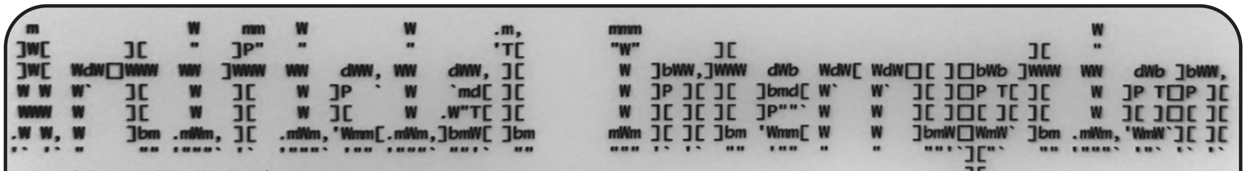
[4] web.archive.org/
➥web/20170219031937/http://zeus.
➥fei.tuke.sk/bps3r/html/ch08s03.
➥html

[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.0l.wtf/

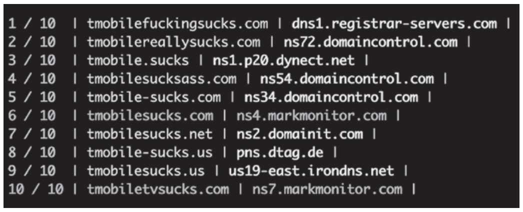


by Alexander Urbelis

## 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.

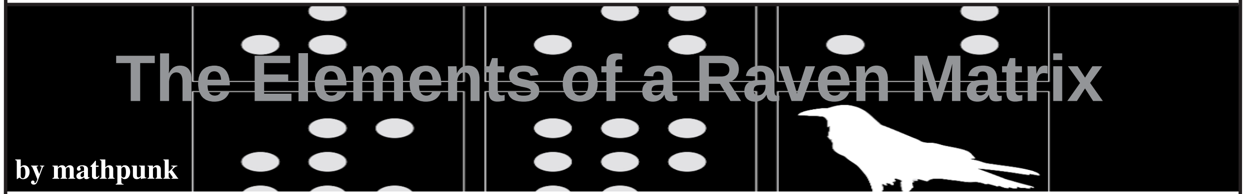
This led to yet another discovery. After reducing the traffic light times, the government minimized quota fines and maximized ticket revenue. What incentive did they have to care at all about Conduent's behavior or the unsafe conditions? They were making buckets of money. "Thirty million dollars greases 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

by 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
SECUREDROP

# HACKER HAPPENINGS

will return soon...

*Until things return to normal, here's a virtual event worth attending that will replace this year's Chaos Communication Congress in Germany.*

**rC3 – remote Chaos Experience**

This year, CCC hosts the
Remote Chaos Experience (rC3)
instead of an on-site event in Leipzig.
This endeavor requires creativity,
joy of experimentation and active support.

A face-to-face event with 17,000 people
will be neither responsible nor legally feasible this year.
But after this tedious and painful 2020,
we really deserve a nice finale!

This is why the rC3 – Remote Chaos Experience will be held.

As much as virtually possible, we want to convey the joy, content,
togetherness and wonderful madness that make up a
Chaos Communication Congress.

Hackers are used to remote work and online meetings.
This makes our annual face-to-face meetings all the
more important. Of course, it will be difficult to re-enact
online all the things that make Congress what it is for us.

But then someone said it would be impossible.
Our ambition was aroused.

Just like every year, we want to see the concentrated energy
and creativity of hackers with dedication.

rC3 will be a variety of distributed small local events in hackspaces with a joint program of streamed talks, online workshops, art, culture and various forms of networked togetherness.

Save the date:
**December 27-30, 2020**
Online and in your local hackspace
with your preferred infection community

More details at *events.ccc.de*

# Marketplace

## For Sale

**HACKER WAREHOUSE** is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

**HEATHKIT BOOK:** Interested in vintage electronics? *Classic Heathkit Electronic Test Equipment* by Jeff Tranter covers Heathkit's test equipment line, with in depth coverage of different models including oscilloscopes, meters, tube testers, etc., as well as a history of Heathkit and resources for collecting and restoration. 140 pages in 11 chapters plus appendices. Retails for $19.95 from lulu.com and amazon.com.

***GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY*** by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

**OPEN SOURCE HARDWARE:** crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see bunnie huang's NeTV2 project).

**SECUREMAC.COM** is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

**PORTABLE PENETRATOR.** Find WPA WPA2 WPS WiFi Keys Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports use for consulting. Coupon code 20% off: 2600. https://shop.secpoint.com

## Help Wanted

**JOIN THE HTTPS://CODEFOR.CASH** community and earn money with freelance programming jobs. All hats welcome!

**VIRTUAL ASSISTANT/PROGRAMMER NEEDED.** I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 97051

## Announcements

**THE MODERN TECHNOLOGY PODCAST NETWORK** contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials.
Feed your head at https:// modern. technology

**TOG IS DUBLIN'S HACKERSPACE.** We run regular events in coding, lock picking, electronics, craft, cad, wikipedia editing, electronic music, brewing, science fiction book club, and monthly socials. We recently celebrated our 11th birthday! TOG is run and funded by volunteer members and we are always looking for new hackers. website: www.tog.ie email: info@tog.ie address: 22 Blackpitts, Dublin 8, D08 P3K4, Ireland.

**DON'T JUST CELEBRATE TECHNOLOGY,** question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

**COVERTACTIONS.COM** is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

***OFF THE HOOK*** is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

## Services

**DO YOU HAVE A LEAK OR A TIP** that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser, attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

**GET YOUR HAM RADIO LICENSE!** KB6NU's "No Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides/. Paperback versions are available from Amazon. E-mail cwgeek@kb6nu.com for more information.

**INTELLIGENT HACKERS UNIX SHELL:** Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

**DIGITAL FORENSICS EXPERTS FOR CRIMINAL DEFENSE!** Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. We can recover

data nationwide from many sources, including computers, external media, tablets, and smartphones. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@
➥senseient.com.

**LOCKPICKING101.COM** is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

**CALL INTO THE PHONE LOSERS OF AMERICA'S** telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to old episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123, 435-625-4232, or 845-470-0336.

**ANTIQUE COMPUTERS.** From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era.
http://www.vintagecomputer.net

**DOUBLEHOP.ME VPN** is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off.
https://www.doublehop.me

**HAVE YOU SEEN THE *2600* STORE?** Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of *2600* and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

**UNIX SHELL ACCOUNTS WITH MORE VHOSTS.** If you like funny, relevant vhosts for IRC, get a JEAH shell. You can also use vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup! BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.

**DISCOUNT WEB HOSTING AND FREE WEB TRAINING.** Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

**BLACKSTONE LAW GROUP LLP.** Unique among law firms, we have married the practice of law with the practice of information security. We are also the only law firm to offer bespoke threat intelligence. Designed to identify the hallmarks of impending cyberattacks (APT activity, phishing, credentials harvesting, etc.), with our own DNS monitoring and threat intel platform, OMNI, we have assisted hundreds of companies worldwide with the early detection, investigation, and termination of sophisticated cybersecurity threats before a breach or reputation damage occurs. Engineered for and by information security professionals, our DNS intel platform goes far beyond ordinary brand protection, safeguarding our clients full circle: from detection to takedown. Our lawyers have been the Chief Information Security Officer and Chief Compliance Officer of some of the world's most recognizable companies, have federal government experience in both intelligence and defense, and been partners in several Am Law 100 firms. At Blackstone Law Group, there is no lag time to "get the lawyers up to speed" on the technical issues surrounding an incident or investigation. Our combination of legal acumen and information security expertise results in great efficiencies that, by design, benefit our clients' bottom line. And perhaps most notably, one of our partners is Alex Urbelis who many readers will recognize from *Off The Hook*. Give us a ring or send Alex a note. We would be glad to speak to you confidentially about our threat intel and legal services. Blackstone Law Group LLP, alex@blackstone-law.com, 1201 Broadway, 9th Floor, New York, NY 10001, P: (212) 779 3070 x 101, https://blackstone-law.com.

**Personals**

**GREETINGS FELLOW TECHNOPHILES!** I am a full-time activist currently incarcerated in the state of Texas for a crime I did not commit. I am looking for a tech-minded person in the free world to help me maintain my sanity while I wait on Habeas proceedings. Activism, Libertarianism, or Anarchism are plusses but not required. If you are interested, write: David Danforth - 2250914, Wallace Unit, 1675 FM 3525, Colorado City, TX 79512.

**WHAT'S UP, HC,** I'm a single, aspiring hacker, programmer, coder, IT, computer engineer noob who is looking for real comradery and information on suggested reading/learning material. I've been inside for 10 years and therefore I'm way out the loop. I've been getting *2600* for about two years so I'm not all the way out the loop but I have 1000 questions. I'm looking for people to network, game, and research with. I have tech ideas I would like to create and collab on along with a woman who is intelligent and tech savvy as me. Brothers are encouraged to write me as well for I would like to only communicate and hang out with my Hacker Community. I'm from Houston, TX. I love to travel and read. All info is requested. If you have tips and suggested paths to learn code through books or your experience is well appreciated. I parole in two years. Even if you're just interested in picking up post-release, send me contact info. For what it's worth, I am also very good looking and fit with pictures. I'm not vain and only want those whose intelligence makes them feel as different as I do with an open mind. Reach me at Edward Lacy, TDC #1772002, 1697 FM 980, Huntsville, TX 77343 or Jpay.com or download the Jpay app and text/type a message to me.

**PENPALS:** Seeking people to write with interests in technology. I'm 30 and from Cleveland, Ohio, but currently incarcerated in rural Pennsylvania. We are on a quarantine lockdown and I'm bored to death. Before prison I worked network operations for an Internet service provider. Also worked at the Geek Squad for a short period. Being out of tech for so long, I'm feeling antiquated. There's no Internet here and hardly any resources to keep up. I have many other interests too, including sailing, general aviation, health/fitness, snowboarding, travel/foreign cultures, etc. I can share with you the many crazy stories of what really happens in prison. Use white paper and white envelope. NO address labels/stickers. It will be rejected and returned. Looking forward to your letters! Token, thanks for the shoutout in 37:1. Shoot me a letter sometime. Dan Nieberding, 61030-060, Federal Correctional Institution, PO Box 1000, Cresson, PA 16630, United States of America.

**ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*** Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.
**Deadline for next issue: 1/21/21.**

# HOPE 2020 FLASH DRIVES!

The HOPE 2020 flash drives are out! All 9 days are meticulously catalogued in both audio and video formats, completely free to copy and share on two large USB drives. In addition to every single talk that was presented (more than 125), you'll also get a video collection of musical performances that were presented each day at midnight, audio of the intermission music for each day, and the renowned "HOPE Bumps" that were shared with attendees between talks.

HOPE 2020 was an unexpected magical period in the midst of some very trying times - and we have the hacker community to thank for making it possible as well as ensuring our survival through what could have been a devastating summer. We're thrilled to be able to preserve and share these moments with presentations from all around the world - a true Hackers On Planet Earth event.

Just $79 (plus shipping) 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.

(We also have a full collection of every HOPE conference from 1994 to 2020 - eight drives for $299 plus shipping!)

*"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

# STAFF

**Editor-In-Chief**
Emmanuel Goldstein

**Associate Editor**
Bob Hardy

**Layout and Design**
typ0

**Cover**
Dabu Ch'wald

**Office Manager**
Tampruf

**Infrastructure**
flyko

**Network Operations**
phiber, olssy

**Broadcast Coordinator**
Juintz

**IRC Admins**
beave, koz, r0d3nt

**Inspirational Music:** Debby McClatchy, The Original Caste, Mano Negra, George Carlin, Black Oak Arkansas, E. Power Biggs
**Shout Outs:** Alzo Slade, Daniel Dale, Georgia, Bobby Goodlatte, Krishna Andavolu, Four Seasons Total Landscaping
**RIP:** Frank Drake

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

***2600** (ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

**POSTMASTER:**
Send address changes to: *2600,*
P.O. Box 752 Middle Island,
NY 11953-0752.

**SUBSCRIPTION CORRESPONDENCE:**
*2600* Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

**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.
2000-2019 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**

***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. There is really nowhere on the planet where these gatherings would be safe at the moment.**

**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.**

**We're asking all meetings to reconnect with us by emailing meetings@2600.com. If you're part of an existing meeting, let us know that you still intend to meet at the last published location or, if you've found something better, the new details. If you don't have a meeting where you are but would like to start one, come up with a location and tell us the details. When we relaunch, your meeting will be part of our new list.**

**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.**

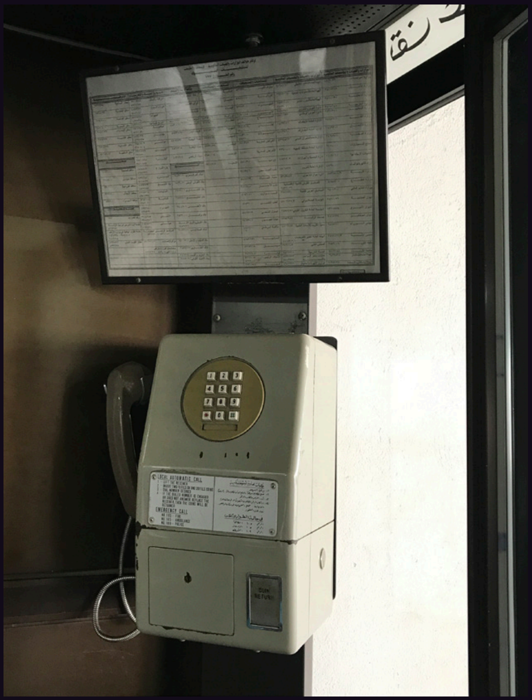
**2) We act in a responsible manner. We don't do illegal things and we don't cause problems for the place we're meeting in. *Most 2600* meetings are welcomed by the establishments we choose.**

**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.**

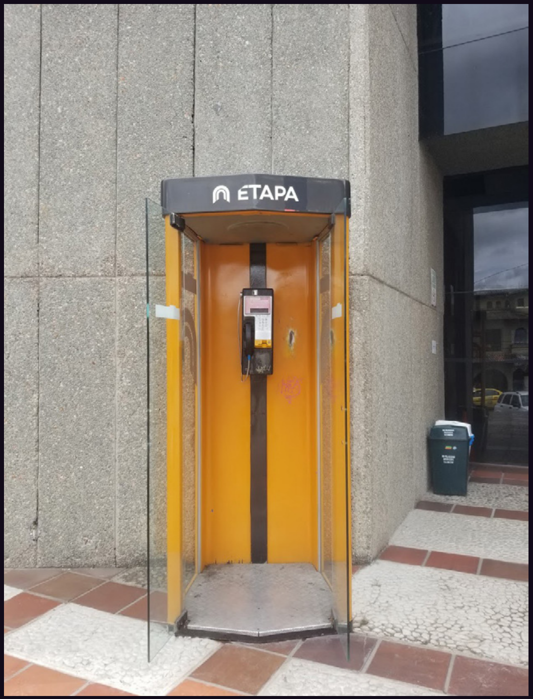
**Follow @2600Meetings on Twitter to find out when meetings will resume. Stay safe!**

# Unusual Payphones



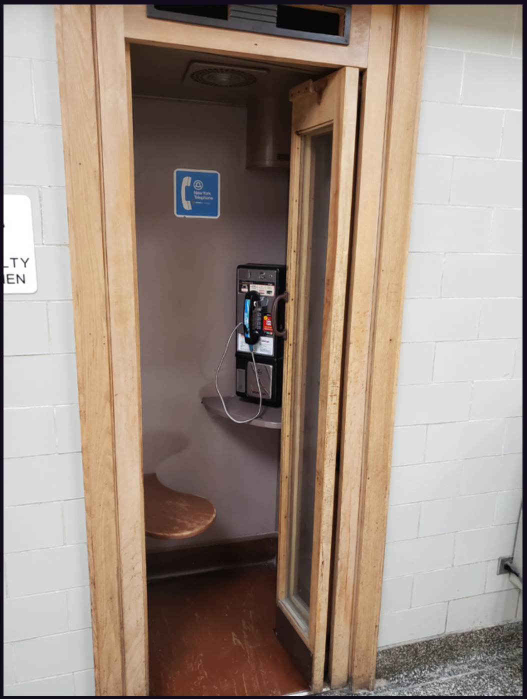
**Kuwait.** Definitely not the kind of payphone we're used to seeing. This model looks incredibly serious with its rather drab coloring and exhaustive list of numbers you might want to call.

***Photo by XBS***



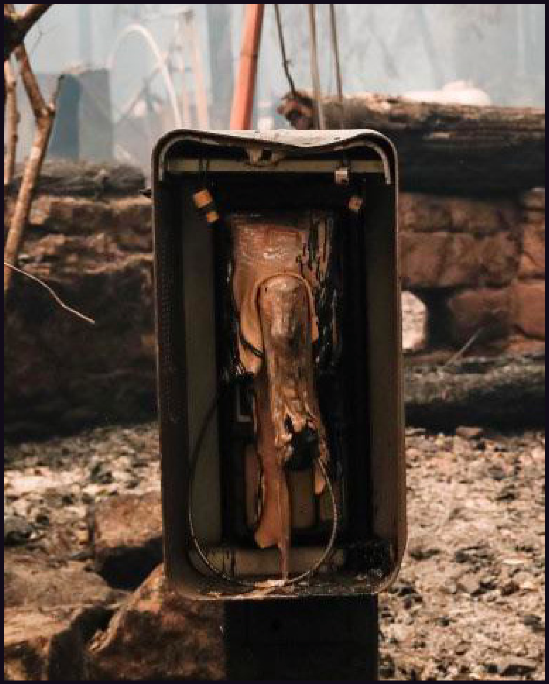
**Ecuador.** Perhaps it's an optical illusion, but this looks like an incredibly thin phone. Seen in Cuenca and run by ETAPA, a local company owned and operated by the city.

***Photo by Benji Encalada***



**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***

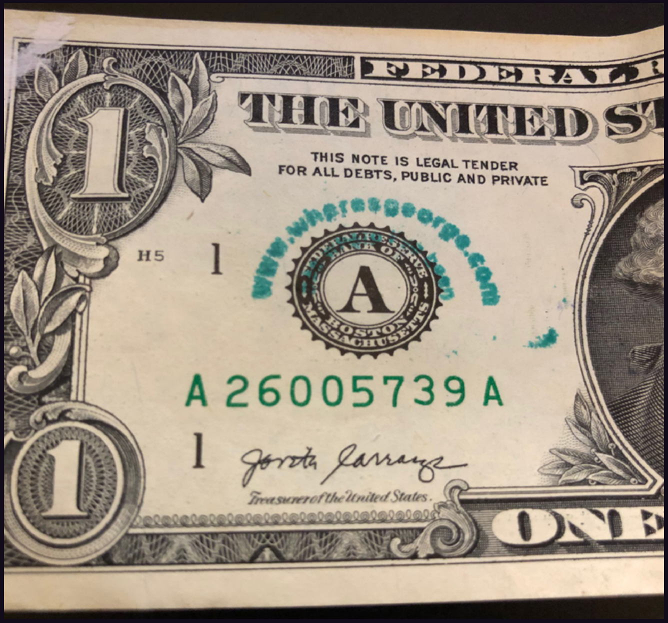


**United States.** This payphone met with an unfortunate end, having the bad luck to be located in the Big Basin Redwoods State Park campground, in Boulder Creek, California. It's remarkable how much of it remained standing after one of the most destructive wildfires in history.

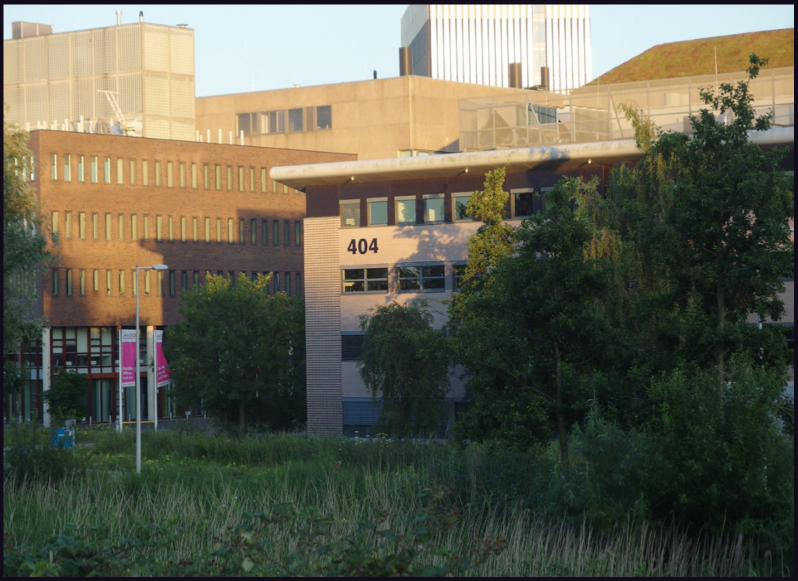
***Photo by Josh Goldberg***

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

# The Back Cover Photos


FEDERAL
THE UNITED ST
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
www.wheresgeorge.com
H5
A
BOSTON MASSACHUSETTS
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.



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.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
*2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues)
and a *2600* t-shirt of your choice.