

Security Now! #572 - 08-09-16

Defcon & Blackhat, Pt.1

This week on Security Now!

A distressing quantity of distressing Win10 news, Apple's changing bug bounty policy, newly disclosed Android takeover flaws, yet another way to track web visitors, hackers spoof Tesla auto sensors, Firefox and LastPass news, some miscellany, then a 19-year old stubborn decision by Microsoft comes home to roost, and a handful of new problems found with HTTP.

Security News

Woody Leonard, Infoworld: "Windows 10 Anniversary Update woes continue"

- <http://www.infoworld.com/article/3104999/microsoft-windows/windows-10-anniversary-update-woes-continue.html>
- "Problems with last week's Anniversary Update keep piling up, and solutions remain elusive"
- Late last week, I recommended that you actively block the Windows 10 Anniversary Update. The past few days have brought yet another wave of complaints. Here's a sample...
- Last week, I talked about the Reddit post from SoloWingX stating that Windows 10 freezes completely after the Anniversary Update. That thread is now up to 680 comments. To all affected people, we haven't yet found a definite solution, so the only option to get a working PC at the moment is to roll back to a previous build in case you updated.
- Edge still has plenty of problems. I've hit situations where Edge will not close by clicking on the red X. Also, I can X out of the last open tab and Edge keeps running, when closing the only open tab should shut down the program as a whole. The problems seem to appear after visiting sites with lots of ads -- like the ones linked to from msn.com, for example. Once the problems start, they don't go away. The only solution I've found is to reboot.
- Two A/V manufacturers have reported problems:
 - Intel's McAfee warns: DO NOT [emphasis in the original] upgrade to the Windows 10 Anniversary Update without first verifying whether your McAfee product is compatible. This caution affects the products listed in the section above... Microsoft intended to implement an upgrade and installation check to ensure that no incompatible McAfee product versions could be installed or present. Due to time constraints, Microsoft could not implement the intended version check in the Windows 10 Anniversary Update
 - Avast offers a similar warning.

- I'm still unclear about the ability to block crapware tiles. I wrote about the problem a couple of weeks ago: Admins can't keep Microsoft from pushing crapware Live tiles onto Win10 Pro PCs because certain Group Policies don't work in the Anniversary Update. My current Win10 Pro AU machine has tiles for Solitaire, Candy Crush Soda Saga, Pandora, Asphalt 8, Age of Empires Castle Siege, FarmVille 2, Minecraft, Twitter, and Get Office -- in other words, about half of my Start menu tiles are unabashed, Microsoft-installed crapware, all on a machine that's been through the official "start fresh" regimen.

Windows 10 Anniversary Update Borks Dual-Boot Partitions

- <https://linux.slashdot.org/story/16/08/03/1614223/windows-10-anniversary-update-borks-dual-boot-partitions>
- It appears that Windows 10 AU is not respecting the contents of non-Windows partitions. It overwrites the drive's boot sector, which is not unexpected, which is why standard practice on dual-boot systems is to install Windows first and Linux, for example, second. But the Win10AU is reportedly overwriting the contents of pre-existing non-Windows partitions.

Win10 AU re-enabling privacy-related features.

- There are many reports of the Win10 Anniversary Update re-enabling many of the privacy-related settings that users had previously disabled.
- Apple has annoyed us by continually turning Bluetooth back on, but this is a bit more worrisome.

Microsoft removes policies from Windows 10 Pro

- <http://www.ghacks.net/2016/07/28/microsoft-removes-policies-windows-10-pro/>
- Professional editions of Windows 10 ship with the Group Policy Editor that enables users and administrators to make changes to the default configuration of the operating system.
- Policy availability was previously uniform.
- But this is no longer the case with the Windows 10 Anniversary Update.
- Some policies now contain a note stating that they only apply to certain editions of Windows 10, with Windows 10 Pro not being listed as one of them.
- And the corresponding Registry keys are no longer working either, so Pro users have no option to make changes to features affected by the change.
- **Examples:**
- Turn off Microsoft consumer experiences
 - Computer Configuration > Administrative Templates > Windows Components > Cloud Content
 - This controls, among other things, the installation of third-party apps and extra links on Windows 10. If you did not wish to have Candy Crush pushed to your operating system, you'd disable the policy to block that from happening. This change prevents Windows 10 Pro users from enabling the policy to block third-party application installations or links.

- Do not show Windows Tips
 - Windows 10 may show tips to the user of the operating system that explain how to use Windows 10, or how to use certain features of the operating system.
 - That option to disable this has been removed.

- Lock screen
 - Computer Configuration > Administrative Templates > Control Panel > Personalization
 - The lock screen displays information such as a clock or notifications to the user of the operating system.
 - The policy "do not display the lock screen" allowed you to turn the lock screen off so that the logon screen is displayed right away.
 - The change blocks the policy on Windows 10 Pro systems. After the Anniversary Update it is only available on Enterprise, Education and Server.

- Similarly, "Prevent changing log screen and logon image" and "Force a specific default lock screen and logon image" are also no longer available on Windows 10 Pro devices.

- Disable all apps from Windows Store
 - Computer Configuration > Administrative Templates > Windows Components> Store
 - The policy allows you to disable all applications from Windows Store. It blocks the launching of all store apps that came pre-installed or were downloaded before the policy was set. Also, it will turn of Windows Store. Once the Anniversary Update is installed the setting applies only to Enterprise and Education editions of Windows 10.

Free Windows 10 Upgrade Still On for Windows 7/8 keys

- <http://www.ghacks.net/2016/08/04/free-windows-10-upgrade-78-keys/>
- <http://www.zdnet.com/article/windows-10-free-upgrade-is-still-available-using-windows-7-and-8-product-keys/>
- MaryJo, writing for All About Microsoft, August 3rd: "In spite of the official end of the free Windows 10 update offer on July 29, it seems any valid Windows 7/8.x retail product key still installs Windows 10 for now."
- Quote: Yes, Microsoft officials insisted and insisted again (links) that after July 29 at 11:59 p.m. UTC, the free Windows 10 upgrade offer would end. But it didn't -- at least not completely. The Get Windows 10 (GWX) promotions seem to have ended. But I've heard from several Windows users that they've been able to take advantage of the free Windows 10 update using their older Windows 7/8.X product keys after July 29. Users have been able to both kick off and activate Windows 10 on machines where they've previously installed Windows 10... AS WELL AS on machines where they have NEVER installed Windows 10 using their Windows 7/8.X product keys. My ZDNet colleague Ed Bott mentioned in passing in an updated post about Windows 10 that he also was able to get Windows 10 for free after July 29 using a never-used Windows 7 Ultimate product key. Paul Thurrott of Thurrott.com also noted last week that he still was able to get Windows 10 for free using an existing product key. While some have noted that Microsoft isn't restricting Windows 7 and 8.X users -- whether legitimately or not -- from continuing to

have access to Windows 10 via the company's assistive technology offer, this key loophole is different.

Apple announces long-awaited bug bounty program

- <https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program>
- At BlackHat, last Thursday (Aug 4th) Apple's Ivan Krstic announced a reversal of Apple's longstanding "we don't pay bug bounties" policy with the news that Apple will begin offering cash bounties of up to \$200,000 to researchers who discover vulnerabilities in its products.
- Apple's previous position was Apple vulnerabilities are so valuable to others -- governments and the black market -- that they would simply be outbid by them. So why bid at all?
- Remember that the FBI reportedly paid nearly \$1 million for the exploit it used to break into Syed Farook's work-related iPhone.
- Rich Mogull, the CEO of Securosis, said: "A bug bounty program is unlikely to tempt any hackers who are only interested in getting a massive payout. For those who only care about cash, Apple could probably never pay enough. But for those who care about making an impact, getting a check from Apple could make all the difference by incentivizing good work.
- Put another way: If you have no interest in allowing your work to be used for evil, but you would like your important security findings to be rewarded and supported... that can now happen on Apple's platforms.

Four newly disclosed 'Quadrooter' flaws affect over 900 million Android phones

- Adam Donenfeld of CheckPoint at DefCon: "Stumping the Mobile Chipset"
- Synopsis: Following recent security issues discovered in Android, Google made a number of changes to tighten security across its fragmented landscape. However, Google is not alone in the struggle to keep Android safe. Qualcomm, a supplier of 80% of the chipsets in the Android ecosystem, has almost as much effect on Android's security as Google. With this in mind, we decided to examine Qualcomm's code in Android devices. During our research, we found multiple privilege escalation vulnerabilities in multiple subsystems introduced by Qualcomm to all its Android devices in multiple different subsystems. In this presentation we will review not only the privilege escalation vulnerabilities we found, but also demonstrate and present a detailed exploitation, overcoming all the existing mitigations in Android's Linux kernel to run kernel-code, elevating privileges and thus gaining root privileges and completely bypassing SELinux (Security Enhanced Linux).
- <http://www.zdnet.com/article/quadrooter-security-flaws-affect-over-900-million-android-phones/>
- All versions of Android are vulnerable to newly revealed flaws.
- They won't be patched until the September security release next month.
- These flaws in Android phones and tablets that ship with Qualcomm chips could let a hacker take full control of an affected device.
- Nearly a billion Android devices are affected by these high risk privilege escalation vulnerabilities, dubbed "Quadrooter," say researchers at security firm Check Point.
- Attacker induces user to install an innocent-appearing application.
- NO special permissions are required for the application.

- The flaws then provide the app with root access.
- Check Point said most phone makers have devices that are vulnerable, including Google's Nexus 5X, Nexus 6, and Nexus 6P, HTC's One M9 and HTC 10, and Samsung's Galaxy S7 and S7.
- The recently-announced BlackBerry DTEK50, which Blackberry touts as the "most secure Android smartphone", is also vulnerable. (As we know, such security claims are purely marketing and have no actual security relevance.)
- Earlier this year, between April and July, Qualcomm fixed the flaws and has issued patches.
- Several have already been pushed out and should be in place, where updates are occurring, by next month's updates.

The HTML5 Battery Status API

- It's been around quietly for some time. (FF since v16, Chrome & Opera - NO Safari or IE.)
- <http://caniuse.com/#feat=battery-status>
- Mozilla: "...provides information about the system's battery charge level and lets you be notified by events that are sent when the battery level or charging status change. This can be used to adjust your app's resource usage to reduce battery drain when the battery is low, or to save changes before the battery runs out in order to prevent data loss."
- Elsewhere: "In the context of Open Web Apps, knowing the battery status can be useful in a number of situations:
 - Utility apps that collect statistics on battery usage or simply inform the user if the device is charged enough to play a game, watch a movie, or browse the Web
 - High-quality apps that optimize battery consumption: for example an email client may check the server for new email less frequently if the device is low on battery
 - A word processor could save changes automatically before the battery runs out in order to prevent data loss
- BatteryManager
 - .charging (bool)
 - .level (float) 0.0-1.0
 - .chargingTime (float) time in seconds to full charge
 - .dischargingTime (float) time in seconds to fully discharge
- Two Princeton University researchers modified a web browser to catalog tracking scripts. They found instances of scripts in the wild that were using the battery API to fingerprint specific devices. This tracking is possible in all current builds of Firefox, Opera, and Chrome.

Hackers Fool Tesla Model S's Autopilot to Hide and Spoof Obstacles

- <https://www.wired.com/2016/08/hackers-fool-tesla-s-autopilot-hide-spoof-obstacles>
- At DefCon, Chinese Researchers working with some from the University of South Carolina, demonstrated the use of off-the-shelf radio-, sound- and light-emitting tools to deceive Tesla's autopilot sensors. They were able to spoof the presence of non-existent obstacles and also mask the presence of real objects in the car's path.

Firefox is getting the Let's Encrypt ISRG X1 root cert.

- https://bugzilla.mozilla.org/show_bug.cgi?id=1289889#c6
- https://bugzilla.mozilla.org/show_bug.cgi?id=1290999
- A Firefox test build with this patch (that adds the ISRG root) has been started.
- (<https://treeherder.mozilla.org/#/jobs?repo=try&revision=62d1b7f6d67c>)

LastPass offers their own TOTP-compatible authenticator app

- <https://lastpass.com/auth/>
- iOS, Android, Windows
- Have Lastpass installed in the browser and logged in.
- <https://helpdesk.lastpass.com/multifactor-authentication-options/lastpass-authenticator/>
- Supports:
 - Time based 6 digit codes
 - One-tap push notifications
 - SMS 6 digit codes

Miscellany

GRC's DNS Spoofability Test is up again!

- Gratuitous ARP

Justin Garrison (@rothgar)

- re: Firefox and the installation of proxy certs
- Assuming traffic is allowed, the user doesn't need a full VM for Firefox, just a portable version run from USB drive and it keeps a separate key store from system installed version.

Netflix: "Stranger Things"

- Goonies, Super8, Close Encounters

SpinRite

Trevor Harrison in Vancouver British Columbia Canada

Subject: With ZFS "Scrub" is SpinRite still needed on ZFS volumes?

Hello Steve,

I am building my first FreeNAS box. Hanging out in the Free NAS IRC channel I've been told that the ZFS "Scrub" is a block by block scrub of the drive to find bad blocks. I know SpinRite works at the "Sector" level below the file system (at the metal level?). So can you explain to us (and even do a ZFS in-depth podcast) as to why ZFS scrub replaces SpinRite or doesn't? I personally think it doesn't, but running SpinRite on a live server with lots of drives...well you get the idea... I'd like to know for sure and understand the differences. (Do you ever SpinRite your GRC servers)?

Also I will be buying SpinRite as soon as I can hear my Yababa Do live?

Kind Regards, Trevor Harrison

Note:

- ZFS provides RAID-style parity blocks but **also** pre-block checksums.
- Scrubbing:
 - read a data block, compute its checksum.
 - read the checksum from disk, compare to computed checksum.
 - compute parity for the block, compute checksum for parity block.
 - read checksum for parity block from disk, compare to computed checksum

And there's more!!

Microsoft won't fix Windows flaw that lets hackers steal your username and password

- <http://www.zdnet.com/article/windows-attack-can-steal-your-username-password-and-ot-her-logins/>
- The flaw, which allows a malicious website to extract user passwords, is made worse if a user is logged in with a Microsoft account.
- Only with Microsoft's (IE & Edge) browsers, not Firefox or Chrome.
- (Also... an eMail to Microsoft Outlook.)
- 19 years ago: <http://insecure.org/splotts/winnt.automatic.authentication.html>
- Title: "WinNT/Win95 Automatic Authentication Vulnerability (IE Bug #4)"
- Microsoft: "We're aware of this information gathering technique, which was previously described in a paper in 2015. Microsoft released guidance to help protect customers and if needed, we'll take additional steps," the spokesperson said.
- Lawrence Abrams (Bleeping Computer)
 - <http://www.bleepingcomputer.com/news/security/understanding-the-windows-credential-leak-flaw-and-how-to-prevent-it/>

Four HTTP/2 Protocol implementation flaws:

- At BlackHat last week, security researchers at Imperva revealed details for multiple implementation vulnerabilities in the HTTP/2 implementations.
- <http://thehackernews.com/2016/08/http2-protocol-security.html>
- <http://blog.imperva.com/2016/08/http2-faster-and-better-than-http-11-but-is-it-more-secure.html>
- **In the Slow Read attack**, a malicious client deliberately reads responses very slowly. This is hauntingly similar to the well-known Slowloris DDoS attack experienced by major credit card processors in 2010. The Imperva research team identified variants of this vulnerability across most popular web servers, including Apache, IIS, Jetty, NGINX and nhttp2.
- **The HPACK Bomb** is a compression-layer attack resembling a zip bomb. (It's a form of data interpretation exploit.) The attacker crafts small and seemingly innocent messages

that decompress into a significant amount of data (gigabytes) on the server, bloating memory footprint and often crashing the server.

- **The Dependency Cycle Attack** takes advantage of the flow control mechanisms that HTTP/2 introduced for network optimization. The malicious client crafts requests that induce a dependency cycle, which forces the server into an infinite loop as it tries to process these dependencies.
- **With Stream Multiplexing Abuse**, an attacker uses flaws in the way servers implement the stream multiplexing functionality to crash the server.

The TCP HEIST attack

- HEIST: HTTP Encrypted Information can be Stolen through TCP-windows
- https://tom.vg/papers/heist_blackhat2016.pdf
- HEIST: New attack steals SSNs, e-mail addresses, and more from HTTPS pages
- <http://arstechnica.com/security/2016/08/new-attack-steals-ssns-e-mail-addresses-and-more-from-https-pages/>
- Fully browser-side capability to measure precise TCP packet sizes.
- This allows many of the compression-driven exploits WITHOUT a MITM.