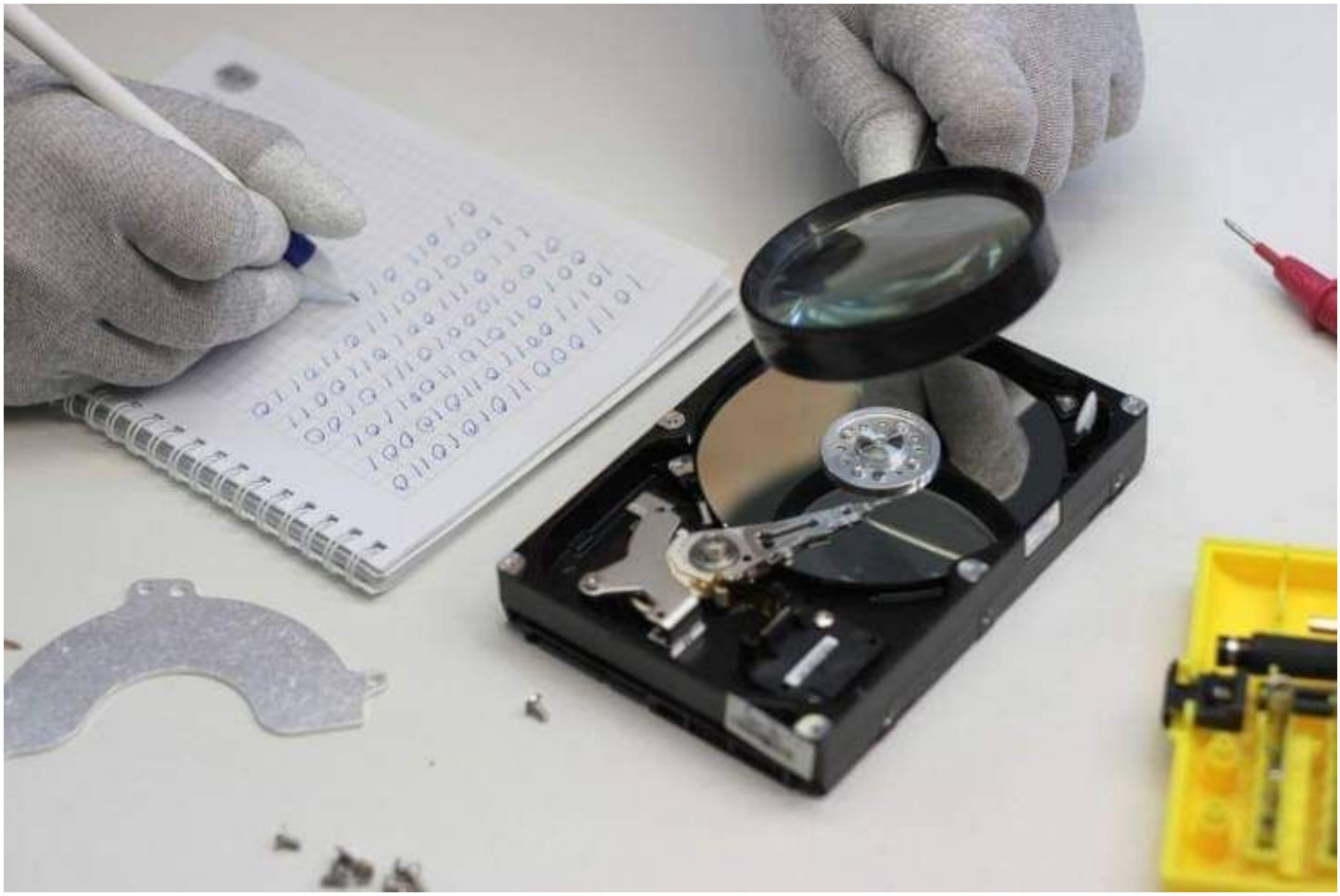
Security Now! #773 - 06-30-20

Ripple20 Too

This week on Security Now!

This week we look at news in the shortening of certificate lifetime change, at Apple's decision to deliberately ignore support for a bunch of new WebAPIs, at Apple's announcement of DoH support, at some troubling Mozilla/Comcast news, at some welcome legislation to head-off the use of facial recognition and at another less welcome attempt to outlaw strong encryption. We also look at the grow legislation against mandatory "chipping" and remind our listeners about the utility of VirusTotal. Then, after catching up with a bit of miscellany and listener feedback, we revisit last week's very worrisome revelation of the many flaws in a very widely used embedded TCP/IP stack. There's much news there... and none of it's good.

11010010 00110110 00001101 11010011



Browser News

Apple forces the industry down to one-year web browser certificate lifespans

Last February we talked about Apple's surprise announcement during the CA Browser Forum that in the future it would be rejecting **any** web server certificate having a "Not Valid Before" date after August 31, 2020, having a certificate lifetime greater than 398 days. In other words, starting just two months from now from September 1st of this year on, all CA certificates issued for use by web browsers must be issued with a one year plus 33 days lifetime. This is the death of the more convenient two or three year web server certs. Now everyone needs to refresh their certs annually.

When this news hit earlier this year I discussed the many implications of this issue in depth and detail. So I won't repeat that all here again. The reason this is back in the news is that now Mozilla and Google -- and thus all of the Chromium-based offshoots -- have also announced their exactly-aligned policies.

Google's Ryan Sleevi posted:

> Enforce 398-day validity for certificates issued on-or-after 2020-09-01
>
> Enforce publicly trusted TLS server certificates have a
> lifetime of 398 days or less, if they are issued on or after
> 2020-09-01.
>
> Certificates that violate this will be rejected with
> ERR_CERT_VALIDITY_TOO_LONG and will be treated as misissued.

https://chromium.googlesource.com/chromium/src/+/ae4d6809912f8171b23f6aa43c6a4e8e627de784

And Mozill's Kathleen Wilson posted:
"Limit re-use of domain name verification to 395 days #206"

For anyone who's interested in a long and interesting discussion thread among the industry insiders who make these sometimes Earth shattering decisions, I've included the Google Groups discussion thread in the show notes:
https://groups.google.com/forum/#!msg/mozilla.dev.security.policy/mz1buYdIy-I/oo9zHBADAQAJ

Safari to eschew 16 new web API's for the sake of user privacy

Apple has decided against implementing 16 new web technologies for Safari because they individually and collectively they would pose a credible threat to user privacy by opening new opportunities for user fingerprinting.

The 16 APIs that Chrome will have and Safari will not are:

- Web Bluetooth - Allows websites to connect to nearby Bluetooth LE devices.
- Web MIDI API - Allows websites to enumerate, manipulate and access MIDI devices.
- Magnetometer API - Allows websites to access data about the local magnetic field around a user, as detected by the device's primary magnetometer sensor.
- Web NFC API - Allows websites to communicate with NFC tags through a device's NFC reader.
- Device Memory API - Allows websites to receive the approximate amount of device memory in gigabytes.
- Network Information API - Provides information about the connection a device is using to communicate with the network and provides a means for scripts to be notified if the connection type changes.
- Battery Status API - Allows websites to receive information about the battery status of the hosting device.
- Web Bluetooth Scanning - Allows websites to scan for nearby Bluetooth LE devices.
- Ambient Light Sensor - Lets websites get the current light level or illuminance of the ambient light around the hosting device via the device's native sensors.
- HDCP Policy Check extension for EME - Allows websites to check for HDCP policies, used in media streaming/playback.
- Proximity Sensor - Allows websites to retrieve data about the distance between a device and an object, as measured by a proximity sensor.
- WebHID - Allows websites to retrieve information about locally connected Human Interface Device (HID) devices.
- Serial API - Allows websites to write and read data from serial interfaces, used by devices such as microcontrollers, 3D printers, and others.
- Web USB - Lets websites communicate with devices via USB (Universal Serial Bus).
- Geolocation Sensor (background geolocation) - A more modern version of the older Geolocation API that lets websites access geolocation data.
- User Idle Detection - Lets website know when a user is idle.

As I mentioned above, most of these APIs will only be found implemented in Chromium-based browsers -- although that's quite a lot of browsers -- and Firefox has a few.

Whereas 3rd-party cookies were once the tracking mechanism of choice, as we know, they are readily blocked by savvy users. And much as I had naïve hopes for the "do not track" header, DNT was DOA. In the place of cookies, the use of surreptitious fingerprinting has been steadily growing to the point that fingerprinting has now become the standard means of tracking users online for the advertising technology market. This growth has been driven by the browser vendors steady addition of anti-tracking features to their browsers.

But not only are all current fingerprinting techniques blocked, but each additional web API which provides even weakly unique information about the current user, can be aggregated to create a more unique composite.

Apple said that "WebKit's first line of defense against fingerprinting is to not implement web features which increase fingerprintability and offer no safe way to protect the user."

And as for traditional Web APIs which have been implemented in Safari for years, Apple says it has been working to reduce their fingerprintability vector. To that end, Apple said it had:

- Removed support for custom fonts. This means only presenting built-in fonts which are the same for all users with the same system.
- Removed minor software update information from the user agent string. The string only changes with the marketing version of the platform and the browser.
- Removed the Do Not Track flag, which ironically was used as a fingerprinting vector, adding uniqueness to the users who had enabled it.
- Removed support for any plug-ins on macOS. Other desktop ports may differ. (Plug-ins were never a thing on iOS.)
- Require a user permission for websites to access the Device Orientation/Motion APIs on mobile devices, because the physical nature of motion sensors may allow for device fingerprinting.
- Prevent fingerprinting of attached cameras and microphones through the Web Real-Time Communication API (WebRTC).

Apple also got on the DoH & DoT bandwagon

Last Wednesday, during Apple's developer conference, Tommy Pauly, Internet Technologies Engineer at Apple explained that the fall releases of iOS 14 and macOS 11 would support both the DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) protocols.

That's the good news, kinda. From what Tommy said, it doesn't as though it's going to be a consumer-friendly feature. At least not at the start. He said that developers could create apps to apply DoH/DoT settings for the entire operating system (via network extension apps or MDM profiles), or to individual apps, or to an app's selected network requests.

What most security-aware users would like to have is their entire iOS device or Mac using a DoH/DoT provider of their choice. So I suppose someone could create an app to enable that. But why not a setting in the OS's network settings? That would seem to be the far better solution.

Tommy said: "There are two ways in which encrypted DNS can be enabled. The first way is to use a single [encrypted] DNS server as the default resolver for all apps on the system. If you provide a public [encrypted] DNS server, you can now write a network extension app that configures the system to use your server. Or, if you use Mobile Device Management to configure enterprise settings on devices, you can push down a profile to configure encrypted DNS settings for your networks.

"The second way to enable encrypted DNS is to opt-in directly from an app. If you want your app to use encrypted DNS, even if the rest of the system isn't yet, you can select a specific server to use for some or all of your app's connections." But, as I understand it, an app would first need to have that option added.

In any event, Apple is not going to be left as the odd man out. They are joining the rest of the industry in the move to encrypt DNS. Given how slowly most of these things change, this move to encrypted DNS has moved at warp speed!

Mozilla + Comcast + DoH: Strange Bedfellows

I'm unsure whether to call Mozilla and Comcast and DoH strange bedfellows or strained bedfellows. The disquieting news is that Comcast's Xfinity broadband Internet service will be joining Firefox's Trusted Recursive Resolver (TRR) program. And, worse, it will be enabled and Comcast will be the default DoH resolver for all Firefox users on Comcast's network.

So let's enumerate the things that are fundamentally wrong with this picture:

First, recall that it was in 2014 that Comcast was caught injecting unsolicited advertisements into its customer's browsing. And the U.S.'s broadband privacy rules were killed by congress in 2017 when congress passed a bill allowing ISPs to collect and sell Web surfing data. Prior to President Trump's signing that bill into law, as he immediately did with some flourish, the FCC's previous privacy rules would have required home Internet and mobile broadband providers to first obtain consumers' opt-in consent before selling or sharing Web browsing history, app usage history, and other private information with advertisers and other companies. But, lawmakers used their authority under the Congressional Review Act (CRA) to pass a joint resolution ensuring that the rules "shall have no force or effect" and that the FCC cannot issue similar regulations in the future.

Then recall how last year, as we talked about at the time, Comcast went ballistic and patently lied in congressional testimony about the move by the browser vendors to secure DNS. Remember that set of slides we reviewed at the time which was just full of nonsense? And in a joint letter to congress, of which comcast was a signatory:

> We would like to bring to your attention an issue that is of concern to all our organizations. Google is beginning to implement encrypted Domain Name System lookups into its Chrome browser and Android operating system through a new protocol for wireline and wireless service, known as DNS over HTTPS (DoH). If not coordinated with others in the internet ecosystem, this could interfere on a mass scale with critical internet functions, as well as raise data competition issues.
>
> Google is unilaterally moving forward with centralizing encrypted domain name requests within Chrome and Android, rather than having DNS queries dispersed amongst hundreds of providers. When a consumer or enterprise uses Google's Android phones or Chrome web browser, Android or Chrome would make Google the encrypted DNS lookup provider by default and most consumers would have limited practical knowledge or ability to detect or reject that choice. Because the majority of worldwide internet traffic (both wired and wireless) runs through the Chrome browser or the Android operating system, Google could become the overwhelmingly predominant DNS lookup provider.
>
> Moreover, the centralized control of encrypted DNS threatens to harm consumers by interfering with a wide range of services provided by ISPs (both enterprise and public-facing) and others. Over the last several decades, DNS has been used to build other critical interne features and functionality including: (a) the provision of parental controls and IoT management for end users; (b) connecting end users to the nearest content delivery networks, thus ensuring the delivery of content in the fastest, cheapest, and most reliable manner; and (c) assisting rights holders' and law enforcement's efforts in enforcing judicial

orders in combatting online piracy, as well as law enforcement's efforts in enforcing judicial orders in combatting the exploitation of minors. Google's centralization of DNS would bypass these critical features, undermining important consumer services and protections, and likely resulting in confusion because consumers will not understand why these features are no longer working.

And, finally... LOCALLY resolved DNS has NEVER been a privacy issue as far as the wider Internet is concerned. When a consumer uses their own ISP's local DNS resolver their queries never emerge onto the Internet. As we know, the local resolver is also a cache which is able to satisfy most queries without asking anyone else. And when the local cache doesn't contain the answer being sought, IT, and not the ISP's customer, goes out onto the Internet to issue one or more queries to obtain and then cache the answer on behalf of the customer. In other words, the ENTIRE POINT of using DoH is specifically and only to blind the user's own ISP to the content of their DNS queries. We're telling our ISP to keep their nose out of our business.

Based on past evidence and behavior it's clear that our ISPs are every bit as desperate to know our business as is every other entity out on the Internet that wants to track our behavior and our every action. So, with the speedy deployment of browser-based DoH, it was inevitable that ISPs would be bringing up their own DoH servers to recapture those DNS lookups that they were rapidly being blinded to.

What's most distressing is that we're going to witness the tyranny of the default swinging Firefox's users away from Cloudflare and NextDNS and back to their ISPs... whom all of our experience suggests simply cannot be trusted to keep their hands off of that data.

https://blog.mozilla.org/blog/2020/06/25/comcasts-xfinity-internet-service-joins-firefoxs-trusted-recursive-resolver-program/

Mozilla's announcement said:

Mozilla, the maker of Firefox, and Comcast have announced Comcast as the first Internet Service Provider (ISP) to provide Firefox users with private and secure encrypted Domain Name System (DNS) services through Mozilla's Trusted Recursive Resolver (TRR) Program. Comcast has taken major steps to protect customer privacy as it works to evolve DNS resolution.

Eric Rescorla, Firefox CTO, said: "Comcast has moved quickly to adopt DNS encryption technology and we're excited to have them join the TRR program. Bringing ISPs into the TRR program helps us protect user privacy online without disrupting existing user experiences. We hope this sets a precedent for further cooperation between browsers and ISPs."

For its part, Comcast has reaffirmed its commitment to the privacy of their users. Their explicit statement about privacy highlights three points:

https://corporate.comcast.com/stories/privacy-with-comcasts-xfinity-internet-service

1. As your Internet Service Provider, we do not track the websites you visit or apps you use through your broadband connection. Because we don't track that information, we don't use it to build a profile about you and we have never sold that information to anyone.

2. We do not sell, and have never sold, information that identifies who you are to anyone. We also don't sell, and have never sold, your location data when you use our Xfinity Mobile service.

3. We delete the DNS queries we have as an Internet Service Provider every 24 hours.

That being true, one wonders why these ISP's were so forceful in, and spent so much money lobbying to, overturn the FCC's previous privacy protections?

In any event, our Comcast-connected Firefox-using listeners should be aware of this. It is still possible to explicitly override the forthcoming Comcast default and to again aim your browser's DNS-over-HTTPS to Cloudflare or NextDNS. At some point you'll need to do that explicitly.

Security News

"The Facial Recognition and Biometric Technology Moratorium Act"
...was proposed last Thursday by two senators (Ed Markey and Jeff Merkley), and two representatives (Pramila Jayapal and Ayanna Pressley). Although a growing number of US cities have been banning government use of the technology -- with Boston last week becoming the tenth U.S. city to do so -- the bill would put in place the first nationwide ban on facial recognition technology.

The sense is that the use of facial recognition technology has sprung up unbidden because it had suddenly become feasible and practical, but that the nation's lawmakers had never been given the opportunity to weigh in on whatever limitations and guidelines, if any, should also be imposed.

So the newly proposed bill would "prohibit biometric surveillance by the Federal Government without explicit statutory authorization and to withhold certain Federal public safety grants from State and local governments that engage in biometric surveillance."

That means federal agencies would be barred from using biometric surveillance systems (which in addition to facial recognition can also include voice recognition). Additionally, it would prohibit the use of federal dollars to be spent on facial recognition technology, and "condition federal grant funding to state and local entities, including law enforcement, on those entities enacting their own moratoria on the use of facial recognition and biometric technology."

The ban has no definitive time limit in place, and would continue until Congress passed a law to lift it -- which is, I think, exactly the way it should be done..

Privacy concerns around facial recognition – and specifically the inadvertent apparent racial bias repeatedly demonstrated by the technology – came into focus earlier this week when the

American Civil Liberties Union filed a complaint alleging that an African American man was arrested in Detroit after a facial recognition system falsely matched his photo with security footage of a shoplifter. According to the ACLU, this is the first known example of misidentification through faulty facial recognition technology leading to a wrongful arrest. The senior legislative counsel with the ACLU said: "No one should have to go through what the Williams family has gone through. It's past time Congress halted the use of face recognition and stopped federal money from being used to invest in invasive and discriminatory surveillance."

A forthcoming research paper to be published by Springer Publishing, Berlin, Germany bears the somewhat ominous title: "A Deep Neural Network Model to Predict Criminality Using Image Processing" describes AI algorithms that can predict crime based only on a person's face.

In response, at last count, 2,435 professors, researchers, practitioners, and students spanning the fields of anthropology, sociology, computer science, law, science and technology studies, information science, mathematics, and more including experts and academics from organizations including MIT, Microsoft, Harvard and Google recently signed an open letter denouncing this paper, calling it out for promoting racial bias.

https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16

Their letter, published on Medium last Tuesday was titled: "Abolish the #TechToPrisonPipeline" with the subheading: "Crime prediction technology reproduces injustices and causes real harm" with the byline: "Coalition for Critical Technology"

And as we have previously noted, Microsoft, Amazon and IBM, which have all developed their own facial recognition platforms, have all recently banned the sale of the technology to police departments and pushed for federal laws to regulate the technology.

Senator Markley, in his statement about the proposed legislation, said: "Facial recognition technology doesn't just pose a grave threat to our privacy, it physically endangers Black Americans and other minority populations in our country. At this moment, the only responsible thing to do is to prohibit government and law enforcement from using these surveillance mechanisms."

So that's the happy proposed legislation. Here's the not-so-happy legislative proposal...

"The Lawful Access to Encrypted Data Act"
This new legislation was introduced by the US Senate's Judiciary Committee Chairman Lindsey Graham, Senator Tom Cotton and Senator Marsha Blackburn. They argued that ending the use of "warrant-proof" encrypted technology would "bolster national security interests" and "better protect communities across the country." They added that such encryption cloaks illicit behavior during criminal investigations into terrorists and other bad actors.

As we know, there's been no other single topic that has so captured my interest and attention. Along with the more recent question of managing the posting and presentation of counter-factual information on the web, the question of whether encryption should remain warrant-proof is the issue of the day... And it's going to be fascinating to watch this play out.

We already have last year's EARNIT Act, also introduced by Lindsey Graham, a can of slime whose language begins: "A Bill to establish a national commission on online child exploitation prevention, and for other purposes." As we know, it threatens to revoke a non-complying company's legal protections under Section 230 which shields the company from criminal and civil liability for user-generated content. I much prefer a straightforward heads-up fight over what we're really talking about.

Tom Cotton, one of the Bill's three co-sponsors said: "Tech companies' increasing reliance on encryption has turned their platforms into a new, lawless playground of criminal activity. Criminals from child predators to terrorists are taking full advantage. This bill will ensure law enforcement can access encrypted material with a warrant based on probable cause and help put an end to the Wild West of crime on the Internet."

Yeah. Good luck with that. We all know that lawful users will obtain weaker privacy protection while actual criminals, who will be much more motivated to hide their illicit activity, will simply switch to non-US platforms that continue to provide warrant-proof encryption.

And in a somewhat bizarre carrot and stick, this latest attempt at legislation also directs our illustrious Attorney General, Bill Barr to create a "prize competition" to award participants who create a "lawful access solution in an encrypted environment." Right. Like Apple or Signal or Facebook are going to sign up for that prize. Though I suppose that this might be an effort to spur some innovation to get some much smaller players to propose technological solutions to the problem.

So far, none of this legislation ever seems to go anywhere. That's presumably because those who query members about their feelings and probable votes never even get close to imagining that the bills have a snowflake's chance of actually passing.

However, some welcome legislation did recently pass in Michigan's House...

Michigan State's legislative House passed the "Microchip Protection Act"
Even though forced RFID chip implants for workers is not an issue yet, the state of Michigan decided to join seven other states in getting out in front of that one by formally and preemptively outlawing compulsory microchip implants for employees.

The legislation notes that although there are only a few known U.S.-based companies embedding microchips in its employees, several job providers could be following soon – including businesses in Michigan. Assuming that this legislation passes, which appears likely, Michigan would become the eighth state to explicitly outlaw compulsory chipping. The existing seven states are: California, Maryland, New Hampshire, North Dakota, Oklahoma, Wisconsin and Utah. All of these already prohibit the required implantation of a microchip in any person for any reason, not just employees.

Don't forget about VirusTotal
A recent posting on the VirusTotal blog announced a new addition to Google's multi-malware-scanner:

https://blog.virustotal.com/2020/06/virustotal-cynet.html

In clever programmereese the blog was titled: VirusTotal += Cynet

For those not conversant in coding, the "+=" expression is a simplification of a = a+ b. It should always be the goal of computer languages to both minimize writing errors and maximize reading ease. Shortening "a = a + b" to "a += b" is VASTLY easier to both write and to read. It's easier to read because it explicitly reveals the programmer's intent to increase 'a' by 'b'. It's true that the longer version does the same, but the intent is much less clear. Anyway, I digress...

We welcome the Cynet engine to VirusTotal. In the words of the company:

"Cynet 360 is an autonomous breach protection platform that includes multi-layered anti malware capabilities including AI-based static analysis, process behavior monitoring, memory monitoring, sandboxing, and granular whitelisting, interlocking together to protect against malicious executables, exploits, scripts, Macros, LOLbins, malicious process injection and other fileless attacks. Cynet 360 protection ranges across the entire malware lifecycle identifying malicious attributes in either the pre-execution stage by analyzing the file in its binary form or across multiple stages throughout the process execution."

The blog notes that "Cynet has expressed its commitment to follow the recommendations of AMTSO and, in compliance with our policy, facilitates this review by Virus Bulletin, an AMTSO-member tester." (AMTSO is the Anti-Malware Testing Standards Organization).

I wanted to mention this mostly to remind all of our listeners of VirusTotal, a service which I use and would hate to be without.

The other day I needed some piece of long abandoned software. So I went digging around the Internet and ostensibly found it on VetusWare (https://vetusware.com/) an abandonware site. Much as I wanted to trust the download, this is precisely how malware gets into people's machines. So I first inspected the packaging, checked for file signatures, dates, and so forth. And a key part of any such checking I do is to always drop any questionable file onto VirusTotal at VirusTotal.com.

I'm not suggesting that anyone should regard anything VirusTotal tells you as gospel... but it's one additional piece of useful telemetry about anything you might have reason to question. Just remember that it's always there and it's free to use.

Miscellany

Edge on Win7

I updated a Win7 machine of mine and it DID receive an offer to install Edge. Win Update showed that two important updates were available, but Edge was NOT selected. When I installed it it was aggressive about copying Chrome's settings. I allowed it to do so and it installed all of the same add-ons -- LastPass and uBlock Origin.

New version of Gravity.

I fixed a bug in the most recent release of Gravity being hosted on GRC to creating v3.0.10. The bug was not mine. A couple of weeks ago Gravity users, including me, were unable to open several recent postings in the grc.spinrite.dev newsgroup. Gravity would just crash. This is where community-driven open source software really comes into its own. Gravity was abandoned some time ago. But it is by far my favorite way of interacting with newsgroups and newsgroups are by far the best way I have found of working with a community of people who are interested in participating in the development testing of new code. So when my trusty old Gravity died when the year switched to 2020, I needed to open it up to fix it. At that time I also added a few additional features that I had long wanted, such as automatically jumping down to and auto-selecting a newsgroup's first unread posting.

Anyway, the problem last week occurred when more than one base64-encoded object was attached to a posting. Thunderbird was used to create such a posting, and Gravity never had the ability to open such a posting due to an error in its code. The original coder failed to set the length of a string. (How familiar does that sound?) So, anyway, I found and fixed the problem and we now have v3.0.10 available for download from GRC. I'm just noting it for those who have been using Gravity and might not have see that activity over in GRC's newsgroups.

Closing The Loop

BlueLED @blueled

@SGgrc Can you tell us again, what was the brand and model of the switch/router you were using for traffic control? It was not a common brand as I remember.

So, the software is pfSense. It's open source, based upon FreeBSD UNIX, and is wonderful. It can be loaded onto any Intel PC based hardware that FreeBSD supports. So it's perfect for a DIY user. For someone who wants a pfSense-based appliance, the company NetGate offers turnkey ready-to-go pfSense based routers for sale, starting with the SG-1100 (no relation) for $179.

https://www.netgate.com/
https://www.netgate.com/products/appliances/

SpinRite

Work on SpinRite's AHCI driver is continuing and we're making rapid progress. I don't have anything specific yet to announce, though I did notice that more than 1500 people had grabbed a copy of our new InitDisk utility for reformatting USB drives, so that's neat.

Ripple20 Too

Last week's titled topic was our disclosure and discussion of the very worrisome "Ripple20" discovery that a highly used (for several decades) embedded TCP/IP stack was riddled with at least 19 vulnerabilities, several of the worst being very serious no-user-action-required remote code execution. I ended that discussion last week by noting that "The Internet's already target-rich environment just got a whole lot richer."

We're back to this important topic this week as a great many more details of the impact of this sweeping industry-wide problem are coming to light.

Our often-cited friends at BleepingComputer have pulled together the most comprehensive coverage that I've seen, so I'm going to start by paraphrasing some of what they've written because it nicely characterizes the industry's present situation:

BleepingComputer wrote: The dust is far from settled following the disclosure of the 19 vulnerabilities in the TCP/IP stack from Treck, collectively referred to as Ripple20, which could help attackers take full control of vulnerable devices on the network.

Treck's code is fundamental for the embedded devices it is implemented on, because it bestows network communication to them and is present on gadgets used in a variety of sectors: technology, medical, construction, mining, printing, energy, software, industrial control systems (ICS), telecom, retail and commerce.

The company has notified its customers and issued patches, but a week after the Ripple20 announcement from security research group JSOF, the full impact [still] remains unclear. This is because Treck's code is licensed and distributed under different names or serves as a foundation for a new network stack.

[And I'll interject that it turns out that it is also internationalized, resold and rebranded under other names as well, so a mid-chain OEM might not even know that their system is using vulnerable code that originated at Treck.]

Concerted efforts from national-level cybersecurity agencies and private companies in the field are ongoing to identify businesses with products vulnerable to issues in the Ripple20 vulnerability set.

What is clear at the moment, though, is that the healthcare industry is particularly affected and should be on high alert.

Elad Luz, head of research at CyberMDX, a company focused on security in medical devices and involved in identifying vulnerable products, told BleepingComputer that their initial investigation placed healthcare industry's exposure at more than seven times than that of manufacturing.

And that was confirmed -- with numbers -- by [the security firm] Forescout who is also involved in the effort. On the day of the disclosure, Forescout revealed that there were six times more

vulnerable healthcare-related equipment than in the retail sector. What are the numbers?

https://www.forescout.com/company/blog/identifying-and-protecting-devices-vulnerable-to-ripple20/

#	Vertical	Devices matching Treck signatures
1	Healthcare	52,935
2	Retail	8,347
3	Manufacturing	7,333
4	Government	5,904
5	Financial Services	5,225
-	**Others**	**11,346**

Forescout explained that, from their analysis, the most common device types running Treck include infusion pumps, printers, UPS systems, networking equipment, Point of Sale devices, IP cameras, video conferencing systems, building automation devices and Industrial Control System devices.

They added that to exploit Ripple20 vulnerabilities, an attacker needs a direct connection to an affected device or a routed path to internal networks. This means devices directly connected to the internet are those most at risk. An attacker could target these devices first, compromise them and move laterally within the network to access or infect other devices.

As an example of the impact of these vulnerabilities, a series of Shodan searches for 37 specific known-vulnerable device models from 18 different vendors (including printers, IP cameras and video conferencing systems, networking equipment and Industrial Control System devices) revealed there are around 15,000 internet-connected instances of these affected devices that could potentially be directly compromised by anybody on the internet.

Compared to the number of known-vulnerable devices, estimated in the many hundreds of millions, that number is not high, but that was only a scan for specific known signatures. And, after all, it only takes one exposed device on the network of a nuclear power plant or managing a nation's electric power grid to ruin everyone's day. It is estimated that the actual number of publicly exposed Internet-connected devices is a great deal higher, they just aren't readily identifiable from a Shodan scan and/or they haven't been identified yet.

BleepingComputer has assembled a nice alphabetical list of known-affected manufacturers and their devices:

Aruba Networks
A preliminary advisory based on an initial investigation is available from Aruba Networks (HPE subsidiary), listing L2/L3 switches produced under the Aruba or HP ProCurve brand names.

Baxter US
The Baxter healthcare company announced that some of its Spectrum Infusion System's Wireless Battery Modules are impacted by Ripple20 because they run Digi Net+OS with Treck's TCP/IP stack:

35083 - b wireless battery module
35162 - b/g wireless battery module
35195 - a/b/g/n wireless battery module
35223 - a/b/g/n wireless battery module
36010 – a/b/g/n wireless battery module

B. Braun
The medical and pharmaceutical device company notified that vulnerable Treck code is present in its Outlook 400ES Safety Infusion Pump System and no other products are affected by the Ripple20 set of issues.

A Braun advisory stated that: "To date, B. Braun has received 24 patches from Treck to resolve vulnerabilities in the software. We have analyzed the patches and determined that 20 of them are not applicable to the Outlook 400 ES platform (the product is not susceptible to these vulnerabilities). The four remaining patches continue to be analyzed to determine the scope, severity, and impact of each vulnerability"

Beck/HMS Industrial Networks AB
Older products from the company run vulnerable components but most HMS products do not use Treck's software library. The company provides a list of products that are not vulnerable and will update it as more products are discovered to be safe from Ripple20.

CareStream
CareStream announced that several of its products may be impacted by Ripple20, promising an updated list as other their investigation continues.

CR975
DIRECTVIEW Max CR System
DIRECTVIEW Classic CR System
DIRECTVIEW Elite CR System
HPX Pro
HPX-One

It's worth noting that the U.S. CERT Coordination Center at Carnegie Mellon on June 23 lists CareStream equipment as being vulnerable to all Ripple20 vulnerabilities.

Caterpillar
Isn't being forthcoming with details, but an undisclosed number of products are known to be vulnerable to Ripple20.

Cisco
The following routing and switching gear from Cisco is vulnerable to all security flaws disclosed in the Ripple20 advisory from JSOF.

Product	Cisco Bug ID Fixed Release Availability
Routing and Switching - Enterprise and Service Provider	
Cisco ASR 5000 Series Routers	CSCvu68945
Cisco GGSN Gateway GPRS Support Node	CSCvu68945
Cisco IP Services Gateway (IPSG)	CSCvu68945
Cisco MME Mobility Management Entity	CSCvu68945
Cisco PDSN/HA Packet Data Serving Node & Home Agent	CSCvu68945
Cisco PGW Packet Data Network Gateway	CSCvu68945
Cisco System Architecture Evolution Gateway (SAEGW)	CSCvu68945

The company is currently investigating its product line to determine if other products are affected by the flaws and will update the advisory with new information.

Dell
Ripple20 vulnerabilities in Dell products are inherited from an Intel component that is present in Dell Client Platforms (advisory) and from Teradici firmware and remote workstation cards in Dell Precision and Dell Wyse Zero Client products (advisory).

Dell has released fixes and encourages customers to prioritize updating their systems to the latest firmware version.

Digi International
The company found that any embedded device using the NET+OS 7.X software development platform along with the products below are affected by Ripple20:

- Connect SP
- Connect ME
- Connect ES
- Connect EM
- Connect WME
- Connect 9C
- Connect 9P
- ConnectPort X4 (all variants)
- ConnectPort X2 (NOT X2e)
- ConnectPort TS (Not LTS)
- AnywhereUSB (excluding Plus)
- NetSilicon 7520, 9210, 9215,9360, 9750

New firmware versions are available for the products since late April and customers are strongly recommended to install them, the company advises in its security notice.

Eaton
The multinational power management company announced in a security bulletin that some of its products rely on Treck's library to implement IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4, and ARP and are vulnerable to multiple Ripple20 issues.

The company's efforts to identify all affected products are ongoing. Below is a provisional list:

CL-7 voltage regulator control
Form 4D recloser control
Form 6 recloser control
Edison Idea and IdeaPLUS relays (all variants)
Metered Input Power Distribution Units
Metered Outlet Power Distribution Units
Managed Power Distribution Units
High Density Power Distribution Units

What was I saying about power grids??

Green Hills Software
This developer of real-time operating systems (RTOS) and programming tools for embedded devices provides the GHnet v2 network stack, which is based on Treck's TCP/IP stack.

HCL Technologies
An undisclosed number of products from this vendor are vulnerable to Ripple20 but no official statement is currently available on the company's page for security bulletins.

Hewlett Packard Enterprise (HPE)
No advisory is available at the moment but information is expected to be released in the near future in a security bulletin from the company.

HP Inc. and Samsung
An advisory from the vendor refers to HP and Samsung printer vulnerable to Ripple20. Dozens of then are affected:

HP Laser
HP LaserJet Pro
HP Neverstop Laser
Samsung proXpress
Samsung MultiXpress
HP DeskJet
HP OfficeJet
HP OfficeJet Pro
HP Ink Tank
HP Smart Tank

All printers have received new firmware that correct the issues; customers are strongly advised to install the updates, the security bulletin Urges.

Another advisory from the company asserts that other issues related to the Treck TCP/IP stack in HP products have been inherited from Intel components. And speaking of Intel...

Intel
Some versions of Intel Active Management Technology (AMT) and Intel Standard Manageability (ISM) are vulnerable to three issues in the Ripple20 set.

MaxLinear
CyberMDX lists MaxLinear chip maker among the vendors with products affected by Ripple20. The company has not published any statement or advisory naming the impacted devices.

Rockwell Automation
An advisory from Rockwell Automation is available for customers only. An undisclosed number of products from this company is affected by the entire Ripple20 vulnerability set.

Schneider Electric
Dozens of products from Schneider Electric are impacted by all 19 Ripple20 vulnerabilities. The vendor published a list, updated on June 24, with dozens of devices that are vulnerable.

The advisory from Schneider Electric also recommends mitigations to limit the risk of exploitation. An up-to-date version of the document can be downloaded from the company's security notification for Ripple20.

Teradici
Teradici software firm acknowledged that Ripple20 issues exist in versions of Tera2 Zero Client firmware 20.01.1 and prior as well as Tera2 Remote Workstation Card 20.01.1 and prior.

The developer has released new firmware versions to fix the bugs, the company announced in an advisory from June 17.

Xerox
In a short security bulletin on June 16, Xerox confirmed that some of its devices are impacted by Ripple20 and provided new firmware versions for three of its printers:

Xerox B205
Xerox B210
Xerox B215

Zuken Elmic
The company distributes Treck's TCP/IP stack under the name KASAGO. This means that any product running this library is vulnerable to Ripple20. And, again, given the actual number of devices known to be affected by this, this is still just scratching the surface.