Security Now! #652 - 02-27-18

WebAssembly

This week on Security Now!

This week we discuss Intel's Spectre & Meltdown microcode update, this week in cryptojacking, Tavis strikes again, Georgia on my mind (and not in a good way), news from the iPhone hackers at Cellebrite, Apple to move its Chinese customer data, e-Passports? Not really, Firefox 60 loses a feature, the IRS and cryptocurrencies, Android P enhances Privacy, malicious code signing news, a VERY cool Cloudfront/Troy Hunt hack, a bit of errata, miscellany, and closing the loop feedback from our terrific listeners, and a closer look at WebAssembly.

Security News

Intel Spectre & Meltdown Microcode Update Status

https://newsroom.intel.com/news/latest-intel-security-news-updated-firmware-available/
Intel has now released production microcode updates to their OEM customers and partners for Kabylake and Coffeelake-based platforms, plus additional Skylake-based platforms.
This represents their 6th, 7th and 8th Generation Intel® Core™ product lines as well as their latest Intel® Core™ X-series processor family. It also includes their recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for data center systems.

https://newsroom.intel.com/wp-content/uploads/sites/11/2018/02/microcode-update-guidance.pdf

This Week in CryptoJacking (MalMining?)

Tesla Corporation is the latest victim of cryptoJacking.

RedLock Cloud Security Intelligence (CSI)

Under the title of: "The Cryptojacking Epidemic"
<quote> ..."we are beginning to witness the evolution of crytopjacking as hackers recognize the massive upside of these attacks and begin to explore new variations to evade detection."

In the case of Tesla, the hackers infiltrated Tesla's Kubernetes console which was not password protected.

(Kubernetes is an open source platform originally developed by Google and now being independently maintained and developed by the Cloud Native Computing Foundation. It that automates Linux container operations and eliminates many of the manual processes involved in deploying and scaling containerized applications.)

So, within one of Tesla's unsecured Kubernetes pods, access credentials were exposed to Tesla's AWS environment which contained an Amazon S3 (Amazon Simple Storage Service) bucket that had sensitive data.

And in addition to the data exposure, hackers were performing some rather sophisticated crypto mining -- employing advanced evasion techniques -- from within that Tesla Kubernetes pod:

Unlike other crypto mining incidents, the hackers did not use a well known public "mining pool" in this attack. Instead, they installed mining pool software and configured the malicious script to connect to an "unlisted" or semi-public endpoint. This makes it difficult for standard IP/domain based threat intelligence feeds to detect the malicious activity.

The hackers also hid the true IP address of the mining pool server behind CloudFlare. This allows the hackers to obtain a new IP address on-demand by registering for a free CDN service. This makes IP address based detection of crypto mining activity even more challenging.

The mining software was configured to listen on a non-standard port to elude detection of the

malicious activity based on well-known port number traffic.

And RedLock noted that Tesla's Kubernetes dashboard showed that the instance's CPU usage was not high. So rather than running full-bore and going for broke, they likely configured the mining software to keep the usage low to evade detection.

What this all suggests is that we ARE, in fact, on the verge of moving into a cryptomining, or cryptojacking, epidemic.

Viruses never made money for anyone by themselves... so they were an annoyance.

Then, when the idea of crypto-based ransomware occurred to someone we saw an epidemic explosion of random-based file encryptions.

Today, now that we have real-world currency exchangeable cryptocurrencies, bad guys have the relatively new ability to monetize the theft of idle CPU resources, which was, until now, not obviously useful to anyone other than the SETI project.

We've often noted how porous security actually is. The ability to monetize stolen CPU cycles creates a new and heightened level of "intrusion pressure"... which is predictably going to result in enhanced levels of intrusion.

Google's Tavis Ormandy peers into uTorrent... and we can pretty much predict the rest.
https://260blog.com/technology/bittorrent-client-utorrent-suffers-security-vulnerability-updated/

BitTorrent's uTorrent is the Internet's #1 peer-to-peer file torrent application used by many many millions of active users everyday.
After checking out uTorrent last November, Tavis, on behalf of Google's Project Zero, found some problems and reached out to BitTorrent.

As we know, Google's Project Zero allows developers a 90-day window to address security flaws. But BitTorrent had remained quiet.

Twitter: Tavis Ormandy /Verified account / @taviso
@bramcohen (Creator of BitTorrent. Now doing cryptocurrency stuff) "I don't think bittorrent are going to make a 90 day disclosure deadline, do you have any direct contacts who could help? I'm not convinced they understand the severity or urgency.

BitTorrent's "fix" for the trouble is in the beta channel but not yet a stable release.

And... Tavis is not impressed. He wrote: "Hmm, it looks like BitTorrent just added a second token to uTorrent Web. That does not solve the DNS rebinding issue, it just broke my exploit."

So they appear to have muted a symptom rather then curing the disease... and the disease appears to be significant. The flaw is a well known class of vulnerabilities knows as "DNS

Rebinding" that potentially allows outsiders to remotely execute code on user's machines through uTorrent’s remote control feature.

Here's what we know from Tavis:

By default, utorrent create an HTTP RPC server on port 10000 (uTorrent classic) or 19575 (uTorrent web). There are numerous problems with these RPC servers that can be exploited by any website using XMLHTTPRequest().

To be clear, visiting *any* website is enough to compromise these applications.

uTorrent web (http://web.utorrent.com)
==========

As the name suggests, uTorrent Web uses a web interface and is controlled by a browser as opposed to the desktop application. By default, uTorrent web is configured to startup with Windows, so will always be running and accessible. For authentication, a random token is generated and stored in a configuration file which must be passed as a URL parameter with all requests. When you click the uTorrent tray icon, a browser window is opened with the authentication token populated, it looks like this:

http://127.0.0.1:19575/gui/index.html?localauth=localapic3cfe21229a80938:

While not a particularly strong secret (8 bytes of std::random_device), it at least would make remote attacks non-trivial. Unfortunately however, the authentication secret is stored inside the webroot (wtf!?!?!?!), so you can just fetch the secret and gain complete control of the service.

```
$ curl -si http://localhost:19575/users.conf
HTTP/1.1 200 OK
Date: Wed, 31 Jan 2018 19:46:44 GMT
Last-Modified: Wed, 31 Jan 2018 19:37:50 GMT
Etag: "5a721b0e.92"
Content-Type: text/plain
Content-Length: 92
Connection: close
Accept-Ranges: bytes

localapi29c802274dc61fb4        bc676961df0f684b13adae450a57a91cd3d92c03
94bc897965398c8a07ff    2       1
```

This requires some simple dns rebinding to attack remotely, but once you have the secret you can just change the directory torrents are saved to, and then download any file anywhere writable...

Georgia state moves to criminalize independent computer security research
http://www.legis.ga.gov/legislation/en-US/Display/20172018/SB/315

2017-2018 Regular Session - SB 315
A BILL to be entitled "an Act to amend Part 1 of Article 6 of Chapter 9 of Title 16 of the Official Code of Georgia Annotated" , relating to computer crimes, so as to create the new crime of unauthorized computer access; to provide for penalties; to change provisions relating to venue for computer crimes; to provide for forfeiture; to provide for related matters; to repeal conflicting laws; and for other purposes.

On Feb 12th the bill passed in the Georgia Senate and is now in the Georgia House.

LANGUAGE: "(b.1)

(1) Unauthorized Computer Access. Any person who accesses a computer or computer network with knowledge that such access is without authority shall be guilty of the crime of unauthorized computer access.

(2) This subsection shall not prohibit: (A) A parent or legal guardian of an individual who is under the age of 18 from monitoring computer usage, denying computer usage, or copying data from such individual's computer;

And... "All laws and parts of laws in conflict with this Act are repealed."

There are no exceptions or exemptions for the intent of the "unauthorized access", nor for the responsible disclosure of any vulnerabilities which might be found.

As a consequence, honest researchers risk prosecution for VERIFYING

If we have learned ANYTHING about security it's that saying its secure means absolutely nothing.

As we might imagine, the EFF has blown a gasket over this. And everyone knows how I feel about this. I doubt we've had many of these podcasts in the past year where I have not reiterating that the worst thing that will ever happen is if we criminalize security research.

Cellebrite may now be able to unlock iPhones 5 through X.
Cellebrite, popular with governments and law enforcement for hacking into devices, is telling potential clients that it can unlock iOS 11 devices.
https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#53d2d5ec667a

Thomas Fox-Brewster writing his security column for Forbes:

In what appears to be a major breakthrough for law enforcement, and a possible privacy problem for Apple customers, a major U.S. government contractor claims to have found a way to unlock pretty much every iPhone on the market.

Cellebrite, the Israel-based vendor that's become the U.S. government's company of choice when it comes to unlocking mobile devices, is this month telling customers its engineers currently have the ability to get around the security of devices running iOS 11. That includes the iPhone X, a model that Forbes has learned was successfully raided for data by the Department for Homeland Security back in November 2017, most likely with Cellebrite technology.

The Israeli firm, a subsidiary of Japan's Sun Corporation, hasn't made any major public announcement about its new iOS capabilities. But Forbes was told by sources (who asked to remain anonymous as they weren't authorized to talk on the matter) that in the last few months the company has developed undisclosed techniques to get into iOS 11 and is advertising them to law enforcement and private forensics folk across the globe. Indeed, the company's literature for its Advanced Unlocking and Extraction Services offering now notes the company can break the security of "Apple iOS devices and operating systems, including iPhone, iPad, iPad mini, iPad Pro and iPod touch, running iOS 5 to iOS 11."

Thomas' column goes into much greater detail, citing interesting but hearsay accounts of various models of iPhones being accessed... but without definitive detail... specifically because Cellebrite protects these secrets as much as Apple protects theirs... and in this case with the clear intent to keep their methods secret FROM Apple:

iPhones must be physically sent to Cellebrite for them to work their magic. Even if it could be packaged into remotely usable software, Cellebrite wouldn't do that for fear that Apple would quickly close whatever hole Cellebrite had found.

Apple to move Chinese customer iCloud data -- and its encryption keys -- to China

Like Microsoft for Azure and Office 365 services and Amazon, Apple is complying with a new Chinese law which requires the data for Chinese citizens to reside in China. For all of these companies it's a matter of complying or losing China.

Greater China is Apple’s second-most-important market after the U.S., with $44.76 billion in revenue in its last fiscal year, a fifth of Apple's total revenue for the year.

What has stirred some controversy is that Apple has indicated that it also plans to store the encryption keys for its Chinese users in China... whereas neither Microsoft nor Amazon have said one way or the other.

This raises understandable concerns for privacy advocates who worry that China may become heavy handed once the keys reside within its territory.

A Beijing-based attorney who was asked about the decision said Chinese iPhone users are disappointed by Apple’s changes to iCloud data storage because privacy protection in China is weak. However, he said users there “still consider that iPhone is better than some other pure Chinese-made phones for privacy policy and protection.”

Apple’s cloud partner in China is (Guay'-Cho) "Guizhou on the Cloud Big Data Industry Co.", or Guizhou-Cloud, which is overseen by the government of Guizhou province. Apple plans to shift

operational responsibility for all iCloud data for Chinese customers in China to Guizhou-Cloud by tomorrow, Feb. 28. Customer data will migrate to servers based in China over the course of the next two years. And Apple declined to say when the encryption keys would move to China.

Apple began notifying iCloud users in China last month that Guizhou-Cloud would be responsible for storing their data.

Updated terms and conditions for China users say that Apple and Guizhou-Cloud "will have access to all data" and "the right to share, exchange and disclose all user data, including content, to and between each other under applicable law."

Ronald Deibert, a political-science professor at the University of Toronto's Munk School of Global Affairs who has researched Chinese government hacking operations, said: "Given that Apple's China operations will be managed by a Chinese company, it seems implausible that the government will not have access to Apple data through the local company."

Reporters Without Borders has urged journalists in China to change their geographic region or close their accounts before Feb. 28, saying Chinese authorities could gain a backdoor to user data even if Apple says it won't provide one.

Apple said it has advised Chinese customers that they can opt out of iCloud service to avoid having their data stored in China. Data for China-based users whose settings are configured for another country, or for Hong Kong and Macau, won't go on Chinese servers, and Apple said it won't transfer anyone's data until they accept the new mainland-China terms of service.

Signature verified? Nope!
Introduced and mandated more than a decade ago, in 2007, all newly issued passports must now be e-passports.

Citizens of the 38 countries on the visa waiver list must have an e-passport in order to be admitted to the US.

These E-passports have an electronic chip containing cryptographic information and machine-readable text, making it easy to verify a passport's authenticity and integrity.

The Border staff have long since deployed e-passport readers at most ports of entry since it makes reading and automatically logging the passport data easier, quicker and more efficient.

Now get this: Although all e-passport data have been cryptographically digitally signed from the start, Customs and Border Protection has never had the software necessary to authenticate the information stored on the e-passport chips.

Somehow this fell across the radar of Senators Ron Wyden (D-OR) and Claire McCaskill (D-MO), who wrote to US Customs and Border Protection (CPB) acting commissioner Kevin K. McAleenan for clarification of this rumor.

<quote> "CBP does not have the software necessary to authenticate the information stored on

the e-passport chips. Specifically, CBP cannot verify the digital signatures stored on the e-passport, which means that CBP is unable to determine if the data stored on the smart chips has been tampered with or forged," the letter stated... and the CBP has been aware of this glaring lapse since at least 2010 when the Government Accountability Office (GAO) release a report highlighting the gap in technology.

Firefox losing individual cookie management
https://www.ghacks.net/2018/02/26/mozilla-removes-individual-cookie-management-in-firefox-60/

Martin Brinkmann, writing for Ghacks:

The most recent version of Firefox Nightly, currently at version 60, comes with changes to Firefox's cookie management. Mozilla merged cookie settings with site data in the web browser which impacts how you configure and manage cookie options. If you run Firefox 59 or earlier, you can load about:preferences#privacy to manage privacy related settings in Firefox. If you set the history to "use custom settings for history" or "remember history", you get an option manage cookie settings and to remove individual cookies from Firefox. A click on the link or button opens a new browser window in which all set cookies are listed. You can use it to find set cookies, look up information, remove selected or all cookies. Mozilla engineers changed this in recent versions of Firefox 60 (currently on the Nightly channel).

Nothing's certain besides death and taxes...
Coinbase tells 13,000 users their data will be sent to the IRS soon (Within 21 days)
https://www.theverge.com/2018/2/26/17055264/coinbase-cryptocurrency-tax-irs-compliance-court-order

Coinbase informed about 13,000 customers who had completed transactions totaling more than $20,000 through their accounts in a single year between 2013 and 2015, that it WILL be complying with an IRS court order compelling it to disclose the details of those previous year transactions.

The IRS made the original request back in November 2016, asking for the Coinbase records of all the people who bought bitcoin from 2013 to 2015 to seek out those who were evading cryptocurrency taxes. The Verge reported that anyone affected by the order should now have received an email from Coinbase to that effect.

Coinbase heavily resisted the summons. But ultimately, in November last year, the San Francisco court ruled Coinbase had to turn over identifying records including taxpayer IDs, names, dates of birth, addresses, and transaction records from that period.

In an email and on its website Friday, Coinbase noted that it had: "... fought this summons in court in an effort to protect its customers, and the industry as a whole, from unwarranted intrusions from the government."

It informed its 13,000 affected customers that the "court order requires us to produce

information specific to your account," but that the company could not provide legal or tax advice. And 2018 is shaping up to be the year that tax collectors get serious about bitcoin earnings, meaning that it's a good time to be extra careful about compliance.

Android "P" to block camera and mute Mic for non-foreground apps.
https://thehackernews.com/2018/02/android-p-camera-apps.html

It would be nice of the "P" edition of Android stood for Privacy.

We've talked extensively about app permissions in Android. About apparently overly broad permissions, about permission auditing and management. And about how background applications which are loaded but which you haven't been using for some time can be used to stealthily monitor and spy.

According to the Android Open Source Project (AOSP) commit, Google is working on two built-in features in Android P to protect its users from malicious apps spying on them using their smartphones' camera or microphone.

Spotted by XDA developers, the source code commit for both the camera and microphone changes notes that apps that are "idle" (aka running in the background) "for more than a certain amount of time" without specifying themselves, will not be able to continue using the microphone or camera.

Android P will keep an eye on the app's UID and block it from accessing the camera and microphone in any way whenever that UID is idle. Repeated attempts of requesting access to the camera would generate errors and Android "P" will simply mute the microphone for background apps so that they only hear silence.

Android "P", the next major version of Android, is expected at this year's Google I/O developer conference that will take place from May 8 to May 10 at the Shoreline Amphitheatre in Mountain View, California.

Malicious code signing certificates are no longer stolen -- they are created.
https://www.recordedfuture.com/code-signing-certificates/
Threat intelligence firm "Recorded Future" dug into the underground certificate supply industry and came away with some surprising discoveries:

PDF: "The Use of Counterfeit Code Signing Certificates Is on the Rise"
https://go.recordedfuture.com/hubfs/reports/cta-2018-0222.pdf

Certificates registered in names of real corporations are surprisingly easy to come by.

These modern certificates are no longer being stolen from legitimate organizations... instead, the legitimate credentials of legitimate (and unaware) corporate entities are being used to create new legitimate code signing certificates that the "owning" company is completely unaware of.

The certificates are issued by established companies, such as Comodo, Thawte, and Symantec.

Legitimately signed code is up to twice as likely to pass unnoticed through A/V systems and signing with EV certificates often suppresses SmartScreen OS warnings.

This signing is extremely effective in malware obfuscation.

The earliest instances of stolen code signing certificates were seen in 2011.

But by 2015 -- three years ago -- non-stolen created-to-order code signing certificates became widely available in the criminal underground.

The most affordable version of a code signing certificate costs $299, but the most comprehensive Extended Validation (EV) certificate with a SmartScreen reputation rating is listed for $1,599.

In their full report, Recorded Future wrote: "Contrary to a common belief that the security certificates circulating in the criminal underground are stolen from legitimate owners prior to being used in nefarious campaigns, we confirmed with a high degree of certainty that the certificates are created for a specific buyer per request only and are registered using stolen corporate identities, making traditional network security appliances less effective."

Auto Password Pwning System
John Graham-Cumming @jgrahamc
Beauty of @Cloudflare Workers is that it was easy to integrate @troyhunt's new pwned password service to add a header indicating whether a POSTed password is pwned or not. Then the server can warn the user.

https://gist.github.com/jgrahamc/21f31c8fb4b2c27bda4f605197d5143f
<QUOTE> Cloudflare Workers that adds an "Cf-Password-Pwnd" header to a POST request indicating whether the 'password' field appears in Troy Hunt's database of pwned passwords.

Troy Hunt:
I think this is one of the coolest use cases I've seen for Pwned Passwords yet: it's a @Cloudflare worker (code that runs in their edge nodes) that can automatically check a password on form post (such as login) and add a response header indicating pwnage. That's awesome.

I've Just Launched "Pwned Passwords" V2 With Half a Billion Passwords for Download
https://www.troyhunt.com/ive-just-launched-pwned-passwords-version-2/

Last Thursday -- a long and wonderfully detailed posting.

Google: "Troy Hunt: I've Just Launched "Pwned Passwords" V2"

<quote> In total, there were 3,033,858,815 occurrences of those 501,636,842 unique passwords. In other words, on average, each password appeared 6 times across various data breaches. In some cases, the same password appeared many times in the one incident - often

thousands of times - because that's how many people chose the same damn password!

https://haveibeenpwned.com/

Errata

Very Stable Genius @r3cgm
@SGgrc @leolaporte "Deeee-bold", it's *not* "Dye-bold" (voting machines). As a former employee who has written you several times over the years with this same request, please stop making me cringe every time the name is mispronounced. :) Love the podcasts!

Michael Horowitz / @defensivecomput
Steve, What you said on the last SecNow about DNS servers was not the whole story. Peplink routers can over-ride all DNS requests from devices connected to their routers. In this case you WILL use the DNS servers in the router, *not* those hard coded in your computer. From perspective of router, its easy, just look for outgoing port 53 traffic.

Miscellany

Hardware Offloading and Ubiquity EdgeRouters
https://help.ubnt.com/hc/en-us/articles/115006567467-EdgeRouter-Hardware-Offloading-Explained

SpinRite

At 10:31 AM 2/17/2018, you wrote:
Hello,
My name is David Stidolph. I have been a LONG time user of SpinRite, but I have an immediate need. I need to recover a laptop drive and I cannot find my iso.

Any chance I can download it again? My current email is <REDACTED (gmail)> My previous email was <REDACTED (RoadRunner> (no longer active).

If I cannot download it, please let me know.
Thanks,
David.

Hi David,

Your original receipt with download instructions has just been sent via email! :)

Your transaction code in your emailed receipt is the key to your download. It will allow you to obtain replacement copies as well as edit your own contact email should it need to be changed.

Sincerely,
GRC

Sales Dept.
Wanted to pass on a spinrite story: My first PC was a 4.77 clone with a 5 megabyte MFM hard drive. When it powered up it sounded like a small jet engine. I got a copy of SpinRite (don't recall whether it was 1.0 or 2.0), but I ran it on that machine. Not only did it recover bad sectors, it quieted the drive down quite a bit. Since then I have saved many hard drives over the years. The software rocks!

Best of luck and I hope you guys sell LOTS.
David Stidolph

Closing The Loop

STEFAN KORRIVO @NoThumbBowler
@GibsonResearch I'm not looking forward to the day that many domains are using different cryptomining and my browser with multiple tabs is hindered useless (since each domain will want 90% of my cpu) and degrade my internet experience :(

Anthony @atdatu
@SGgrc Bluehost wanted me to provide the last 4 characters of my password for identification, does that mean they have my plain password? I thought password is hashed in the db?

Stephen Pickering @Pickering
@SGgrc Hey Steve! I'm in the market for a new Mac. But I hate the idea of buying a new computer that has a patch on it's CPU (for Meltdown and Spectre) which from my understanding hampers performance. Is mine a valid reticence? Thanks! You're the best! @leolaporte

pellucid @pellucid
@SGgrc Does authed mine use your browser for mining across web pages, or only when visiting a particular web page it is hosted on?

Nick Stoler @NickStoler
@SGgrc Re: Javascript mining, wouldn't WebGL allow pretty efficient mining without building it into the browser?

Michael @Krabby127
@SGgrc On #SecurityNow you keep mentioning how browser based mining are currently terrible because JS is inefficient. What about WebGL? That leverages the GPU directly.
Love the show.

Sebastien Boisvert / @CoderSeb
@SGgrc Would WebAssembly make web crypto mining more practical?

Andreas Göb @a_goeb
@SGgrc Second week in a row you talk about JavaScript being way to inefficient for crypto mining. What about e.g., web assembly? webassembly.org

WebAssembly

WebAssembly (wasm, WA) is a web standard that defines a binary format and a corresponding assembly-like text format for executable code in Web pages.

It is an attempt enable executing code nearly as fast as running native machine code. It was envisioned to complement JavaScript to speed up performance-critical parts of web applications and later on to enable web development in other languages than JavaScript.

Its main benefit is that it can load a go MUCH faster than JavaScript… but it's still an interpreted language since it's code written for a virtual stack-based machine.

It was developed at the World Wide Web Consortium (W3C) with engineers from Mozilla, Microsoft, Google and Apple.

It is executed in a sandbox in the web browser after a formal verification step. Programs can be compiled from high-level languages into wasm modules and loaded as libraries from within JavaScript applets.

WebAssembly is a portable stack machine which is designed to be faster to parse than JavaScript, as well as faster to execute, and to enable very compact code representation.