Security Now! #648 - 01-30-17

Post Spectre?

This week on Security Now!

This week we discuss continuing Spectre updates, how not to treat Tavis Ormandy, a popular dating app where you'd really hope for HTTPS but be surprised to find it missing, the unintended consequences of global posting of fitness tracking data, gearing up (or not) for this year's voting machine hack'fest, another record broken by a cryptocurrency exchange heist, bad ads and fake ads, the unclear fate of the BSD operating systems, a caution about Dark Caracal's CrossRAT Trojan, another way to skin the Net Neutrality cat, a bit of errata and miscellany, one of the best SpinRite testimonials in a long time, and some closing the loop feedback from our terrific listeners.

Our Picture of the Week

Security News

InSpectre is now at release #6

- There was a bug in Microsoft's 32-bit implementation if the NTDLL.DLL in Win10/1703.
- The "sense" of YES and NO! have been reversed to reduce "at first glance" confusion.
- ~355,000 downloads.

Microsoft issues a back-out patch for Intel's microcode mess:
https://support.microsoft.com/en-us/help/4078130/update-to-disable-mitigation-against-spectre-variant-2

Update to disable mitigation against Spectre, Variant 2

Summary

Intel has reported issues with recently released microcode meant to address Spectre variant 2 (CVE 2017-5715 Branch Target Injection) – specifically Intel noted that this microcode can cause "higher than expected reboots and other unpredictable system behavior" and then noted that situations like this may result in "data loss or corruption." Our own experience is that system instability can in some circumstances cause data loss or corruption. On January 22, Intel recommended that customers stop deploying the current microcode version on affected processors while they perform additional testing on the updated solution. We understand that Intel is continuing to investigate the potential effect of the current microcode version, and we encourage customers to review their guidance on an ongoing basis to inform their decisions.

While Intel tests, updates and deploys new microcode, we are making available an out-of-band update today, KB4078130, that specifically disables only the mitigation against CVE-2017-5715 – "Branch target injection vulnerability." In our testing, this update has been found to prevent the described behavior. For the full list of affected devices, see Intel's microcode revision guidance. This update covers Windows 7 (SP1), Windows 8.1, and all versions of Windows 10, for client and server. If you are running an affected device, this update can be applied by downloading it from the Microsoft Update Catalog website. Application of this payload specifically disables only the mitigation against CVE-2017-5715 – "Branch target injection vulnerability."

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4078130

Microsoft's advisory also provides registry guidance, which is exactly what GRC's InSpectre also does.

How not to treat Tavis Ormandy
"Hackers could have exploited flaw in all Blizzard games"
https://www.csoonline.com/article/3250627/security/hackers-could-have-exploited-flaw-in-all-blizzard-games.html

Tavis Ormandy has decided to turn his security gaze onto the major online gaming with more than 100 million users.

His first venture informed Blizzard of a significant vulnerability and provided proof of concept code.

This was a glaring vulnerability which allowed any website to abuse the weak authentication built into the common update management system of all of Blizzard's games (World of Warcraft, Overwatch, Diablo III, Starcraft II, etc.) to download, install and run arbitrary malware on any gamer's machine.

Blizzard initially replied, then gave Tavis the cold shoulder and cutoff communications.

They then produced a flawed solution. Tavis explained that this wasn't going to be a robust solution and expressed his displeasure at the way he was treated.

Blizzard has since reopened communications and indicated that a better fix is in the works.

What happened??

HTTPS Everywhere? Well... not yet:
Hackers can see your Tinder photos and figure out your matches
https://www.theverge.com/2018/1/23/16923504/tinder-unencrypted-hackers-swiping-https-protocol

Researchers from the Tel Aviv-based firm Checkmarx found that Tinder’s iOS and Android mobile apps still lack basic HTTPS encryption, meaning that anyone sharing the same Wi-Fi as you can see your Tinder photos or add their own into the photostream.

In other words, Tinder is not using encryption to keep photos safe from strangers who share the same coffee shop Wi-Fi.

To demonstrate this, Checkmarx built a proof-of-concept app called TinderDrift, which is demo'ed on YouTube, that can reconstruct a user’s session on Tinder if that person is sharing the same Wi-Fi.

Although swipes and matches on Tinder are HTTPS-encrypted, Checkmarx explained -- and proved -- that hackers sharing the same network can disambiguate encrypted commands due to the specific patterns of bytes that represent a left swipe, a right swipe, a Super Like, and a match.

The researchers explained that by combining the intercepted photos with the monitoring of the encrypted commands, hackers could figure out what a Tinder user is seeing and doing.

Tinder responded in a statement to The Verge that the unencrypted photos are profile pictures, and Tinder is a free global platform, so the pictures are "available to anyone swiping on the app" anyway.

Of course, what isn't "free and global" are individual Tinder users' choices and reactions to those unencrypted photos which, this research demonstrates, was poorly concealed.

U.S. soldiers are revealing sensitive and dangerous information by jogging
https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html

The unintended consequences of globally-connected fitness tracking devices... work by military personnel.

Voting-machine makers are telling eBay sellers that selling the machines is illegal!
Why? Because the voting-machine makers are already worried about Defcon!
https://www.engadget.com/2018/01/26/voting-machine-makers-are-already-worried-about-defcon/

All that fun we had last year, with the news of the results of Defcon's Voting Village, which revealed the horrifically poor security of US voting machines ... was not being had by all.

The manufacturers were (and are) not happy, and they have been actively threatening sellers of used and retired machines with (illegal) legal action if their machines are resold. The problem is... reselling the machines -- and hacking them -- is not illegal.

Recall that there were machines which all had the same hardcoded password, some lacking any security, some which could be penetrated without physical contact over WiFi. Many whose software was riddled with well-known vulnerabilities and which had not been patched or updated for a decade. Most machines had never been wiped after being decommissioned and one machine still have the voter registration database for 600,000 citizens.

It was an embarrassing catastrophe for the voting machine companies.

Now, in preparation for this years's event, the Voting Village organizers have indicated that they're having a tough time getting their hands on machines for Defcon's white-hat hackers to test and poke at this coming August. Apparently because the voting-machine makers are scrambling to get the machines off eBay and keep them out of the hands of the "good guy" hackers.

Village co-organizer Harri Hursti told attendees at the Shmoocon hacking conference this month they were having a hard time preparing for this year's show, in part because voting machine

manufacturers sent threatening letters to eBay resellers. The intimidating missives told auctioneers that selling the machines is illegal -- which is false.

Someone Stole Almost Half a BILLION Dollars from Japanese Cryptocurrency Exchange
https://thehackernews.com/2018/01/coincheck-cryptocurrency-heist.html
Coincheck, a Tokyo-based cryptocurrency exchange, has suffered what appears to be the biggest hack in the history of cryptocurrencies, losing $532 million in digital assets (nearly $420 million in NEM tokens and $112 in Ripples).

We all recall when, four years ago in 2014, Mt Gox, which was one of the largest bitcoin exchanges at that time, filed for bankruptcy after admitting it had lost $450 million worth of Bitcoins.

In a blog post, the Tokyo-based cryptocurrency exchange confirmed the cyber heist without explaining how the tokens were stolen, and abruptly froze most of its services, including deposits, withdrawals and trade of almost all cryptocurrencies, except Bitcoin.

And Bitcoin took a 5% hit in its market valuation.

Crooks Created 28 Fake Ad Agencies to Disguise Massive Malvertising Campaign
https://www.bleepingcomputer.com/news/security/crooks-created-28-fake-ad-agencies-to-disguise-massive-malvertising-campaign/

And advertising security company "Confiant" discovered the existence of a large and malicious advertising operation. The advertisements purchased by this group reached 62% of ad-monetized websites on a weekly basis.

Confiant believes that about 2.5 million users who've encountered Zirconium's malicious ads were redirected to a malicious site, with 95% of the victims being based in the US.

This group of cyber-criminals created 28 fake ad agencies, purchasing over 1 billion ad views in 2017, which they used to deliver malicious ads that redirected unsuspecting users to tech support scams or sneaky pages peddling malware-laden software updates or software installers.

Codenamed "Zirconium", the entire operation appears to have started in February 2017, when the group started creating the fake ad agencies which later bought ad views from larger ad platforms.

These fake ad agencies each had individual websites and even LinkedIn profiles for their fake CEOs... and their sole purpose was to interface with larger advertising platforms (Google, Facebook, etc.), appearing as legitimate businesses.

The fake ad agencies would buy ads displayed on legitimate sites via these ad platforms.

The ads would allow the Zirconium group to run JavaScript code that executed a "forced redirect," to hijack visitors browsers off the original site to an intermediary domain.

This intermediary domain would fingerprint and classify incoming traffic, then redirect the user to another domain operated by Zirconium. The crooks would use this third domain as an affiliate traffic jump-off point, allowing others to buy the traffic they hijacked from legitimate sites.

In many cases, users were redirected to pages offering fake (malware-laced) Flash updates, websites offering (malware-infested) software installers, tech support scams, or other scareware pages.

YouTube got hit with Coinhive, CPU-draining cryptocurrency mining advertising.
https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/

YouTube was recently found to be displaying coinhive-laced, cryptocurrency-mining ads.

Visitors' A/V was firing off warning of the events and CPUs were being pinned.

Trend Micro said that the ads drove a more than three-fold spike in Web miner detections during that period. They said the attackers behind the ads were using Google's DoubleClick ad platform to display them to YouTube visitors in select countries, including Japan, France, Taiwan, Italy, and Spain.

A Google representative, asked about this incident replied: "Mining cryptocurrency through ads is a relatively new form of abuse that violates our policies and one that we've been monitoring actively. We enforce our policies through a multi-layered detection system across our platforms which we update as new threats emerge. In this case, the ads were blocked in less than two hours and the malicious actors were quickly removed from our platforms.

ArsTechnica observed that "It wasn't clear what the representative meant when saying the ads were blocked in less than two hours. Evidence supplied by Trend Micro and on social media showed various ads containing substantially the same JavaScript ran for as long as a week. The representative didn't respond to follow-up questions seeking a timeline of when the abusive ads started and ended."

Are the BSDs dying? Some security researchers think so
https://www.csoonline.com/article/3250653/open-source-tools/is-the-bsd-os-dying-some-security-researchers-think-so.html

Too few eyeballs on code is a security issue as vulnerabilities go unreported and unpatched. Can FreeBSD, OpenBSD, and NetBSD survive?

OpenBSD - the tightest security due to its security focus.
FreeBSD - the most advanced and feature rich, through at some cost in security.
NetBSD - the worst security due its focus upon having the widest "run on anything" device and hardware support.

Are the BSD's dying? Linux has far more in number and active developers. Ultimately, the open source ecosystem may not need or be able to support more than a single solution.... and Linux would be the hands down winner in that case.

The CrossRAT JAVA-based malware developed as part of the Dark Caracal project is nearly undetected
https://thehackernews.com/2018/01/crossrat-malware.html
"Beware! Undetectable CrossRAT malware targets Windows, MacOS, and Linux systems"

Only 2 if 58 A/V scanners currently detect Dark Caracal's "CrossRAT" Trojan as malicious.

There is a well known domain for its C&C server -- but that could be easily changed.

Since CrossRAT requires the entire Java runtime, the best protection would be not having JAVA available, or removing it and not installing it. Only that would stop id dead in its tracks.

This may not be possible for some users who rely upon JAVA, but the majority of users do not need JAVA.

Defying the FCC, New York’s governor has signed an executive order on net neutrality
https://www.washingtonpost.com/news/the-switch/wp/2018/01/24/defying-the-fcc-new-yorks-governor-has-signed-an-executive-order-on-net-neutrality/

First the governor of Montana and then two days later New York's governor signed executive orders to limit their respective states purchases of bandwidth to only those providers who abide by the principals of Net Neutrality.

So, in other words, any broadband provider who is found to be throttling or otherwise interfering with any content provider's delivery of content over their bandwidth will be disqualified as providers for those states' government's use of Internet connectivity.

The New York state government -- every facility in the state -- is a massive purchaser of Internet services. So this represents a serious consideration for any provider who might otherwise have been planning to eventually make anti-Neutrality moves.

Errata

Ryan Dey @RyanDey
I didn't appreciate the flippant nature of your coverage of Intel's Spectre mitigation work. Speculative Execution has been a business-as-usual feature for a long time, and there are a lot of people working very very hard to re-engineer the microcode and change everything on a dime. Your disrespectful remarks on their less-than-perfect first efforts doesn't help anything, and likely insults many young coders who view you as a role model.

Miscellany - Binge Time:

Netflix: "Altered Carbon"
Ten episodes release this Friday the 2nd.

SpinRite

Subject: SpinRite is great!
Hi Steve, if that is your real name,

I purchased a copy of SpinRite about a hundred years ago, you know, when the dinosaurs ruled the Earth, and, I am a amazed at how many times SpinRite has saved the day.

I am a Hacker/Penetration Tester/Software Engineer/Super Genius who enjoys torturing hard drives on the weekends. I really enjoy doing things like playing around with Linux kernel code, and, since I am a Super Genius, I can feel free to ignore any and all warnings on the various forums. However, every once in a while I will be exploring the frontiers of ignorance and write some code that seems to completely destroy the hard drive itself. I will make one innocent change to the kernel code, reboot the PC, and, all of a sudden I hear the PC beeping for mercy, see smoke shooting out of the back of the PC, and see a tear in the space-time continuum forming in the middle of my living room. I check to see what the problem is, and, sure enough my PC can no longer read the hard drive.

That's OK though. Since I am a level 14 Hacker Elf, probably, and a Super Genius, I know that I can easily fix the problem. I reach into my satchel and pull out my Magic SpinRite disk, pop it into the CD drive, and, wait while SpinRite does some stuff that is probably very technical. I walk away, praying to the computer gods that they may forgive me, and most of all, hope that SpinRite can fix the problem.... yet again.

I have done these terrible things to poor defenseless hard drives many, many, many times, and, every time SpinRite manages to fix the problem. The best part is I can happily continue to torture poor defenseless hard drives on the weekends without fear of completely destroying them because I know that SpinRite can apparently fix anything.

While it might be true that hyperbole is my best friend, the underlying theme of this testimony is true.

Steve, thank you for using your powers for good and not evil, and... SpinRite works pretty well too! / Clete Boyce

Closing The Loop

Neil Gardner @papaneilg
@SGgrc Thank you for Security Now! Learn a lot each week! How does one stop a Win10 machine from updating to Creator Ed?

@SGgrc Will Inspectre work on Mac's if run in a Windows VM?

Battery Management:

> **Richard Bailey @rmjbailey**
> @SGgrc about battery health; the AccuBattery app recommends only charging your phone to 80% to also preserve its longevity. It gives me a tone when it gets to the % I set and I have to disconnect it from the charger.
>
> **Opher Banarie @cubeERT**
> @SGgrc re: Babying batteries - What about overcharging?
> I've been unplugging the device within 10 seconds of 100%.
> Is this no longer necessary?

Peter Kirby @peter_kirby
@SGgrc I was showing someone pic of the week from #647 and it occurred to me: if the backend knows you're only one char off, then they aren't hashing the password like they should or they wouldn't know that.