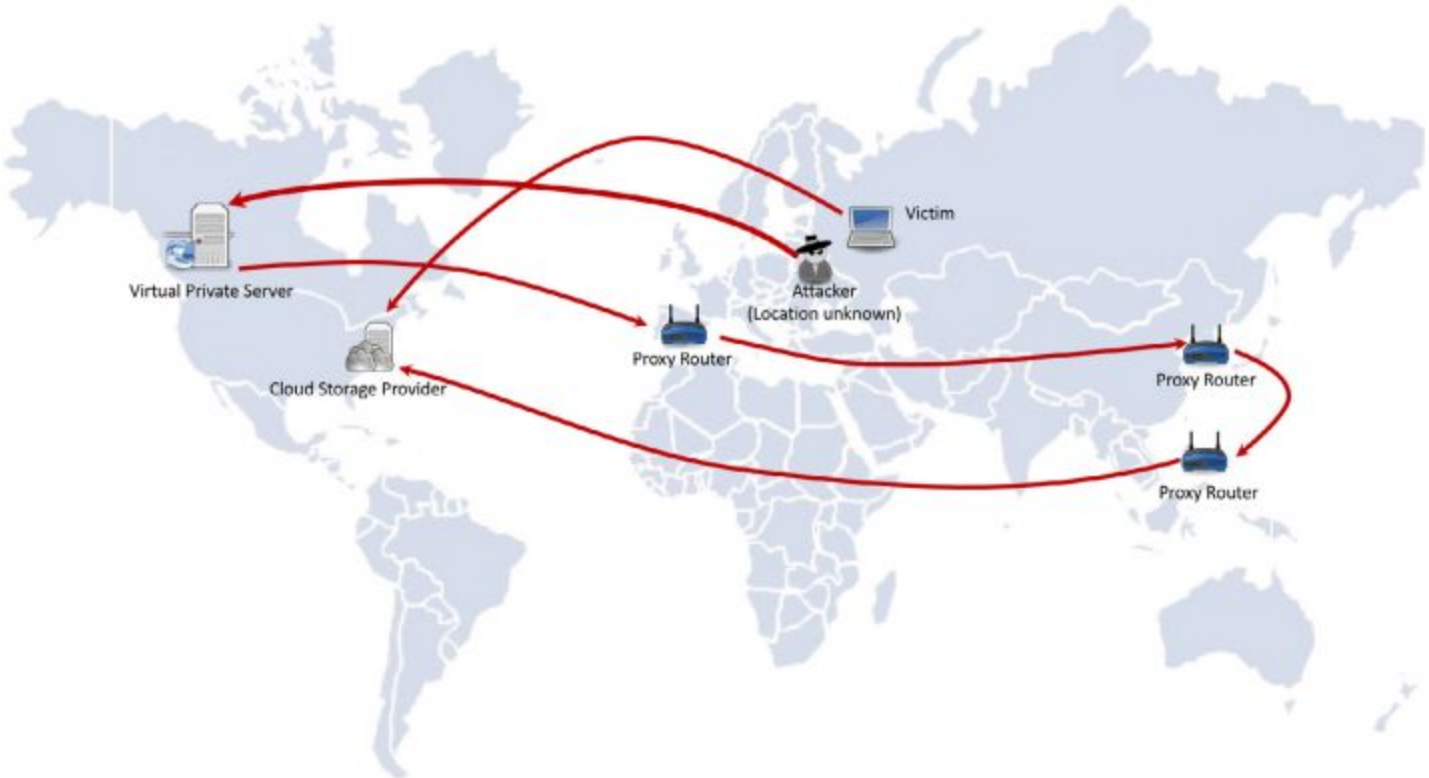
Security Now! #659 - 04-17-18

Never a Dull Moment

This week on Security Now!

This week we discuss AMD's release of their long-awaited Spectre variant 2 microcode patches, the end of Telegram messenger in Russia, the on-time arrival of Drupalgeddon2, Firefox and TLS v1.3, the new and widespread UPnProxy attacks, Microsoft's reversal on no longer providing Windows security updates without A/V installed, Google Chrome's decision to prematurely remove HTTP cookies, the Android "patch gap", renewed worries over old and insecure Bitcoin crypto, new attacks on old IIS, a WhatsApp photo used for police forensics, and an IoT vulnerability from our "you can't make this stuff up" department.

Our Picture of the Week



Security News

The IRS's e-Filing system is... overtaxed!

The site's error message states that the system is down for what its error message states is a "planned outage". If that's the case, it's about the worst timing imaginable since today is the US tax filing deadline!

AMD releases Spectre fixes for chips since 2011

https://www.amd.com/en/corporate/security-updates#paragraph-290416

<AMD April 10th> "Operating System Updates for GPZ Variant 2/Spectre"
Microsoft is releasing an operating system update containing Variant 2 (Spectre) mitigations for AMD users running Windows 10 (version 1709) today. Support for these mitigations for AMD processors in Windows Server 2016 is expected to be available following final validation and testing.

In addition, microcode updates with our recommended mitigations addressing Variant 2 (Spectre) have been released to our customers and ecosystem partners for AMD processors dating back to the first "Bulldozer" core products introduced in 2011.

AMD customers will be able to install the microcode by downloading BIOS updates provided by PC and server manufacturers and motherboard providers. Please check with your provider for the latest updates.

https://developer.amd.com/wp-content/resources/Architecture_Guidelines_Update_Indirect_Branch_Control.pdf

<AMD> AMD64 TECHNOLOGY INDIRECT BRANCH CONTROL EXTENSION
This document describes an indirect branch control feature designed to mitigate indirect branch target injectionon AMD products. There are three defined mechanisms: Indirect Branch Prediction Barrier (IBPB), Indirect Branch Restricted Speculation (IBRS), and Single Thread Indirect Branch Prediction mode (STIBP).

PRESENCE: The presence of the three features are indicated through three CPUID bits. AMD does enumerate these features differently than other x86 vendors.

IBPB support is indicated by CPUID Function 8000_0008, EBX[12]=1.

IBRS support is indicated by CPUID Function 8000_0008, EBX[14]=1. STIBP support is indicated by CPUID Function 8000_0008, EBX[15]=1.

Support for IBPB implies that MSR 0x49 exists in the architecture. Support for IBRS or STIBP implies MSR 0x48 exists. Here is a simple representation in table form:

REMEMBER: The company is still preparing patches for the RyzenFall, MasterKey, Fallout, and Chimera vulnerabilities that came to light last month, considered less dangerous and easier to fix than the Meltdown and Spectre flaws.

From the blunt knife department: Russia's Telegram blockage creates a huge mess
In a futile effort to make its server more difficult to block, Telegram moved a bunch of its IPv4 space IP addresses into net blocks used by Amazon's and Google's cloud platforms.

So what did Russia do? Yesterday, Russia began blocking 15.8 MILLION IPs on those Amazon and Google cloud platforms. Specifically:

52.58.0.0/15
18.196.0.0/15
18.194.0.0/15
35.156.0.0/14

Additionally, Russia's telecommunications regulator asked Apple and Google to pull Telegram from their app stores, requested that popular sideloading site "APK Mirror" cease serving Telegram (which would be the first alternative for Android users, should Google comply and pull Telegram from the Play Store), and even urged VPN providers to prevent Telegram messages from getting through.

The New York Times, in their reporting noted that the ban on Teegram will put the Kremlin in a slightly awkward position because many inside the government, including those in President Vladimir Putin's press office, use Telegram. Russia's Foreign Ministry has announced its intention to move to the Viber messaging app. Viber also states that everything is encrypted... but presumably not so much.

The Drupalgeddon2 arrives right on schedule
https://www.bleepingcomputer.com/news/security/exploitation-of-drupalgeddon2-flaw-starts-after-publication-of-poc-code/
https://thehackernews.com/2018/04/drupal-rce-exploit-code.html

https://research.checkpoint.com/uncovering-drupalgeddon-2/
Uncovering Drupalgeddon 2
(Last Thursday) April 12, 2018

Two weeks ago, a highly critical (25/25 NIST rank) vulnerability, nicknamed Drupalgeddon 2 (SA-CORE-2018-002 / CVE-2018-7600), was disclosed by the Drupal security team. This vulnerability allowed an unauthenticated attacker to perform remote code execution on default or common Drupal installations.

Until now details of the vulnerability were not available to the public, however, Check Point Research can now expand upon this vulnerability and reveal exactly how it works.

In brief, Drupal had insufficient input sanitation on Form API (FAPI) AJAX requests. As a result, this enabled an attacker to potentially inject a malicious payload into the internal form structure. This would have caused Drupal to execute it without user authentication. By exploiting this vulnerability an attacker would have been able to carry out a full site takeover of any Drupal customer.

The vulnerability existed on all Drupal versions from 6 to 8, though has since been patched to those who manually update their site. In this document we will showcase real life attack scenarios around an out-of-the-box installation of Drupal's flagship product, Drupal 8.

Sample PoC exploit code: https://github.com/dreadlocked/Drupalgeddon2

Last Friday the 13th...
Description

This Public Service Announcement is a follow-up to SA-CORE-2018-002 - Drupal core - RCE. This is not an announcement of a new vulnerability. If you have not updated your site as described in SA-CORE-2018-002 you should assume your site has been targeted and follow directions for remediation as described below.

The security team is now aware of automated attacks attempting to compromise Drupal 7 and 8 websites using the vulnerability reported in SA-CORE-2018-002. Due to this, the security team is increasing the security risk score of that issue to 24/25

Sites not patched by Wednesday, 2018-04-11 may be compromised. This is the date when evidence emerged of automated attack attempts. It is possible targeted attacks occurred before that.

Simply updating Drupal will not remove backdoors or fix compromised sites.

If you find that your site is already patched, but you didn't do it, that can be a symptom that the site was compromised. Some attacks in the past have applied the patch as a way to guarantee that only that attacker is in control of the site.

Firefox begins bringing up support for TLS v1.3 - Joins Chrome.
FF v59.0.2
Goto https://ssllabs.com -- Select "Test your browser"
You'll likely see that your browser supports TLS v1.2 max.
Goto "about:config" -- security.tls.version.max
It's likely set to '3' ... set it to '4' / No need to restart anything
Go back to the ssllabs.com tab and refresh the report.
Now you have TLS v1.3.

"UPnProxy" targeting SOHO routers
https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

WAN-exposed UPnP is ==insane==
Akamai has detected more than 4.8 million routers that expose various UPnP services via the WAN interface. Of these, Akamai experts say they've identified active NAT injections on over 65,000 of these devices, meaning these routers have already been compromised and are actively being used to reroute traffic without the device owner's consent or knowledge.

It takes about five seconds at GRC:
Main Menu: Services / ShieldsUP! / "GRC's Instant UPnP Exposure Test"
53,922 open UPnP ports found -- should be =ZERO=
Security Now! Episode #389

Bad guys are using SOHO routers to bounce their traffic round the world just like in the fictional movies... but it's no longer fiction and it's no longer difficult.

In other bad router news, due to the growing population of Android mobile devices, routers are also being hacked to redirect DNS to fraudulent sites for the installation of malware with high permission levels.

Microsoft is now ignoring their own Windows update blocking registry key.
Recall that part of January's updates for Meltdown and Spectre was the decision to block all future updates until a special "updates permitted" registry key was present. [...]

This was a HUGE mess and, in retrospect probably a mistake. Everyone was confused.

And users who elect not to use A/V -- even Microsoft's -- were suddenly without critical security updates.

LAST month's security updates WERE allowed to proceed for Windows 10.

And THIS month's security updates were allowed for Windows 7 and 8.1.

https://support.microsoft.com/en-us/help/4072699/windows-security-updates-and-antivirus-software

Windows Update and WSUS will offer this update to applicable Windows client and server operating systems regardless of the existence or value of the "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat\cadca5fe-87d3-4b96-b7fb-a231484277cc" registry setting. This change has been made to protect user data.

Google's Chrome 70 to deliberately expire HTTP (non-secure) cookies faster.
As of late October 2018 with the release of Chrome v70, Google's Chrome browser will begin deliberately ignoring the expiration of non-secured cookies delivered over HTTP and will cap their expiration to one year

And the longer term plan is to reduce HTTP cookie life to a few days.

This is another clever way of forcing the deprecation of HTTP, though I have somewhat annoyed/mixed feelings, as this is a deliberate violation of the HTTP standard.

At the same time, "Firesheep" showed us that you cannot have secure sessions when session cookies are transiting in the clear.

The "Android Patch Gap"
https://srlabs.de/bites/android_patch_gap/
A German security firm "Security Research Labs" (SRL) revealed that some major Android mobile device OEMs are misrepresenting the completeness of patches for their devices.

The screen may show a "Security Patch Level: <<date>>" while not containing a handful or more of critical security patches.

in an interview with Wired Magazine, the researchers said: "Sometimes these guys just change the date without installing any patches. Probably for marketing reasons, they just set the patch level to almost an arbitrary date, whatever looks best."

Why?

SRL researchers investigated smartphones that had supposedly received and installed the latest Android updates and released the following breakdown of their findings:

0-1 missed patches—Google, Sony, Samsung, Wiko Mobile
1-3 missed patches—Xiaomi, OnePlus, Nokia
3-4 missed patches—HTC, Huawei, LG, Motorola
4+ missed patches—TCL, ZTE

Specifically, the above result focused on security patches for Critical and High severity vulnerabilities that were released in 2017.

There IS some good news on the horizon that we have discussed previously: Google's project "Treble". Treble introduces a re-architecture of Android to dis-entangle the OEM customizations from the OS code, making updates far less involved for OEMs... and thus much more likely to occur.

Essentially... everyone wants everything to be patched, but OEMs -- who really just want to sell and forget electronics to consumers -- have been complaining about how much of their resources are being tied up by this continuing patch activity. So Google is responding to make it much less troublesome.

Back when JavaScript's "SecureRandom()" was neither secure nor random
We have known for about five years that the orginal "SecureRandom()" function provided by JavaScript, despite providing plenty of bits, actually only contained about 48 bits of true entropy.

JavaScript browser-based Bitcoin wallets, and some Wallet apps that also used the early JavaScript libraries, relied upon that low-entropy function to generate both the Bitcoin address =and= the user's private key.

And that, in turn, makes those Bitcoin addresses much (much!) easier to crack using today's much faster technologies.

So we have the trifecta of:

(1) An inherently low entropy private key.
(2) The increase in brute-forcing processing power, and
(3) The significant increase in Bitcoin valuation.

In other words: Means, Motive, and Opportunity.

People holding sufficiently large balances who may have obtained their Bitcoin crypto data from a low entropy source are advised to move their funds to a newly minted Bitcoin address.

An old IIS 6.0 (WinXP / Server 2003) WebDAV flaw gets new life
https://www.bleepingcomputer.com/news/security/windows-servers-targeted-for-cryptocurrency-mining-via-iis-flaw/

Malicious cryptocurrency miners are searching around for any still-exploitable places they can install and run their mining software.

These devices MUST be connected to the Internet and they will optimally be as fast as possible. This places public Internet servers among the ideal targets.

So now another old and long-since-patched bug in Microsoft's IIS v6 -- in the WebDAV service. Just over a year ago a pair of Chinese researchers discovered that an attacker can craft and send a malicious PROPFIND request to an IIS v6 server with WebDAV enabled, that contains an oversized IF header. When the IIS WebDAV controller reads this request, a buffer overflow occurs, allowing attackers to deliver and execute code on the targeted server.

Due to the server's age -- this was the server 2003 which was released with WinXP -- though it still accounts for 11.3% of all IIS server installations -- the code is well past end-of-life and will no longer be updated.

According to Shodan, there are a little over 600,000 publicly accessible IIS 6.0 servers on the Internet, most of them likely running on Windows Server 2003. Fortunately, however, most of them will not have WebDAV, though it will be enabled for any SharePointd Portal servers... so there are still plenty.

Consequently, the "Electroneum" cryptocurrency is being actively mined through an "Internet scale" campaign to find and commandeer any still-available servers.

If you have IIS v6, turn off WebDAV if you can. If you cannot, a free non-Microsoft page IS available:

https://blog.0patch.com/2017/03/0patching-immortal-cve-2017-7269.html

WhatsApp photos of a hand was used as a new source of crime forensics
https://www.bleepingcomputer.com/news/government/eleven-drug-convictions-after-extracting-fingerprint-from-whatsapp-photo/
http://www.bbc.com/news/uk-wales-43711477

From the BBC:
There were just parts of the middle and bottom of a finger visible. As we all know, police records only keep the top part. This meant the image could not be directly matched on national databases. However, other evidence collected meant officers already had a very good idea who was behind the drug selling operation. So they were able to use photographic evidence from the photo, which would normally have been insufficient and ignored, to positively confirm their suspicion and obtain a chain of eleven related convictions.

South Wales Police Dave Thomas said: "While the scale and quality of the photograph proved a challenge, the small bits were enough to prove he was the dealer."

I was reminded of TOR where as we have noted before, it is FAR more practical to =confirm= a suspicion of whose traffic is moving into and out of the network than it is to identify a connection from among all possible endpoints.

From our "You cannot make this up" department
https://thehackernews.com/2018/04/iot-hacking-thermometer.html
An unnamed casino, located in North America, had 10 gigabytes of its internal network data, including all of the casino's "High Roller" database, exfiltrated to a location in Finland...

... through a newly installed Internet-connected aquarium thermometer.

Nicole Eagan, the CEO of cybersecurity company Darktrace, told attendees at an event in London last Thursday how cybercriminals hacked an unnamed casino through its Internet-connected thermometer installed into an aquarium in the lobby of the casino. According to Eagan, the hackers exploited a vulnerability in the thermostat to gain a foothold into the network. Once there, they accessed the high-roller database of gamblers and "then pulled it back across the network, out the thermostat, and up to the cloud."

This is a perfect and classic demonstration of the CRUCIAL need for network isolation and segmentation. We are beginning to see WFi routers with multiple isolated guest networks... and this is precisely what is needed.

Miscellany
Lost In Space / 2018

SpinRite

Mike in Dundas, Ontario
Subject: Overcoming SSE
Date: 15 Apr 2018 13:53:44

Hi Steve and Leo,

I have been waiting a long time to drop you guys a note. I decided the trigger for my correspondence was to be a miraculous save using Spinrite. That is why I titled this document Overcoming Spinrite Story Envy.

I, like many many others, I have heard on this podcast, I purchased a copy of Spinrite as a thank-you for the invaluable service you both provide. I have been listening to Leo for quite some time from very early when he spent a lot of time in Toronto. Thought I would give his new SecurityNow podcast a listen.

You had me from the very beginning. I guess I am a "SN0dder" (Security Now 0-day) er SN0D.:)

However, I've finally given up waiting for a drive to have trouble because I don't think it will ever happen to me personally: I practice Steve's Hard Drive Hygiene protocol to the point where I too have a dedicated Spinrite machine and my daughter uses Spinrite as a verb!

Just wanted to say thanks, and that you guys are the best!