Security Now! #650 - 02-13-18

CryptoCurrency Antics

This week on Security Now!

This week we discuss today's preempted 2nd Tuesday of the month, slow progress on the Intel Spectre firmware update front, a worse-than-originally-thought Cisco firewall appliance vulnerability, the unsuspected threat of hovering hacking drones, hacking at the Winter Olympics, Kaspersky's continuing unhappiness, the historic leak of Apple's iOS boot source code, a critical WiFi update for some Lenovo laptop users, a glitch at Wordpress, a but of miscellany -- including a passwords rap -- some closing the loop feedback from our listeners... and then a look at a handful of CryptoCurrency Antics.

Security News

2nd Tuesday Day... once again!
It appears that our February security update was delivered LAST Tuesday on 2/6/2018.
Today we did receive an update for the Adobe Flash Player 0-day we discussed last week.

February 7th, 2018: Security Issue Update: Progress Continues on Firmware Updates
https://newsroom.intel.com/news/security-issue-update-progress-continues-firmware-updates/

Navin Shenoy: "Intel continues to work closely with industry partners to protect customers against the security exploits disclosed by Google Project Zero. As I shared January 22, we identified the root cause of the reboot issue affecting the initial Broadwell and Haswell microcode updates. Since then, we've been focused on developing and validating updated microcode solutions for those and other impacted platforms.

Earlier this week, we released production microcode updates for several Skylake-based platforms to our OEM customers and industry partners, and we expect to do the same for more platforms in the coming days. We also continue to release beta microcode updates so that customers and partners have the opportunity to conduct extensive testing before we move them into production."

Intel has released Spectre microcode update for Skylake (only)
https://arstechnica.com/gadgets/2018/02/intel-releases-new-spectre-microcode-update-for-skylake-other-chips-remain-in-beta/?comments=1&post=34771297

Intel's first microcode update attempted to add instruction set features to give operating systems control over branch prediction for Broadwell, Haswell, Skylake, Kaby Lake, and Coffee Lake processors. But after the initial reports of "more frequent reboots" on Broadwell and Haswell systems, it was later determined that Skylake, Kaby Lake, and Coffee Lake systems were rebooting, too.

The newest microcode update only applies to Skylake mobile and mainstream desktop chips, so if it passes testing -- which will doubtless be more rigorous this round -- owners of systems containing laptop and desktop Skylake chips may see firmware updates being made available before long. But the updates for other chips appears to be in the future.

Comments indicate that Windows also contains at-boot firmware patching capability.

> <quote>
> Windows has the ability to warm patch microcode on boot using the mcupdate_GenuineIntel.dll and mcupdate_AuthenticAMD.dll drivers (located at C:\Windows\System32) on boot, for Intel and AMD cpu's respectively.
>
> If those drivers - which are more accurately simple blocks of microcode and cpu identifying information - contain newer microcode for the current cpu during boot, then

> Windows loads the microcode from these drivers instead, overwriting the microcode that is included with the firmware. This happens before any actual Windows initialisation, so there are no "partial exposure" issues whereby early processes have access to old microcode and later ones don't; all processes for the operating system past the bootstrap launch after the microcode is replaced.
>
> These changes are of course lost on reboot, so the "system" remains on an older microcode version, but when running Windows the newer microcode is the only one in use.

Win10 does, indeed, have both files and this appears to be 100% credible.

Cisco's "Adaptive Security Appliance" vulnerability got a lot worse -- and is now being exploited.
A couple of weeks ago Cisco released the news of a "10 out of 10" super-critical vulnerability in a large family of Internet-facing enterprise class firewall appliances collectively known as the "ASA" or "Adaptive Security Appliance."

Earlier, Cedric Halbronn from the NCC Group had responsibly disclosed the discovery which Cisco quickly moved to patch.

IT was initially believed that only the VPN component of the ASA devices was vulnerable. But then that became a list of 11 subsystem components and the list of affected equipment grew.

CVE-2018-0101 has received a CVSS severity score of 10 out of 10, meaning it's easy to exploit (reduced attack code complexity), can be exploited remotely, and requires no authentication on the device.

This is not consumer equipment, so it won't directly affect our listeners. But if you are within an enterprise and have any connection to Internet-facing Cisco gear, you'll want to make sure to be patched ... because it only took hackers five days to begin exploiting this bug in the wild against Cisco ASA devices.

Hovering computers will make it increasingly possible to hack equipment that doesn’t connect directly to the internet.
https://www.technologyreview.com/the-download/610196/cyber-warfare-is-taking-to-the-skies-aboard-drones

Cyberwarfare is taking to the skies, aboard drones

Hackers are working on radio relay drones which are able to get into unsuspected places to pickup, record or relay wireless signals from equipment which is believed to be safe due to its physical location.

This is obviously very poor security practice and is "insecurity by design." But we see example after example where expediency is the root cause of downstream trouble. So just plant the seed

that lack of proximity to radio is not any true security.

The Winter Olympics are underway and so is Olympic hacking.
Winter Olympics' Security on Alert, but Hackers Have a Head Start
https://mobile.nytimes.com/2018/02/08/technology/winter-olympics-hackers.html?sf181666538=1

Tensions are expected to be lower with improved diplomatic relations with North Korea, but Russia's hacking efforts are running full bore after Russian athletes were banned from participation.

Everyone is at full alert as attacks have been underway for the months leading up to the events as systems have been continuously probed for weaknesses and data has been exfiltrated en mass despite the best efforts of multi-national cybersecurity teams.

Yesterday, Kaspersky Lab filed another lawsuit against the US.
The suit is related to a ban against the use of its products, which was part of the 2018 National Defense Authorization Act which the Trump administration signed into law last October 1st.

In court documents filed yesterday in U.S. District Court for the District of Columbia, the Russian company is claiming that the ban is unconstitutional. Kaspersky's lawyers say that under the Constitution's Bill of Attainder Clause, Congress is forbidden "from enacting laws which impose individualized deprivations of life, liberty, and property and inflict punishment on individuals and corporations without a judicial trial."

The company wrote that: "Kaspersky Lab believes that these provisions violate the U.S. Constitution by specifically and unfairly singling out the company for legislative punishment, based on vague and unsubstantiated allegations without any basis in fact. No evidence has been presented of any wrongdoing by the company, or of any misuse of its products. We continue to offer our full cooperation to government agencies and others with cybersecurity concerns collaboratively and openly through our Global Transparency Initiative."

The truth is... it's far too easy to conceal misbehavior in contemporary systems.

Windows 10 systems no longer have any choice about accepting updates. Microsoft literally has a institutionalized software implantation system in place today. Microsoft can install any software they wish -- on the fly -- into anyone's machine that they wish.

How ANY country with an adversarial relationship to the US could be running Windows has always been a mystery to me. So the same really does apply to Kaspersky Lab.

Two years ago an Apple intern leaked the iOS "iBoot" source code...
...and a bunch of additional internal Apple tools to a select few close and highly trusted friends in the iPhone jailbreaking community.

This is a classic and perfect case study in how nearly all internal secret corporate data leaks: It's not through a flaw in a highly academically scrutinized cryptographic cipher... it's because someone rightly or wrongly entrusted with the secret cannot resist sharing what he or she is privy to.

So what happened?

https://motherboard.vice.com/en_us/article/xw5yd7/how-iphone-iboot-source-code-leaked-on-github

On Wednesday, an anonymous person published the proprietary source code of a core and fundamental component of the iPhone's operating system. A user named "ZioShiba" posted the closed source code for iBoot—the part of iOS responsible for ensuring a trusted boot of the operating system—to GitHub, the internet's largest repository of open source code.

Jonathan Levin, an iPhone researcher, called it the "biggest leak" in the history of the iPhone. The iBoot code is for iOS 9 and the code is two-years old. But even today, it could help iOS security researchers and the jailbreak community find new bugs and vulnerabilities in a key part of the iPhone's locked-down ecosystem.

Apple confirms iOS source code leak, but downplays it as old and outdated
It's still bad enough to set off a round of DMCA takedowns.
https://www.macworld.com/article/3254231/ios/ios-source-code-leak-github.html

Crucial iPhone source code posted in unprecedented leak (updated)
Apple took it down via a DMCA, but the iBoot code is now in the wild.
https://www.engadget.com/2018/02/08/crucial-iphone-source-code-posted-in-unprecedented-leak/

APPLE: In a statement, Apple said, "Old source code from three years ago appears to have been leaked, but by design the security of our products doesn't depend on the secrecy of our source code. There are many layers of hardware and software protections built into our products, and we always encourage customers to update to the newest software releases to benefit from the latest protections."

Apple used the DMCA to force Github to take the code down... but not before it had well and completely escaped into the wild. It's out there now and it will now live quietly forever, being passed around as a badge of insider status.

Lenovo Warns Critical WiFi Vulnerability Impacts Dozens of ThinkPad Models
https://threatpost.com/lenovo-warns-critical-wifi-vulnerability-impacts-dozens-of-thinkpad-models/129860/

The critical vulnerability affecting Broadcom chipsets used in Apple iPhones, Apple TV and Android devices was patched in all of those mobile devices by Apple and Google last September.

However, it turns out that Lenovo ThinkPads using Broadcom's BCM4356 Wireless LAN Driver for Windows 10 are also vulnerable and at risk.

The vulnerability is rated 10 out of 10 because it is remote, requires no user interaction, and can potentially be used to perform remote code execution attacks... but it DOES require radio-reception range proximity. So it's not "remote" as in North Koreans can get you. If it were to happen it would be a local targeted attack... or a drone flying past! <g>

Lenovo is recommending affected ThinkPad customers update their Wi-Fi driver versions. Affected ThinkPad SKUs are: ThinkPad 10, L460, P50s, T460, T460p, T460s, T560, X260 and ThinkPad Yoga 260.

WordPress Update Breaks Automatic Update Feature—Apply Manual Update
https://thehackernews.com/2018/02/wordpress-update.html

WordPress version 4.9.3 was released last week with patches for a total 34 vulnerabilities, but unfortunately, the new version broke its own automatic update mechanism for all future updates. Whoops!

WordPress discovered the bug within a few hours of the v4.9.3 release and quickly fixed it with the maintenance update v4.9.4. But WordPress admins whose systems had grabbed v4.9.3 during that window will need to install v4.9.4 manually.

The trouble was caused by a PHP dependency which broke the auto updating system. WordPress lead developer Dion Hulse explained:

"#43103-core aimed to reduce the number of API calls which get made when the auto-update cron task is run. Unfortunately, due to human error, the final commit didn't have the intended effect and instead triggers a fatal error as not all of the dependencies of find_core_auto_update() are met. For whatever reason, the fatal error was not discovered before 4.9.3's release—it was a few hours after release when discovered."

Thus, WordPress administrators are being urged to update to the latest WordPress release manually to make sure they'll be protected against future vulnerabilities.

To manually update WordPress installations, admin users can sign into their WordPress website and visit Dashboard / Updates and then click "Update Now."

After the update, make sure that your core WordPress version is 4.9.4.

Miscellany

Simon Zerafa (@SimonZerafa)
Murphy's Law as applied to software design and programming:

Bruce Dawson (@BruceDawson0xB)
"Any mistake that is not explicitly prevented will be made. Any error that can occur, will."

Mo' Passwords
https://www.facebook.com/CollegeHumor/videos/10155483807197807/

SpinRite meets Altered Carbon:

qqq1 (@qqq1)
Dear Steve, I have a question regarding SpinRite. I have come across an old stack of my great-great-great-great (possibly more) grandmother. When trying to spin her up in VR she loads for a very long time but eventually fails. There is also no luck when putting her in a new sleeve. What level would you recommend running SpinRite at to try and recover a failing stack? Thanks for everything, Mitch.

Closing The Loop

Tom Terrific Krauska (@tomterrific1947)
@SGgrc If I change my local computer's DNS to 9.9.9.9 and my router has a different DNS lookup address which has precedence?

SKYNET (@fairlane32)
@SGgrc Does Inspectre run in Boot camp? Can it see the chip? Or should I run it in WINE on the Mac side?

David Lemire (@dlemire60)
I've got a suggestion, @SGgrc, for a unified name: Spectre + Meltdown + the endless stream of news about them = SPECDROWN.

Kyle @craigconsulting
#Smectre With regard to coming up with a convenient combined name for the Spectre and Meldown vulnerabilities. I propose Smectre! Since meldown is of a lesser concern and nobody likes them. Haha @SGgrc @leolaporte #Meltdown #Spectre

Joe McDaniel (@joem5636)
.@SGgrc SMELTER?

Kevin Metcalf (@profmetcalf)
@SGgrc Suggested name for the combined threats of Spectre and Meltdown - Smeltre.

Marko Simo (@m_simo)
@SGgrc Spectre and Meltdown are combined as ‘S&M’ ??

CryptoCurrency Antics

In another worrisome way to get CryptoCurrency Mining into unwitting browsers...
We've seen advertising malware attempting to mine Monero, but now...
UK ICO, USCourts.gov... Thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned
https://scotthelme.co.uk/protect-site-from-cryptojacking-csp-sri/

Over this past week approximately 4,300 websites, many high profile such as cuny.edu, USCourts.gov, cookcountytreasurer.gov, were using their visitors' computers to mine Monero cryptocurrency.

What happened? The web server which serves the "Browse Aloud" web screen reader service was penetrated. The "BrowseAloud" (ba.js) JavaScript was altered to include a document write call which added an invocation of the CoinHive Monero cryptocurrency miner into any page which was offering BrowseAloud assistive technologies.

Since this sort of assistive technology is often required of public governmental institutions, many government site were, in turn, compromised.

List of sites known to be invoking BrowseAloud:
https://publicwww.com/websites/browsealoud.com%2Fplus%2Fscripts%2Fba.js/

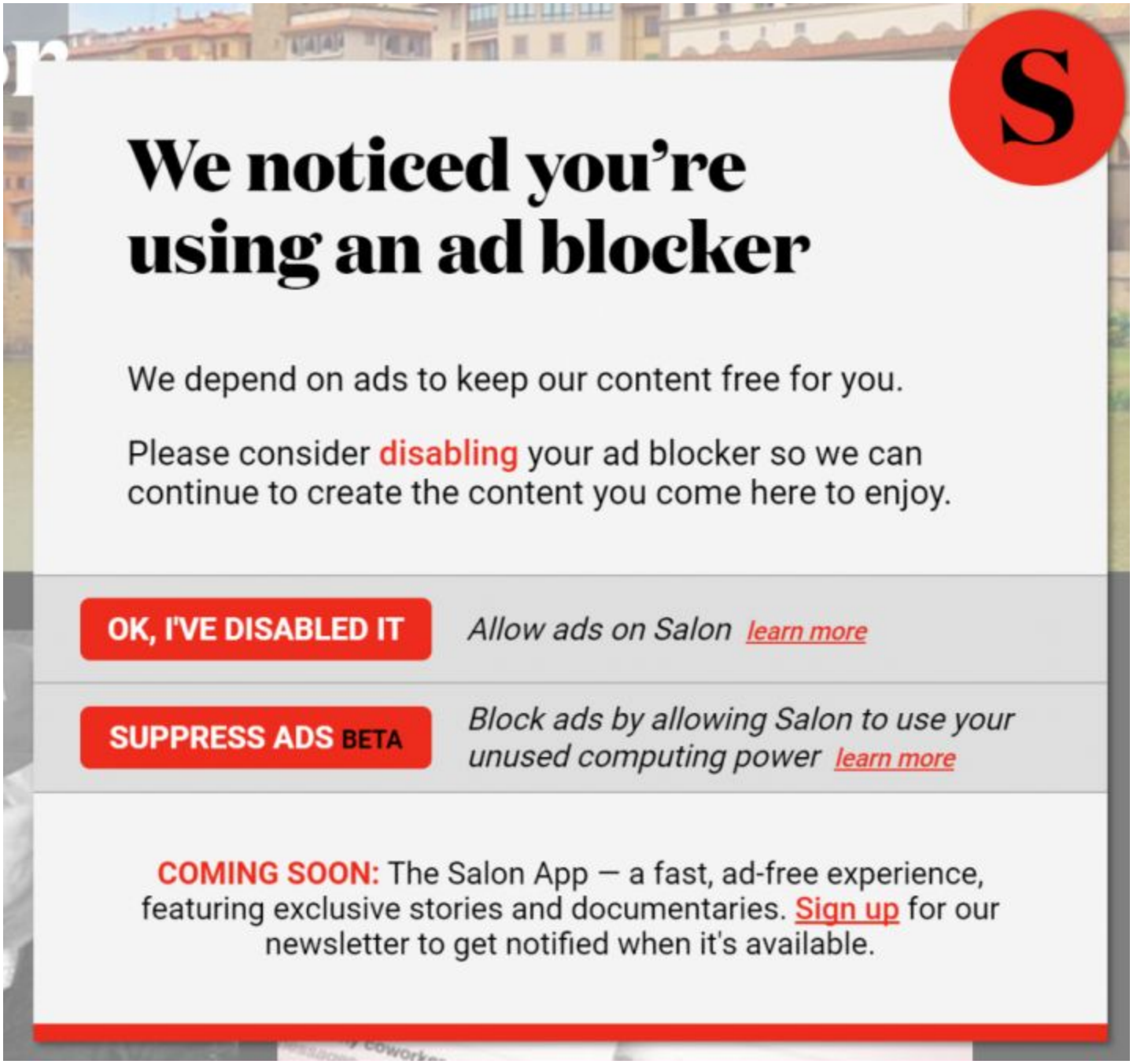
Importing 3rd-party scripting libraries is inherently dangerous.

Browsers have dealt with this danger by enforcing containment -- using the Same Origin Policy to isolate scripts, to limit what a script can do and what it can touch. But here's a nifty example of a script whose purpose was not to breach that containment. It was quite happy to purr along within its own container... because it was soaking up its hosting machine's spare CPU cycles for ultra-low-yield cryptocurrency mining.

Salon.com is offering visitors with Ad Blockers the options of mining Monero
Salon's website explained of the use of Ad blockers: “Recently, with the increasing popularity of ad-blocking technology, there is even more of a disintegration of this already-tenuous relationship; like most media sites, ad-blockers cut deeply into our revenue and create a more one-sided relationship between reader and publisher.”

Salon says about 25 percent of its audience blocks ads.

Now, When a person visits Salon with an ad blocker, a pop up appears asking the person to either remove the ad blocker or allow cryptocurrency mining to occur. A third paid app option is listed as coming soon. If you click “learn more” to find out about the cryptocurrency mining, your computer immediately begins working for Salon before anyone can knowledgeably opt-in.



Cryptocurrency Worth $170 Million Missing From Italian Exchange
BitGrail says it lost about 17 million tokens of Nano
https://www.wsj.com/articles/cryptocurrency-worth-170-million-missing-from-italian-exchange-1518241679

The currency exchange is now insolvent.

Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network
https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html

MAHWAH, New Jersey, Feb. 8, 2018 /PRNewswire/ -- Radiflow, a provider of cybersecurity solutions for critical infrastructure, today announced that the company has revealed the first documented cryptocurrency malware attack on a SCADA network of a critical infrastructure operator.

(SCADA: Supervisory control and data acquisition)

Radiflow discovered this cryptocurrency malware attack as part of routine and ongoing monitoring of the network of a waste water utility customer. The company reports that this attack infected several servers in the network in order to mine ... the Monero cryptocurrency.

Radiflow's research team uncovered that this cryptocurrency malware was designed to run in a stealth mode on a computer or device and to disable its security tools in order to operate undetected and maximize its mining processes for as long as possible.

Nuclear scientists logged on to one of Russia's most secure computers — to mine bitcoin
https://www.washingtonpost.com/news/worldviews/wp/2018/02/09/nuclear-scientists-logged-on-to-one-of-russias-most-secure-computers-to-mine-bitcoin

Several scientists working at a nuclear weapons facility in Russia were arrested on the suspicion that they used one of the country's most powerful supercomputers ... to mine bitcoins, the BBC reported.

The alleged infraction took place at the Federal Nuclear Center in Sarov, a top-secret area surrounded by barbed-wire fences where the Soviet Union's first nuclear bomb was produced during the Cold War.

According to the BBC and the Interfax news agency: "There has been an unsanctioned attempt to use computer facilities for private purposes including so-called mining. As far as we are aware, a criminal case has been launched against them."

Bank robber Willie Sutton's famous explanation of his chosen career:

When asked why he robbed banks, Willie replied,
"I rob banks because that's where the money is."

~30~