Security Now! #537 - 12-08-15

A Mega News Week

This week on Security Now!

- Microsoft’s Patch Tuesday (And Adobe FLASH mega patch tuesday!)
- Microsoft's new moves to force Windows 10 onto unwanting users.
- Even bigger trouble for Dell, and trouble for AOL and Lenovo
- Let's Encrypt public beta goes live!
- What did President Obama mean on Sunday?...
- Perhaps France is (over)reacting?
- The Republic of Kazakhstan paves a worrisome path
- ISIS releases an App for Android
- Mozilla make another good decision (and another new bit of iOS freeware)
- CryptoWall gets even worse
- And even more... plus a bunch of fun Miscellany!

Martin Chadderton @mchadder
@SGgrc didn't know you were branching out Steve?

Security News:

Microsoft's second Tuesday of the Month

- 12 patch bundles, 8 of them critical, 4 important
- Remote Code Execution vulnerabilities for: Office, Uniscribe, Silverlight, "Graphics Component", DNS, JScript & VBScript.
- Critical update packages for their Edge and IE browsers.

Adobe updates FLASH to v20.0.0.235

- https://helpx.adobe.com/security/products/flash-player/apsb15-32.html
- <Adobe> Adobe has released security updates for Adobe Flash Player. These updates address critical vulnerabilities that could potentially allow an attacker to take control of the affected system.
- How many??? 78!!!
- Now at v20.0.0.235
- And still trying to push McAfee "Security Scan Plus" on us.

Microsoft is using Win7 and 8.1 updates to enable and re-enable unwanted upgrades

- http://www.computerworld.com/article/3012278/microsoft-windows/microsoft-sets-stage-for-massive-windows-10-upgrade-strategy.html
- Windows 10 Dramatically Increased Connectivity
- Saying "Dramatically Increased Connectivity" over and over is too laborious, thus: "DIC"
- In the wake of Windows 10 DIC, we've seen the creation of many freeware apps to assist users in managing Windows 10 DIC, because they feel rather strongly about not wanting to have any DIC... regardless of what that DIC's purpose and intentions may be.
- Another large group of people have decided that rather than getting Windows 10 and then working to neuter the DIC, they would prefer to simply remain on Windows 7 or 8.1.

- This has spawned another class of freeware to prevent Microsoft from shoving Windows 10 down everyone's throat.
- One such tool is that GWX Control Panel by Josh Mayfield
- (GWX == Get Windows 10)
- Formerly "GWX Stopper" renamed to GWX Control Panel
- Updated on November 24th to run continuously in the background to periodically check the Windows GWX settings:
- http://ultimateoutsider.com/downloads/ (installer or stand-alone)
- Since Windows 10's release, and thanks to his GWX Control Panel and users, Josh has been monitoring Microsoft's GWX behavior.
- http://blog.ultimateoutsider.com/2015/08/using-gwx-stopper-to-permanently-remove.html
- Josh: "December 1, 2015: I've gotten some very interesting reports from people using the new Monitor Mode feature. Different PCs are seeing different Windows 10 settings get re-enabled for mysterious reasons. They're not false alarms; these settings are really getting re-set by Windows (it's not happening to everybody, just certain

users/computers), and I'm doing research and testing to see what I can do to stop it once and for all. To those of you observing this strange behavior: Hang in there; the next version of GWX Control Panel will have some features intended to help you regain control and better understand what's happening on your PC.

- The Windows Update engine has been updated and the December 1st release says:
  - "This update enables support for additional upgrade scenarios from Windows 7 to Windows 10, and provides a smoother experience when you have to retry an operating system upgrade because of certain failure conditions. This update also improves the ability of Microsoft to monitor the quality of the upgrade experience."

- ComputerWorld writes that <quote> In late October, Terry Myerson, the Microsoft executive who runs the Windows and devices teams -- dubbed the "More Personal Computing" group -- outlined how Microsoft would try to convince users of Windows 7 and 8.1 to upgrade to Windows 10. Rather than wait for customers running the older editions to request a copy of the new OS -- the original idea from the summer -- Microsoft will instead begin to automatically send the upgrade to PCs via Windows Update, the default security maintenance service.

- Gregg Keizer , writing for ComputerWorld continues: <quote> The new push will be a two-step process, with the first kicking in this year, the second in early 2016. First, Microsoft will add the Windows 10 upgrade to the Windows Update list on Windows 7 and 8.1 systems as an "optional" item. That list can be examined by users, letting them choose -- or not -- each optional update.

- Sometime next year, Microsoft will shift the Windows 10 upgrade from optional to the "recommended" list. Updates on that list are automatically downloaded and installed on most PCs.

- The GWX Control Panel app can be downloaded from Mayfield's website.
- The App is free, but Mayfield does accept donations through PayPal.
- Gregg Keizer who interviewed Josh quoted him saying: I get a donation from about one in every thousand downloads.

Dell Foundation Services Remote Information Disclosure

- http://lizardhq.org/2015/11/25/dell-foundation-services.2.html
- Dell Foundation Services "provides a core set of foundational services facilitating customer serviceability, messaging and support functions".
- DFS starts an HTTP server listening for connections on port 7779.
- The previous service tag leak was fixed by removing the JSONP API. (JSON w/Padding)
- But the web service is still available as a SOAP service (Simple Object Access Protocol), and all methods of that web service can be accessed, not just the ServiceTag method.
- One of the methods accessible is List<WmiManagementItem> GetWmiCollection(string wmiQuery) - this returns the results of a given Windows Management Instrumentation (WMI) query, enabling external remote access to information about hardware, installed software, running processes, installed services, accessible hard disks, filesystem metadata (filenames, file size, dates) and more.
- <<< This is where I remind everyone why we're all now behind our own border router,

hopefully with UPNP disabled. >>>
- Nevertheless, many potentially vulnerable hosts can be found via Shodan and the issue can also be exploited over a LAN.

AOL Desktop MiTM Remote File Write and Code Execution

- http://rum.supply/2015/12/05/aol-desktop.html
- AOL Desktop is "the all-in-one experience with mail, instant messaging, browsing, search, content, and dial-up connectivity". It is the direct successor of the old Windows AOL clients from the 1990s.

  Issues in AOL Desktop, version 9.8.1 and below, that have existed since 1993, can be exploited by an entity in a man-in-the-middle position to write files to disk and cause remote command execution.
- FDO91 - "Form Definition Order" http://mazur-archives.s3.amazonaws.com/aol-files/fdo91/tutorial_faq.html
- AOL: FDO stands for Form Definition Operator. AOL communicates using this programming language. For example, after clicking any icon or button in AOL, FDO code is sent by the AOL system and interpreted by your AOL to create a window. So, the FDO language is the language used to describe forms on the AOL client. This site has focus on learning how to program in FDO and provides a surfeit of examples and tutorials for those who want to learn.
- Homemade protocol designed to minimize bandwidth.
- Compiled homegrown scripting language.
- No authentication is done on any packets sent, and the client will execute any FDO it is sent by the server.

  Some FDO opcodes are interesting from an attacker's perspective. The fm_* series of opcodes (the File Management protocol, 0x08xx), have existed since the very first version of AOL for Windows from 1993. This series of opcodes enables reading from and writing to disk.

  The async_exec_app opcode (0x0d19) takes a string operand, and executes the command in that string. This opcode has existed since version 2.0 of AOL for Windows, from 1994.

Lenovo

- Lenovo Solution Center creates a process called LSCTaskService that runs with full administrator rights.
- That service listens on port 55555 for incoming connections using HTTP.
- It can be instructed via GET and POST HTTP requests to execute code in a directory a local user can access.
- Furthermore, Lenovo Solution Center will execute with full privileges, programs found in an arbitrary location on disk where the user can write to. Any malware placed there will be executed with admin rights.
- Any visited web pages are able to pass commands to the local LSC web server to execute with full privileges.

LetsEncrypt public beta goes live

- https://letsencrypt.org/2015/11/12/public-beta-timing.html
- Lots of LetEncrypt support is on the way...
    - LetsEncrypt Windows Compatable Powershell Modules for IIS and Apache (on Windows)
    - http://www.kingbain.com/letsencrypt-powershell-modules-for-iis-and-apache/
    - https://github.com/ebekker/ACMESharp/wiki/Example-Usage
    - Get HTTPS for free!
    - https://gethttpsforfree.com
    - https://github.com/diafygi/gethttpsforfree
    - This is a project that allows you to get a free HTTPS certificate without having to install any software or having to share your private keys with anyone. It uses the non-profit Let's Encrypt certificate authority to issue the free certificates. Hooray for free certs!
    - A Simple LetsEncrypt client
    - https://github.com/kuba/simp_le
    - Let's Encrypt Without Sudo
    - https://github.com/diafygi/letsencrypt-nosudo
    - The Let's Encrypt initiative is a fantastic program that offers free https certificates! However, the one catch is that you need to use their command program to get a free certificate. The default instructions all assume that you will run it on your your server as root, and that it will edit your apache/nginx config files.

        I love the Let's Encrypt devs dearly, but there's no way I'm going to trust their script to run on my server as root, be able to edit my server configs, and have access to my private keys. I'd just like the free ssl certificate, please.

        So I made a script that does that.

Obama's Sunday evening address from the Oval Office:

- <quote> ... And we constantly examine our strategy to determine when additional steps are needed to get the job done. [...] And that's why I will urge high-tech and law enforcement leaders to make it harder for terrorists to use technology to escape from justice.

France considers blocking Tor and public Wi-Fi after Paris attacks

- (I was briefly distracted by a sidebar animation of a flamethrower mounted on a quadcopter, which led to the question of drone-mounted firearms... we'll discuss in Miscellany.)
- Security forces outline new counter-terrorism measures in internal document
- http://www.theverge.com/2015/12/7/9860416/france-block-tor-public-wifi-paris-attacks
- <The Verge> French security forces have drafted proposals that would ban public Wi-Fi and access to the Tor network, Le Monde reports, citing internal documents from the Ministry of Interior. The anti-terror proposals come three weeks after Islamic extremists killed 130 people and injured more than 300 in a series of attacks across Paris.

    According to Le Monde, the documents outline two legislative proposals that French police and security forces would like to implement in the wake of last month's attacks. One pertains to the country's current state of emergency protocol, the other concerns

France's counter-terrorism laws. Both could be formally presented as early as January, the newspaper reports, adding that the ministry has yet to decide on the measures they outline.

- TOR:
  - Non-emergency counter-terrorism measure, therefore permanent.
  - The French proposal includes a measure that would "forbid and block" communications on the Tor network within the country.

    It also includes a measure that would oblige VoIP services to hand over encryption keys at the request of the government. The Tor Project, which runs the Tor network, did not immediately respond to a request for comment.
  - China has been blocking TOR since 2012 and both Iran and Russia have targeted TOR as well.

- Public Wi-Fi:
  - The measure to block "free and shared" Wi-Fi connections falls under the proposed state of emergency changes... so temporary while the state of emergency exists.
  - The documents obtained by Le Monde argue that public Wi-Fi networks should be blocked because it's difficult for security forces to identify users connected to them.

    Police also proposed changes that would allow them to search vehicles and luggage without consent, and to conduct identity checks without providing justification.

    France's state of emergency expands the government's ability to conduct warrantless searches, place suspects under house arrest, and seize the personal data of suspected terrorists. Following last month's attack, lawmakers extended the state of emergency for three months and passed an amendment that makes it easier for authorities to unilaterally shut down websites.

The Republic of Kazakhstan requires all Internet users to install new communications certificate.

- http://telecom.kz/en/news/view/18729
- https://web.archive.org/web/20151202203337/http://telecom.kz/en/news/view/18729
- November 30th, 2015:

  Kazakhtelecom JSC notifies on introduction of National security certificate from 1 January 2016

  From 1 January 2016 pursuant to the Law of the Republic of Kazakhstan «On communication» Committee on Communication, Informatization and Information, Ministry for investments and development of the Republic of Kazakhstan introduces the national security certificate for Internet users.

  According to the Law telecom operators are obliged to perform traffic pass with using protocols, that support coding using security certificate, except traffic, coded by means of cryptographic information protection on the territory of the Republic of Kazakhstan.

  The national security certificate will secure protection of Kazakhstan users when using

coded access protocols to foreign Internet resources.

By words of Nurlan Meirmanov, Managing director on innovations of Kazakhtelecom JSC, Internet users shall install national security certificate, which will be available through Kazakhtelecom JSC internet resources. «User shall enter the site telecom.kz and install this certificate following step by step installation instructions”- underlined N.Meirmanov.

Kazakhtelecom JSC pays special attention that installation of security certificate can be performed from each device of a subscriber, from which Internet access will be performed (mobile telephones and tabs on base of iOS/Android, PC and notebooks on base of Windows/MacOS).

Detailed instructions for installation of security certificate will be placed in December 2015 on site telecom.kz.

PR department
Kazakhtelecom JSC

30.11.2015

- Kazakhstan Announces Plan to Spy on Encrypted Internet Traffic
  - http://motherboard.vice.com/read/kazakhstan-announces-plan-to-spy-on-encrypted-internet-traffic

ISIS: The Islamic State releases its own smartphone app

- http://www.telegraph.co.uk/technology/news/12036736/Islamic-State-releases-its-own-smartphone-app.html
- The Islamic State has released its own app for Android smartphones which it uses to spread propaganda including videos of beheadings and messages about terrorist attacks in various parts of the world.

  The existence of the App was uncovered by the Ghost Security Group, a vigilante collective that aims to disrupt Isil's online operations.

  Rather than using the Google Play Store, which would allow Google to take it down, Isis is distributing installation links through encrypted Telegram App messages.

  Although thousands of Twitter accounts have been taken down, and Telegram has banned dozens of Isil channels, the use of its own app would allow Isil to avoid such attempts to police and block its communications.

Mozilla cancels plans for browser-based advertising

- Mozilla says it's getting out of the ad business so it can "focus on content discovery."
- https://blog.mozilla.org/advancingcontent/2015/12/04/advancing-content/
- Darren Herman, VP of Content Services…

  One of the many benefits of the Web is the ability to create unique, personalized experiences for individual users. We believe that this personalization needs to be done with respect for the user – with transparency, choice and control. When the user is at the center of product experiences everyone benefits.

Over the past two years, we've ideated, built and scaled a content platform that respects users. We served tens of billions of pieces of content. We experimented with all content – including advertising. We proved that advertising can be done well while respecting users. We have learned a ton along the way.

Our learnings show that users want content that is relevant, exciting and engaging. We want to deliver that type of content experience to our users, and we know that it will take focus and effort to do that right.

We have therefore made the decision to stop advertising in Firefox through the Tiles experiment in order to focus on content discovery. We want to thank all the partners who have worked with us on Tiles. Naturally, we will fulfill our current commitments as we wind down this experiment over the next few months.

Advertising in Firefox could be a great business, but it isn't the right business for us at this time because we want to focus on core experiences for our users. We want to reimagine content experiences and content discovery in our products. We will do this work as a fully integrated part of the Firefox team.

We believe that the advertising ecosystem needs to do better – we believe that our work in our advertising experiments has shown that it can be done better. Mozilla will continue to explore ways to bring a better balance to the advertising ecosystem for everyone's benefit, and to build successful products that respect user privacy and deliver experiences based upon transparency, choice and control.

Mozilla (today!) releases "Focus" content blocker for iOS 9.

- "Focus helps you improve the privacy and performance of your mobile browsing experience. You control what types of page content are allowed."
- Free.
- Based on Disconnect.me's open source block list.
- Uses Apple's content blocker API, so only works with Safari (not Mozilla's own Firefox).
- Not many features, just Yes/No switches for:
  - Block ad trackers
  - Block analytics trackers
  - Block social trackers
  - Block other other trackers
  - Block web fonts

Firefox for iOS is now available in the US iOS store.

"Angler" Exploit Kit being used in new multi-faceted drive-by campaign

- https://heimdalsecurity.com/blog/security-alert-angler-exploit-kit-spreads-cryptowall-4-0-via-new-drive-campaign/
- Angler is the kit we've seen being distributed by malicious adware
- NOW this has switched to infecting vulnerable webservers...
- New campaign is multi-payload
- The first payload consists of the notorious data thief "Pony", which systematically harvests all usable usernames and passwords from the infected system and sends them to a series of Control & Command servers controlled by the attackers.
- Next, Angler is dropped onto the machine:

- The Angler exploit kit scans for vulnerabilities in popular third party software and in insecure Microsoft Windows processes if the system hasn't been updated. Once the security holes are identified, Angler exploits them and force-feeds CryptoWall 4.0 into the victim's system.
- A/V detection is extremely low for this new campaign.
- FBI estimates that CryptoWall is costing victims about $18 annually.

SpinRite

From: Jeff Barr
Subject: SpinRite saves the Walking Dead

Thanks Steve a a wonderful product. Long time Security now listener yadda yadda. I have been using SpinRite for years running it on all my hard drives every year or so and nothing seems to be happening... just like it should.

A couple weeks ago I finished DVR recording the latest season of walking dead on my Dish network VIP 722k DVR. All 8 episodes ready for a weekend of dead fun watching. The DVR got unplugged for some reason -- probably the dog -- but that is not important. When it powered back up I was presented the error of 'Hard Drive failed. Call for support.' Well a call to support told me to return the unit for replacement and there was nothing that could be done. Returning the DVR would loose ALL my shows with over 30 hours of fine quality HD TV. Unacceptable.

I do not endorse opening a Dish DVR, they are a cranky company but there were no 'warranty void' stickers on my box so who will know? I opened it up and extracted the hard drive. A normal everyday Segate SATA hard drive. I plugged it into my SpinRite machine and fired it up. SpinRite grudgingly reported no devices connected. I investigated. The BIOS registered the drive but every time I ran SpinRite there was no device. The internet told me there are some tricks with Dish drives. Use power from the DVR and SATA from the computer. Several power up sequences with swapping cables. None of these worked for me.

Finally with little hope left I downloaded and created a Ubuntu boot USB stick, and fired up for one last try. Using the hdparm tool I unlocked the 'power-up in stand-by mode' on the drive. # hdparm -S 0 /dev/sda. After that, I poked around a little bit on the drive in linux and found plenty of files and directories with all but cryptic names. With my task complete, I booted my SpinRite CD yet again and hoped for the best. This time SpinRite found the drive and was happy to scan all 4 partitions. After running for 6 hours on the 500gig drive, it marked 4 sectors as unrecoverable but at least it ran and recovered everything else. I returned the drive to the DVR unit and waited for the eternal dish power up sequence.

The unit booted and all my TV shows are back. I then spent the weekend watching Walking dead and I am now all caught up. I don't know if you mentioned Dish network hard drives before and it took a bit of 'above and beyond' to get the drive visible... but hoooray it saved another drive!!! I am now transferring all important shows to portable hard drive and will send this unit back.

Thanks again for bringing the dead back to life.

Jeff
Tempe Arizona

Miscellany

The teenager behind the drone gun now has a drone-mounted flamethrower
"(But can it baste?)"
http://www.theverge.com/2015/12/8/9871732/drone-flamethrower-austin-haughwout
http://www.theverge.com/2015/7/16/8976337/drones-quadcopters-handguns-legal
<quote> This isn't the first video we've seen of a firearm attached to a consumer-grade drone, but it is the most convincing. The 14-second clip, uploaded to YouTube last Friday, claims to show a "homemade multirotor with a semiautomatic handgun mounted on it." The drone fires four times, with the recoil from each shot pushing it backwards in the air. If the footage is real, then the craft is certainly illegal — at least from the perspective of the Federal Aviation Authority (FAA), which regulates aircraft and drones.
There have been fakes before
<The Verge> [But] While the FAA certainly doesn't want people mounting guns on quadcopters, there's no reason that people might try to claim this activity as their right. Does the Second Amendment apply to drones with guns? Legal scholars have already investigated similar claims covering robotic weapons, for example, with one law clerk, Dan Terzian, suggesting in a 2012 paper [titled] "The Right to Bear (Robotic) Arms" that there is a "very real possibility of robots being [defined as] arms under current Second Amendment doctrine." Presumably the same interpretation might also cover drones.

Wells Fargo Login
Many people are using the 14-character password, so I think Leo's suggestion that something odd was amiss is most likely correct.

LibSodium v1.0.6 WOW!!
http://doc.libsodium.org/internals/roadmap.html

Giving Law Enforcement the (wrong) finger...
via: moriturimax (@moriturimax)
One thing about the podcast where A panic finger was mentioned re:law enforcement. If they wanted to make sure you were using the correct finger, couldn’t they lift your fingerprint from the Home button/sensor and compare them? Overkill maybe, but they DO do that stuff for a living.
Cheers, thanks again.

Number of Primes under 2^1024 is ~2.53274×10^305
(And, by the way... '9' is definitely NOT prime! <g>)
http://www.wolframalpha.com/input/?i=number+of+primes+less+than+2^1024

Speaking of "Aluminum"
Infinity Hammer @infinity_hammer
Something that came to mind when you and Leo were discussing the number of syllables in the word "aluminum". I noticed that you often say the word "mischievous" with four syllables as if there were an "i" after the "v". :-) Love your podcast.

"Childhood's End" / Starting NEXT Monday -- 3-night miniseries on SyFy
Arthur C. Clarke, 1953
And the official kick off of The Expanse

Steve's Sci-Fi Reading Guide:
http://bit.ly/sgscifi

Auralux was a huge smash.
"Monument Valley" is FREE... until MIDNIGHT TONIGHT!
http://www.monumentvalleygame.com/
Initial release April 3, 2014
Developer: Ustwo
Android, iOS, Windows Phone
Free App Timing:
Barry Wallis (@BarryWallis)
Yes, Monument Valley is still free. There is generally a new free app every week starting on Thursday evening (PST) and it stays free until the next Thursday. If I remember correctly, there is no new free app during the Christmas holiday.

Consider using Outlook when iOS Mail says "This message has no content"

Next Week...

The Moral Character of Cryptographic Work
Author: Phillip Rogaway / Date: December 1, 2015
http://web.cs.ucdavis.edu/~rogaway/papers/moral.html
Philip's paper was written to accompany his invited talk at Asiacrypt 2015.
It is not a standard research paper.
The talk was delivered on December 2, 2015, in Auckland, New Zealand.

Abstract: Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plea for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.