

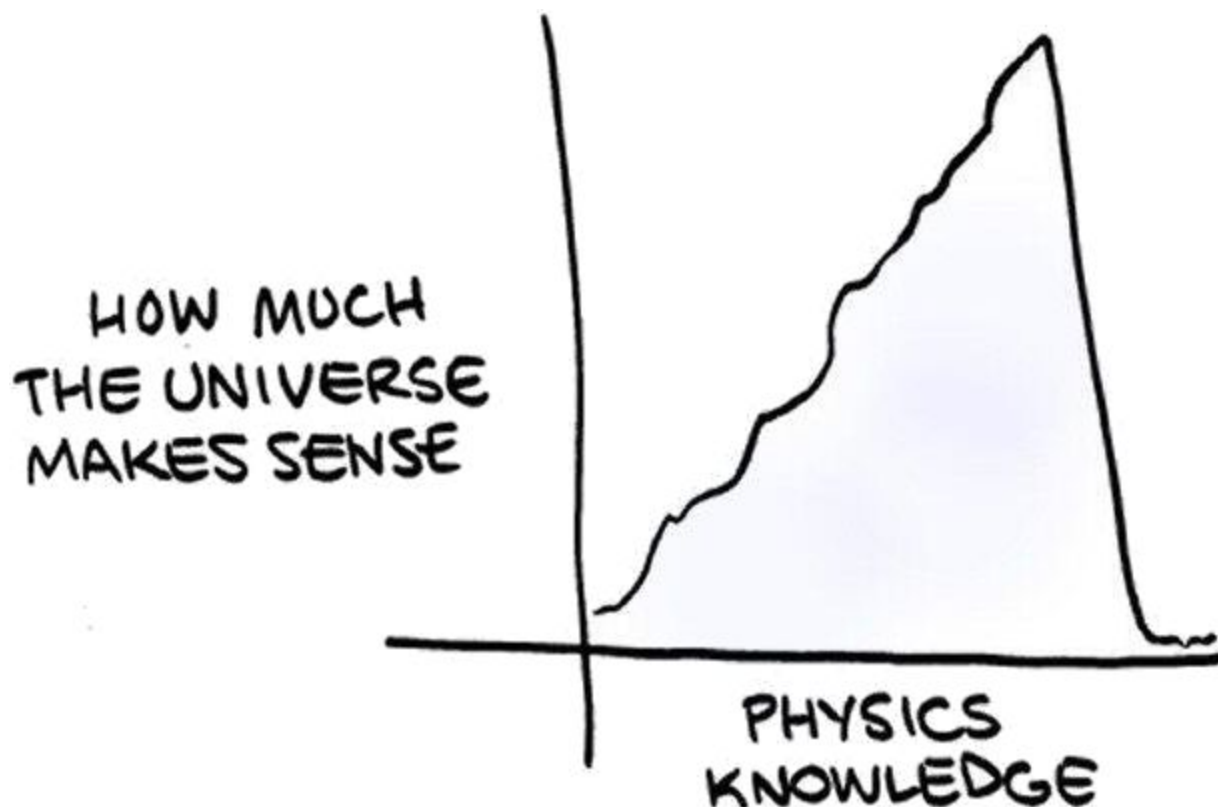
Security Now! #609 - 04-25-17

The Double Pulsar

This week on Security Now!

This week Steve and Leo discuss how one of the NSA's Vault7 vulnerabilities has gotten loose, a clever hacker removes Microsoft deliberate (and apparently unnecessary) block on Win7/8.1 updates for newer processors, Microsoft refactors multifactor authentication, Google to add native ad-blocking to Chrome... and what exactly *are* abusive ads?, Mastercard to build a questionable fingerprint sensor into their cards, are Bose headphones spying on their listeners?, 10 worrisome security holes discovered in Linksys routers, MIT cashes out half of its IPv4 space, and the return of two meaner BrickerBots. Then some Errata, a bit of Miscellany, and, time permitting, some "Closing the Loop" feedback from our podcast's terrific listeners.

Our Picture of the Week



By Cartoonist Zach Weinersmith

Security News

DoublePulsar

- From the "This didn't take long" department: Less than two weeks after the third dump of the Shadow Brokers document dump, believed to have originated with NSA, make tens of thousands of Windows machines are now infected with the "DoublePulsar" backdoor.
- DoublePulsar in a RAM-resident implant which gets into Windows through the "EternalBlue" exploit, also believed to have originated with the NSA.
- Across the industry, malware researchers are comparing this to the CONFICKER worm that plagued us nine years ago, back in 2008. Concicker leveraged a Windows RPC flaw to propagate and even now, nearly a decade later, malware sleuths are constantly discovering Conficker infections.
- Security Now #193, April 23rd, 2009: "Conficker" - Steve analyzes Conficker, the sophisticated worm that has spread to more than 10 million PCs worldwide.
- The numbers vary, but there's consensus that more than five million of Windows machines have port 445 publicly exposed and as many as 50,000 machines have already been infected.
- A malware hunter "@Below0Day" performed a 25-hour Internet scan.

```
<finished time="1492513797" timestr="2017-04-18 11:09:57" elapsed="40560" />  
<hosts up="5561708" down="0" total="5561708" />
```

- He posted: Started it on the 19th around 7am. On the 20th around 8am it was done!
 - 30,626 instances of #DOUBLEPULSAR implant detected!
 - Masscan port 445 ~ 5,561,708 open ports!
- Meanwhile, Binary Edge, a Swiss-based security firm reported finding more than 107,000 infected machines in their recent multi-day scan. And Errata Security's Robert Graham (developer of the early BlackIce personal firewall) reportedly detected approximately 41,000 infected machines.
- Dan Tentler, founder and CEO of the Phobos Group, said internet-net wide scans he's running have found about 3.1 percent of vulnerable machines are already infected (between 62,000 and 65,000 so far), and that percentage is likely to go up as scans continue. Tendler said: "This is easily describable as a bloodbath."
- It's a classic backdoor. Tendler said: "It does not open new ports. Once the backdoor is present, it can do one of four things: either it responds to a specific ping request (such as a heartbeat), it can uninstall itself, load shellcode, or run a DLL on the host. That's it. It's only purpose is to provide a covert channel by which to load other malware or executables."

- DoublePulsar hooks into the kernel in RAM and rides along on port 445. This allows its presence to be "pinged" for detection. While resident, attackers have the ability to execute any raw shellcode payload that they choose.
- Matthew Hickey, founder of U.K. consultancy Hacker House added: "The fact that people are using these attack tools in the wild is unsurprising. It shows you these tools were very well developed, very weaponized and don't require a lot of technical sophistication. So attackers are quick to adopt them into their repositories and toolkits. Subsequently, they're using them as-is."
- Kaspersky Labs / Threatpost:
DoublePulsar works on older Windows Server versions with older versions of PatchGuard kernel protection; modern versions of Windows such as Windows 10 have better kernel checks that could help block or prevent these hooks deep into the OS. Once DoublePulsar is on a compromised host, an attacker can drop additional malware or executables onto a machine, meaning that this bug will quickly move from the exclusive realm of nation-state hackers to cybercriminals, and it may be a matter of time before ransomware and other commodity malware and botnets take advantage of these exploits to spread.
- One drawback for the attacker is that since the attack lives in memory, once a machine is rebooted, it's gone. DoublePulsar also comes with a kill or burn command that won't remove the infection, but does prevent others from making use of the backdoor.
- Woody Leonard, writing in his "Woody on Windows" InfoWorld column, notes that even if your own machine is not exposed publicly, if any other machine on your private network is exposed, the infection of that machine can spread within the network. And I'll note that port 445 is how Windows machines glue themselves together within an intranet, so that most systems within a network DO have access to each other's port 445.
- Woody's column has a bunch of carefully organized version and patch information for Win 7, 8.1 and 10, with which versions of what are needed to be secure against this.
 - <http://www.infoworld.com/article/3191897/microsoft-windows/more-shadow-broke-rs-fallout-doublepulsar-zero-day-infects-scores-of-windows-pcs.html>
- Detection Script
 - <https://github.com/countercept/doublepulsar-detection-script>

A user-designed patch to allow Win7 & 8.1 to run on the latest Intel chipsets

- <https://github.com/zeffy/kb4012218-19>
- Kaby Lake and Ryzen PCs
- Bleeping Computer:
GitHub user Zeffy has created a patch that removes a limitation that Microsoft imposed on users of 7th generation processors, a limit that prevents users from receiving Windows updates if they still use Windows 7 and 8.1.

This limitation was delivered through Windows Update KB4012218 (March 2017 Patch Tuesday) and has made many owners of Intel Kaby Lake and AMD Bristol Ridge CPUs very angry last week, as they weren't able to install any Windows updates.

Microsoft's move was controversial, but the company did its due diligence, and warned customers of its intention since January 2016, giving users enough time to update to Windows 10, move to a new OS, or downgrade their CPU, if they needed to remain on Windows 7 or 8.1 for various reasons.

When the April 2017 Patch Tuesday came around last week, GitHub user Zeffy finally had the chance to test four batch scripts he created in March, after the release of KB4012218.

His scripts worked as intended by patching Windows DLL files, skipping the CPU version check, and delivering updates to Windows 7 and 8.1 computers running 7th generation CPUs.

The four batch scripts are now available on GitHub, open-sourced and ready to be inspected, just in case anyone fears Zeffy might have disguised any malware.

According to Zeffy's README file, he created the four batch scripts by reverse engineering the KB4012218 Windows Update, and comparing versions of the new files with the ones already on his PC.

By running a simple diff operation on these files, he was able to discover two new functions "IsCPUSupported(void)" and "IsDeviceServiceable(void)" inside the March 2017 version of wuaueng.dll, delivered through KB4012218.

Zeffy's scripts patch this DLL file and make the two functions output "1", which translates to "supported CPU." This, in turn, starts the update procedure, delivering new security updates to users Microsoft wanted to block.

"The only downside of these solutions is you have to apply a new patch whenever wuaueng.dll gets updated," says Zeffy in his GitHub repo README. Fortunately, the entire task doesn't take long to complete.

Bleeping Computer hasn't tested Zeffy's patch because we don't have a 7th-gen CPU on hand. It's recommended that you create a system restore point and save a copy of the original wuaueng.dll file just in case things go horribly wrong.

Links:

- <https://www.bleepingcomputer.com/news/microsoft/user-made-patch-lets-owners-of-next-gen-cpus-install-updates-on-windows-7-andamp-8-1/>
- <http://www.pcworld.com/article/3191247/windows/user-created-patch-lets-kaby-lake-and-ryzen-pcs-receive-windows-7-updates.html>
- <http://www.computerworld.com/article/3191427/microsoft-windows/developer-lifts-windows-7s-update-blockade-with-unsanctioned-patch.html>
- <http://www.networkworld.com/article/3190832/security/bypass-microsofts-update-block-for-windows-7-8-1-pcs-with-kaby-lake-ryzen.amp.html>

Microsoft refactors multifactor

A Microsoft Windows account may now be registered with the Microsoft Authenticator app for iOS and Android... after which the app will receive a Windows logon confirmation prompt. So you unlock your mobile device, acknowledge the request, and you're in.

Is this multifactor?

Microsoft says yes because they think that phrase is the holy grail. But I would say, no, since "multifactor" means multiple SECRET factors, and your username is not a secret -- leaving this with having just one factor -- your device.

But "multifactor", per se, is not the holy grail. We have only needed to resort to the added encumbrance of multiple factors because the "factors" themselves have been individually weak. So having more "individually weak" single factors, where they must all be correct in aggregate, provides stronger final security.

But... If you have a super-strong single factor, the result is super-strong authentication. I'm, of course, quite familiar with this notion, because it's the entire basis for SQL. SQL provides super-strong, single-factor, fully open system, low-encumbrance authentication.

Links:

- <https://blogs.technet.microsoft.com/enterprisemobility/2017/04/18/no-password-phone-sign-in-for-microsoft-accounts/>
- <https://arstechnica.com/information-technology/2017/04/microsoft-turns-two-factor-authentication-into-one-factor-by-ditching-password/>
- <https://threatpost.com/microsoft-touts-new-phone-based-login-mechanism/125065/>
- <http://fortune.com/2017/04/19/microsoft-password/>

Google to add NATIVE ad blocking to Chrome

<https://www.wsj.com/articles/google-plans-ad-blocking-feature-in-popular-chrome-browser-1492643233>

WSJ: Alphabet Inc.'s Google is planning to introduce an ad-blocking feature in the mobile and desktop versions of its popular Chrome web browser, according to people familiar with the company's plans.

The ad-blocking feature, which could be switched on by default within Chrome, would filter out certain online ad types deemed to provide bad experiences for users as they move around the web.

Google could announce the feature within weeks, but it is still ironing out specific details and still could decide not to move ahead with the plan, the people said.

Unacceptable ad types would be those recently defined by the Coalition for Better Ads, an industry group that released a list of ad standards in March. According to those standards, ad formats such as pop-ups, auto-playing video ads with sound and "prestitial" ads with countdown timers are deemed to be "beneath a threshold of consumer acceptability."

In one possible application Google is considering, it may choose to block all advertising that appears on sites with offending ads, instead of the individual offending ads themselves. In other words, site owners may be required to ensure all of their ads meet the standards, or could see all advertising across their sites blocked in Chrome.

Google declined to comment.

The ad-blocking step may seem counter-intuitive given Google's reliance on online advertising revenue, but the move is a defensive one, people familiar with the plans said.

[And I think it's a BRILLIANT and welcome move, leveraging the strength of Chrome to enforce content behavior much as Google as used their Chrome dominance to enforce encryption behavior.]

Uptake of online ad blocking tools has grown rapidly in recent years, with 26% of U.S. users now employing the software on their desktop devices, according to some estimates.

By switching on its own ad-filter, Google is hoping to quell further growth of blocking tools offered by third-party companies, the people said, some of which charge fees in exchange for letting ads pass through their filters.

Google already pays to be part of an "Acceptable Ads" program offered by Adblock Plus. As a result, advertising on Google's search engine and some of the other ads it powers are allowed to pass through Adblock Plus's filters.

But the continued growth of ad-blocking is a worrying trend for Google, which generated over \$60 billion in revenue from online advertising in 2016. It's also a concern for other online publishers and services that rely on advertising revenue to support their businesses, many of which work with Google to help sell advertising space on their properties.

The Chrome browser now accounts for a large portion of web-browsing globally, so switching on ad-filters within it could give Google more control over the ad-blocking situation, industry observers say.

In the U.S. Chrome has nearly 47.5% of the browser market across all platforms, according to online analytics provider StatCounter.

Coalition for Better Ads Releases Initial Better Ads Standards for Desktop and Mobile Web in North America and Europe

- <https://www.betterads.org/coalition-for-better-ads-releases-initial-better-ads-standards-for-desktop-and-mobile-web/>
- <https://www.betterads.org/standards/>

- Desktop:
 - Pop-up Ads
 - Auto-playing Video Ads with Sound
 - Prestitial Ads with Countdown
 - Large Sticky Ads

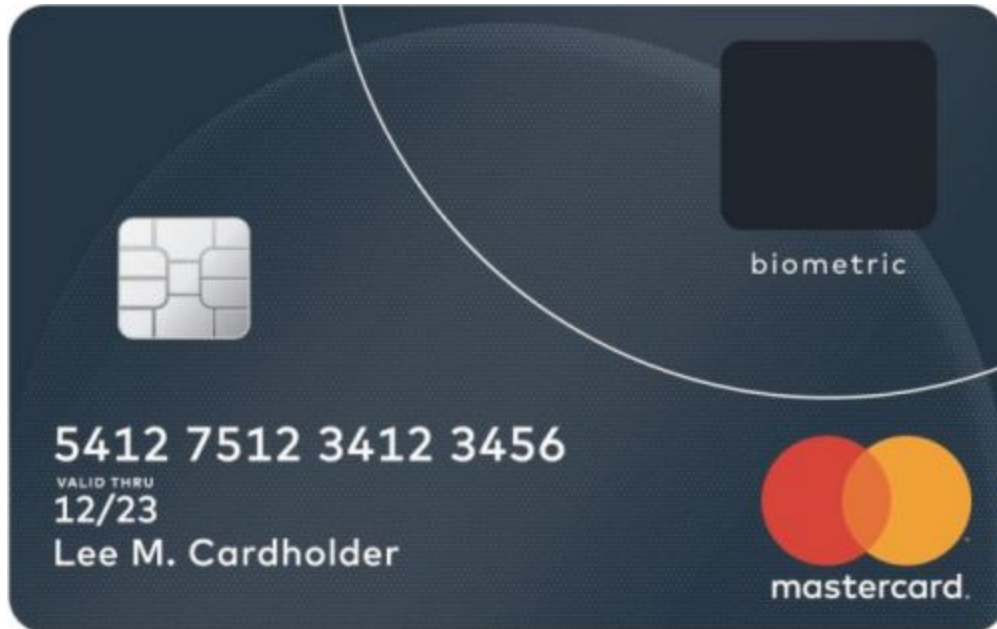
- Mobile: (Same)
 - Pop-up Ads
 - Auto-playing Video ads with Sound
 - Prestitial Ads
 - Large Sticky Ads.

 - PLUS...
 - Ad Density higher than 30%
 - Flashing Animated Ads
 - Positional Ads with Countdown
 - Full-screen Scrollover Ads

"Thumbs Up: Mastercard Unveils Next Generation Biometric Card"

<http://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/>

EMV Terminals: EMV stands for Europay, MasterCard, and Visa.



A cardholder enrolls their card by registering with their financial institution. Upon registration, their fingerprint is converted into an encrypted digital template that is stored on the card. The card is then ready to be used at any EMV card terminal globally.

When shopping and paying in-store, the biometric card works like any other chip card. The cardholder inserts the card into a retailer's terminal while placing their finger on the embedded

sensor. The fingerprint is verified against the template and – if the biometrics match – the cardholder is successfully authenticated and the transaction can then be approved with the card never leaving the consumer's hand.

The problems:

- You cannot turn your card over to a restaurant server to pay your tab.
- Security Theater:
Fuzzy matching prevents security: If it was a long exact PIN, then it could be hashed to create an exact key that could decrypt an enclave to reveal one's account number and authorization.

But, as we know, fingerprints are not precise. So a "heuristic go/no-go judgement" needs to be made about whether the fingerprint is "close enough". That means that, just as "Zeffy" simply removed the "IsCPUsupported?" test from the most recent Microsoft Update, someone could hardwire the "is fingerprint close enough?" test to unlock the card.

Some Bose Wireless Headphones Track and Share What You Listen to, Lawsuit Says

<http://www.consumerreports.org/privacy/some-bose-wireless-headphones-track-what-you-listen-to/>

First of all... it's NOT the headphones that are tracking, it's the optional companion Bose app that "improves the user experience."

According to the class action lawsuit complaint filed last week in a federal court in Illinois, when owners of Bose wireless headsets use the Bose Connect app on their smartphones, it collects information about the songs listened to and allegedly transmits this data — along with other identifying information — to third parties. The lawsuit contends this collection and sharing occurs without the users' permission, and amounts to a "wholesale disregard for consumer privacy rights."

The Bose Connect app is not a music player. It's a companion app that is intended to give the owners of various Bose headsets and Bose speakers additional control over their devices. For example, it allows for more variable levels of noise canceling. It also lets users share the same audio between two Bose wireless devices.

The plaintiff claims that Bose Connect is programmed to "continuously record the contents of the electronic communications that users send to their Bose Wireless Products from their smartphones, including the names of the music and audio tracks they select to play along with the corresponding artist and album information, together with the Bose Wireless Product's serial numbers."

The serial number information is important, notes the lawsuit, because if a customer has registered their product with Bose, then the company can put together all the collected audio information along with the personal data provided during the registration process: name, email address, and phone number.

One of the third parties that allegedly receives information from the Bose Connect app is Segment.io, a company whose homepage touts, "Collect all of your customer data and send it

anywhere.”

By designing the Bose Connect app to “contemporaneously and secretly collect” information about what a user is listening to, and then sending that allegedly intercepted information on to a third party, the lawsuit contends that Bose has violated the Federal Wiretap Act.

The complain adds: “No party to the electronic communications alleged herein consented to [Bose’s] collection, interception, use, or disclosure of the contents of the electronic communications.” It notes that users of these devices were never given the option to consent.

Jay Edelson who is representing the plaintiffs said: “This case shows the new world we are all living in. Consumers went to buy headphones and were transformed into profit centers for data miners.”

<https://consumermediallc.files.wordpress.com/2017/04/bosecomplaint.pdf>

Multiple security holes discovered in Linksys routers

Last Thursday, Tao Sauvage, a security researcher with IOActive published the results of his reverse engineering of the most recent models of Linksys routers. In his case it was model EA3500 Series also known as "Smart Wi-Fi" router. Smart Wi-Fi is the latest family of Linksys routers and includes 25 different models that use the latest 802.11N and 802.11AC standards. Even though they can be remotely managed from the Internet using the Linksys Smart Wi-Fi free service <<shudder>> Tao focused upon the router itself.

Note that this includes four WRT model routers as well.

They extracted and forensically examined the router's firmware, identifying simply by inspection, 10 security vulnerabilities ranging from low to high risk, six of which can be exploited remotely by unauthenticated attackers.

Two of the security issues they identified allow unauthenticated attackers to create a Denial-of-Service (DoS) condition on the router. By sending a few requests or abusing a specific API, the router becomes unresponsive and reboots. The Admin is unable to access the web admin interface and users are unable to connect until the attacker stops the DoS attack.

Attackers can also bypass the authentication protecting the CGI scripts to collect technical and sensitive information about the router, such as the firmware version and Linux kernel version, the list of running processes, the list of connected USB devices, or the WPS pin for the Wi-Fi connection. Unauthenticated remote attackers can harvest sensitive information using available APIs to list all connected devices and their respective operating systems, access the firewall configuration, read the FTP configuration settings, or extract the SMB server settings.

An AUTHENTICATED attacker can inject and execute commands on the operating system of the router with root privileges. One possible action for such an attacker is to create backdoor accounts and gain persistent access to the router. Backdoor accounts would not be shown on the web admin interface and could not be removed using the Admin account. It should be noted that they did not find a way to bypass the authentication protecting that vulnerable API and that

authentication is different from the authentication protecting the CGI scripts. However, they discovered that 11% of the ~7,000 publicly exposed routers were using default credentials and could therefore be taken over and "rooted" by remote attackers.

They disclosed the vulnerabilities and shared the technical details with Linksys in January 2017. Since then, they have been in constant communication with Linksys to validate the issues, evaluate the impact, and synchronize their respective disclosures.

They noted in their reports that Linksys has been exemplary in handling the disclosure and that Linksys is taking security very seriously. Linksys is proactively publishing a security advisory to provide temporary solutions to prevent attackers from exploiting the security vulnerabilities they identified, until a new firmware version is available for all affected models.

Using SHODAN to search for vulnerable devices,

They found about 7,000 vulnerable devices exposed at the time of the search. The large majority of the vulnerable devices (~69%) are located in the USA and the remainder are spread across the world, including Canada (~10%), Hong Kong (~1.8%), Chile (~1.5%), and the Netherlands (~1.4%). Venezuela, Argentina, Russia, Sweden, Norway, China, India, UK, Australia, and many other countries representing < 1% each.

<http://www.linksys.com/us/support-article?articleNum=246427>

Linksys (Now owned by Belkin, not Cisco): We are working to provide a firmware update for all affected devices. While we are building and testing the fixes we recommend performing the following steps:

- 1) Enable Automatic Updates. Linksys Smart Wi-Fi devices include a feature to automatically update the firmware when new versions are available.
 - <http://www.linksys.com/us/support-article?articleNum=140124#b>
- 2) Disable WiFi Guest Network if not in use.
 - <http://www.linksys.com/us/support-article?articleNum=140861>
- 3) Change the default Administrator password.
 - <http://www.linksys.com/us/support-article?articleNum=142491>

MIT is selling off HALF of their 16 Million IPv4 Addresses

Back in the 1970's MIT senior research scientist at MIT's Computer Science and Artificial Intelligence Lab saw the importance of IPv4 addresses and requested an early allocation of them, both to support research and eventually to support all of computing at MIT. They were given the entire 18/8 Class A IPv4 network. So all IPs beginning with 18.x.x.x.

14 million of those addresses were never used and they recently concluded that at least eight million -- or half of their original allocation -- are excess and can be sold without impacting their current or future needs.

The funds raised from the sale will support MIT's migration to IPv6, and Amazon was the winning

bidder, purchasing the IPv4 space from MIT.

IPv4 addresses, subject to discounts for quantity, are going for around \$11 to \$12/each.

Recently Closed Auctions:

- http://www.ipv4auctions.com/previous_auctions/

Also, last Thursday, BrickerBot.3 appeared... and then BrickerBot.4

- (And their author has been heard from)
- Persistent Denial of Service: PDoS
 - <https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/>
- The latest BrickerBots are attacking harder and faster with greater geographical dispersion and different sources than earlier BrickerBots. They also evidence additional research, having altered and added at least four new exploit attempts.
- The latest BrickerBots are, like the earlier ones, using the same Mirai exploit to compromise and gain entry to the devices. Specifically, any 'busybox' based Linux device that has Telnet publicly exposed with factory default credentials is a potential victim.
- The Author has spoken:
The Janit0r reached out to Victor Gevers (<https://twitter.com/0xDUDE>) based on a comment Victor made in one of the first articles on BrickerBot.1 and .2. The person confirmed he is the Janit0r on Hackforums and he is the author of BrickerBot.
- Quote: "Like so many others I was dismayed by the indiscriminate DDoS attacks by IoT botnets in 2016. I thought for sure that the large attacks would force the industry to finally get its act together, but after a few months of record-breaking attacks it became obvious that in spite of all the sincere efforts the problem couldn't be solved quickly enough by conventional means."
- Quote: "I consider my project a form of "Internet Chemotherapy" I sometimes jokingly think of myself as The Doctor. Chemotherapy is a harsh treatment that nobody in their right mind would administer to a healthy patient, but the Internet was becoming seriously ill in Q3 and Q4/2016 and the moderate remedies were ineffective."

Errata

Vasile

- Re SN608 Punycode: Just to be meticulous (I know you treasure 100% accuracy) , Unicode has space for up to 0x110000 code points, more than could fit into 16 bits. They can be encoded in multiple ways, ranging from variable-length UTF-8 to fixed-size UTF-32.
- Right.
 - ASCII is 128 "code points" (7 bits.)
 - Extended ASCII is 256 "code points" (8-bits)
 - UNICODE is divided into "planes" with 16-bits per plane, and last week I was only referring to what's known as the "basic multilingual plane", which is 16-bits and thus 64k code points.
 - But there are also up to 16 "supplemental planes", each having 64k code points, for a grand maximum total of 17, 64k planes, of 1,114,112 code points.

Rick (@rpodric)

- @SGgrc Just a note re the apparent fix in Chrome 59 for Punycode, that 59 is the dev version. 57 is current stable, with 59 due by Jun 6.
- My Chrome is back on #49 and I just reverified that Punycode is disabled.

Miscellany

elheffe

- @SGgrc Not sure if I should thank you or be mad -- Frontier Saga is sucking my productivity away!
- Yeah, tell me about it! I've finished all 19 books in print. And, if anything, the 2nd series starts off EVEN BETTER than the first. Book #3 of the second series is unbelievably good! Worth reading everything up to there just for the setup! :) Enjoy!!
- elheffe: I am halfway through book six. Had to tear myself away to work on cleaning the garage. You weren't kidding about it being non-stop action! Thanks for everything you do! Keep the recommendations coming.

Opher Banarie (@cubeERT)

- <https://www.youtube.com/watch?v=oIS5n9Oyzsc>
- This explains so much!

SpinRite

From: "KeenDreams"

Subject: A slightly different spinrite story with an apology

Date: Wed, 19 Apr 2017

Dear Steve, First off thanks for the informative podcast, I've been listening since I started grad school five years ago and have learned quite a bit thanks to you. I was recently feeling nostalgic and decided to buy an old Win95 laptop off Ebay to play some of the DOS games from my youth. It was great at first, but my excursions into the world of Commander Keen were interrupted a week later when the laptop stopped booting. The first thing I thought of was my copy of Spinrite which had saved my butt back in undergrad once or twice. When I booted it up, however, I was surprised to see a name I didn't recognize at all in the license field. Confusion came over me as I stared at the screen, but then it dawned on me, I must've pirated it. I felt so bad that I couldn't start the scan until I sent a yabba dabba doo your way, but needless to say the old machine was back up and running after my now legitimate copy of SpinRite worked its magic. My sincerest apologies Steve, I would use the excuse of being a poor undergrad who desperately needed his research papers back, but that doesn't change a SpinWrong into a SpinRite.

KeenDreams

(If he has Win95 running... he's GOT to try "ChromaZone" :)

Closing The Loop

Andy Pastuszak

- @SGgrc I really like your idea of capturing and keeping 2FA setup QR codes. But the problem is, I have had 2FA in a few places for years. Is there any way to get those QR codes again?
- Andy, I had the same problem, since I had already established several accounts with Google Auth, which won't export (for which I'm glad for security sake). Fortunately, every service I have encountered so far will allow you to CHANGE your TOTP secret. So I just logged in one last time with the original code, asked the site for a new one, and then printed that new one for all future needs on all devices.

Some early results from our listener's fingerprint tests:

- Paul Dawson
Hi Steve, after listening to SN608 and your article about smartphone fingerprint sensors I decided to put mine to the test. I have an iPhone 6 with IOS 10.3.1. I have taught my iPhone two finger prints (well, both thumbs actually). I have asked 84 people to try and unlock my iPhone with their fingerprint. I am glad to report that not one of them managed to achieve this. Since my iPhone locks out the fingerprint detector after a few failed attempts, I even used my passcode to allow people several attempts at gaining access. From my findings I think I am happy that the fingerprint system is secure enough for me. Best regards Paul Dawson Lincolnshire UK P.S love the show
- Andy Norman
@SGgrc Surely our own prints from other fingers likely closer match than random finger. Have not managed to unlock iPhone with my other fingers
- Terry E Snyder Jr.
I have an iPad Air 2 and secure it with my thumbprint. I discovered to my chagrin that my 3 year old son is also able to unlock my iPad with his thumb!

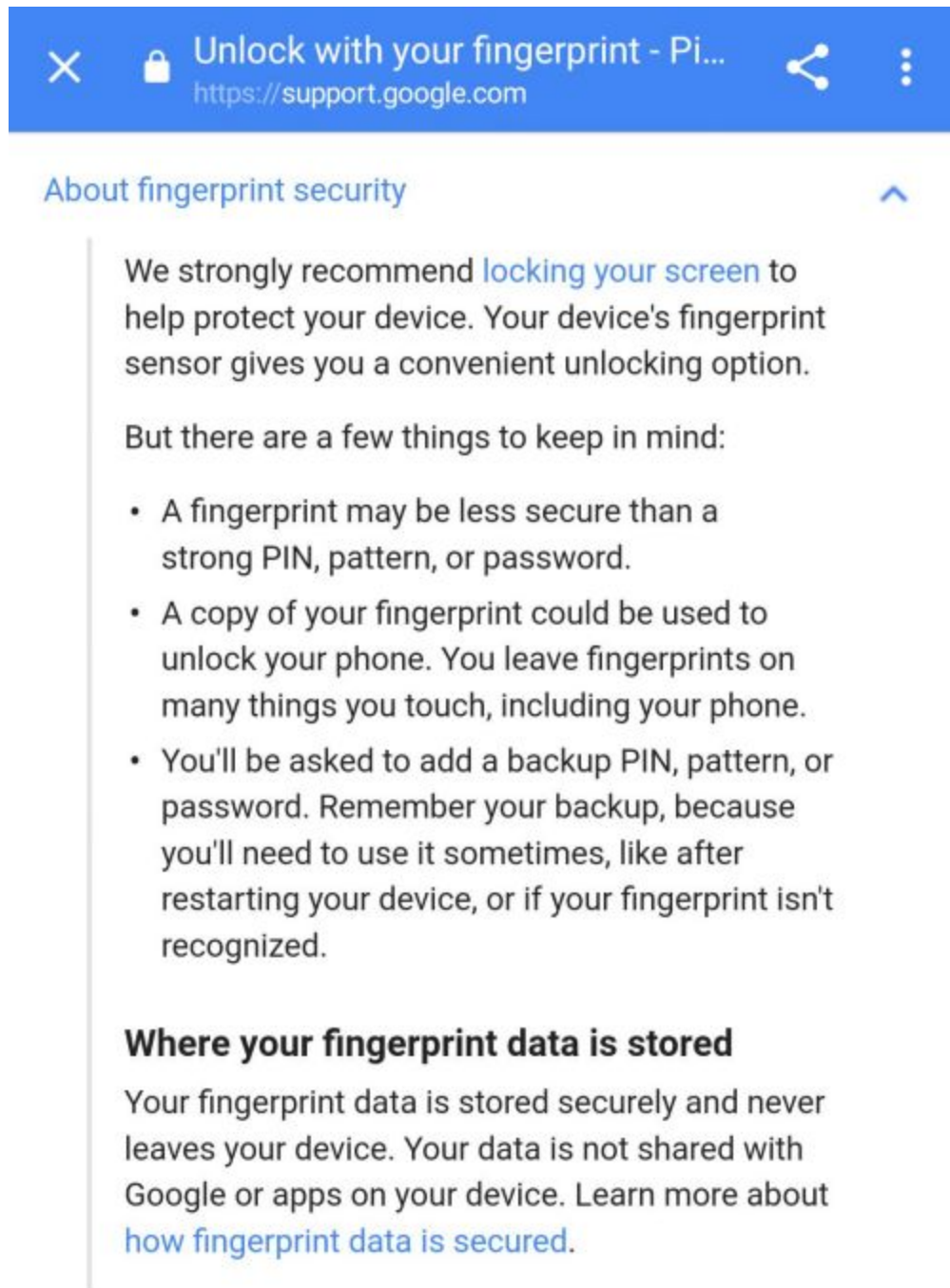
The first time I saw it happen I was using the feature that locks an app to be the only app he is allowed to use. Next thing I knew he was out of the app. I just thought the app crashed. The next thing I knew he was able to unlock my iPad without my fingerprint and I watched him never try to type in my pass key. After hearing the latest Security Now episode it finally all makes sense. Thanks for a great show and long time SpinRite user. Looking forward to its next release and SQRL.

- Phil
Wow after listening to @SGgrc, I let my wife try to unlock my phone with her fingerprint, works about 1 in 10 tries. Scary!

@SGgrc After removing a bunch of saved fingers it stopped working. Wonder what I got in there?

NeoRenfield

- @SGgrc Google says, about the Pixel fingerprint reader, "may be less secure than a strong PIN, pattern, or password"



The screenshot shows a mobile browser interface. At the top is a blue address bar with a close button (X), a lock icon, the text "Unlock with your fingerprint - Pi...", the URL "https://support.google.com", a share icon, and a menu icon (three dots). Below the address bar is the page title "About fingerprint security" with an upward arrow icon. The main content area has a light blue background and contains the following text:

We strongly recommend [locking your screen](#) to help protect your device. Your device's fingerprint sensor gives you a convenient unlocking option.

But there are a few things to keep in mind:

- A fingerprint may be less secure than a strong PIN, pattern, or password.
- A copy of your fingerprint could be used to unlock your phone. You leave fingerprints on many things you touch, including your phone.
- You'll be asked to add a backup PIN, pattern, or password. Remember your backup, because you'll need to use it sometimes, like after restarting your device, or if your fingerprint isn't recognized.

Where your fingerprint data is stored

Your fingerprint data is stored securely and never leaves your device. Your data is not shared with Google or apps on your device. Learn more about [how fingerprint data is secured](#).

BlueLED

- Steve: Highly recommend this page for all uBlock Origin users:
<https://github.com/gorhill/uBlock/wiki/Dynamic-filtering:-quick-guide>

Steven Doyle

- @SGgrc If ISP's were to start requiring certificate installation, would your HTTPS fingerprinting still indicate a man in the middle?

Chris Sullivan

- @SGgrc Experimented w/'puny' Apple site from SN608. Found LastPass did *not* get tricked and would not give my creds to phony site

Thomas Smailus

- How was #punycode ever anything but a bad idea if the DNS system doesn't also support it cleanly?

Martin Badke

- @SGgrc The garage entry keypad COULD have repeated digits. Number of codes possible is 4^4 . Still sad. I've seen similar for cash safes.

P. Hoffman

- @SGgrc Possible mitigation for ISP snooping: OpenVPN server in Amazon EC2. < \$1/day. Easy to change IP addr at will. Thoughts? Thanks