Security Now! #570 - 07-26-16

Q&A #238

This week on Security Now!

- Apple gets Stagefright, is Russia trying to influence the US presidential election?, Microsoft's battles and wins against U.S. privacy overreach, Grace Hopper (who coined the term "software bug") brilliantly demonstrates “a nanosecond”, a bug-fix update to pfSense, a "doing it weird" look at the CUJO security appliance, a bunch of errata, a bit of miscellany, and a DOZEN notes and questions from our listeners.

Star Trek “Beyond”

An engaging action film set in our JJ Abrams rebooted Star Trek universe

Security News

Cisco's Talos group discovers & privately reports a "Stagefright" like bug in iOS & OS X.
http://blog.talosintel.com/2016/07/apple-image-rce.html
Tyler Bohan of Cisco Talos discovered FIVE remote code execution vulnerabilities present in the image rendering code of OS X.

- **Tagged Image File Format (TIFF) (CVE-2016-4631)**
  The Tagged Image File Format (TIFF) is a file format that is popular with graphic artists, photographers and the publishing industry because of its ability to store images in a lossless format. TIFF was created to try to establish a common scanned image file format in the mid 1980s. Cisco Talos has discovered a vulnerability in the way in which the Image I/O API parses and handles tiled TIFF image files. When rendered by applications that use the Image I/O API, a specially crafted TIFF image file can be used to create a heap based buffer overflow and ultimately achieve remote code execution on vulnerable systems and devices.

  This vulnerability is especially concerning as it can be triggered in any application that makes use of the Apple Image I/O API when rendering tiled TIFF images. This means that an attacker could deliver a payload that successfully exploits this vulnerability using a wide range of potential attack vectors including iMessages, malicious web pages, MMS messages, or other malicious file attachments opened by any application that makes use of the Apple Image I/O API for rendering these types of files.

  Furthermore, depending on the delivery method chosen by an attacker, this vulnerability is potentially exploitable through methods that do not require explicit user interaction since many applications (i.e. iMessage) automatically attempt to render images when they are received in their default configurations. As this vulnerability affects both OS X 10.11.5 and iOS 9.3.2 and is believed to be present in all previous versions, the number of affected devices is significant.

- **OpenEXR File Format (CVE-2016-4629, CVE-2016-4630)**

- **Digital Asset Exchange File Format (CVE-2016-1850)**

- **BMP File Format (CVE-2016-4637)**
  The BMP file format is both long standing, and has a fairly straightforward structure. The BMP file header contains information about the size, layout, and type of the image. A vulnerability exists within the way that the height property of an image is handled. This can be exploited when a specially crafted BMP image file is saved, then opened and part of the size information is manipulated. The exploit leads to an out of bounds write resulting in remote code execution when opened in any application using the Apple Core Graphics API.

Conclusion (paraphrasing a bit) : Image files are an excellent vector for attacks since they can be easily distributed over web or email traffic without raising the suspicion of the recipient.

These vulnerabilities are all the more dangerous because Apple Core Graphics API, Scene Kit and Image I/O are used widely by software on the Apple OS X platform.

Organizations should patch software to the latest release in order to resolve these vulnerabilities. Additionally, organizations may wish to consider blocking files at network gateways if the file is of a type that is never, or very rarely, going to be encountered within the legitimate business of the organization. (e.g. TIFF files!)

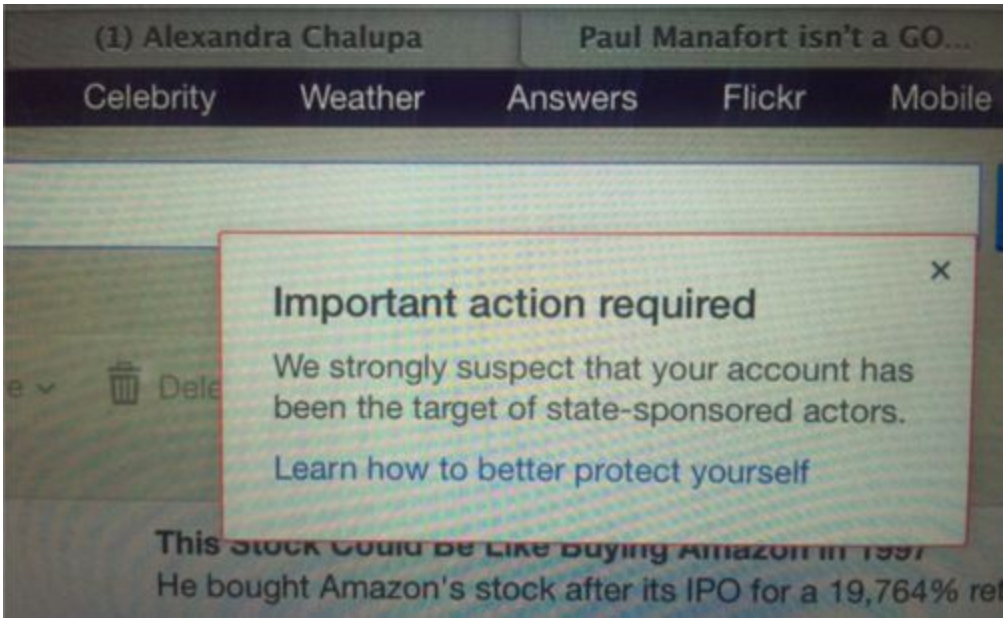
- iOS before v9.3.3 -or- OS X before v10.11.6
- Note that NONE of my devices offered to update themselves.

Russia reputed to have hacked into a DNC staffer's eMail account and involving itself in the US election outcome.

- Multiple analysts confirm that Russian state actors penetrated DNC eMail.
- The news relating to these eMail items was published by Wikileaks.
- Wikileaks' Julian Assange refuses to attribute the source of their documents, Russian or otherwise.
- Michael Isikof, respected reporter
    - https://www.yahoo.com/news/exclusive-hacked-emails-of-dnc-oppo-researcher-point-to-russians-and-wider-penetration-154121061.html

  Just weeks after she started preparing opposition research files on Donald Trump's campaign chairman Paul Manafort last spring, Democratic National Committee consultant Alexandra Chalupa got an alarming message when she logged into her personal Yahoo email account.

  "Important action required," read a pop-up box from a Yahoo security team that is informally known as "the Paranoids." "We strongly suspect that your account has been the target of state-sponsored actors."



["Quickly??" Huh?] Chalupa — who had been drafting memos and writing emails about Manafort's connection to pro-Russian political leaders in Ukraine — quickly alerted top DNC officials. "Since I started digging into Manafort, ***these messages have been a daily occurrence on my Yahoo account despite changing my password often."***

A Yahoo spokesman said the pop-up warning to Chalupa "appears to be one of our notifications" and said it was consistent with a new policy announced by Yahoo on its Tumblr page last December to notify customers when it has **strong evidence** of "state sponsored" cyberattacks. Bob Lord, the company's Chief Information Security Officer wrote in the Tumblr post: "Rest assured, we only send these notifications of suspected attacks by state-sponsored actors when we have a high degree of confidence."

Microsoft's battle against US Government law enforcement overreach
https://www.washingtonpost.com/news/the-switch/wp/2016/07/14/microsoft-just-won-a-huge-legal-victory-about-email-privacy/

- The Second Circuit Court of Appeals (New York) sided with Microsoft in a case over whether the U.S. government could force the tech giant and other companies to hand over customer emails stored overseas.

- The decision reverses the original 2014 court order requiring Microsoft to turn over email content stored on a server in Ireland.

- The original warrant that sparked the legal showdown was for emails connected to a narcotics case.

- Judge Susan Carney found that the federal "Stored Communications Act" only applies to data stored in the United States — and thus can't be used to force a company to produce information from servers outside the country.

- Now, with their original warrant invalidated, the government must proceed through a much lengthier process set up through a mutual legal assistance treaty with the Irish government to obtain the data.

- However... Ireland filed a brief supporting Microsoft in the case, as did many tech companies, including Apple and Cisco.

- Privacy advocates celebrated the decision. The EFF wrote: "This is a groundbreaking decision that helps protect privacy rights around the world."

- In her reporting of this for the Washington Post, Andrea Peterson noted: "The government was less enthusiastic."

- After the ruling, Andrea interviewed Microsoft's chief legal officer, Brad Smith:
Andrea: "Tell me about the case and what it means for the average user?"

- Brad: "The case started when Microsoft received a search warrant three years ago and we found that the email the warrant was seeking what was stored on our server computers at our data center in Ireland. We store email in a data center that is close to our customers.

  We contested the search warrant because we believe that U.S. search warrants don't reach beyond U.S. territory -- that's the traditional legal rule for search warrants, and that's what the 2nd Circuit Court of Appeals concluded.

  It matters greatly to customers who don't live in the United States. One of the things that we've found as a company is that our customers not only care about their privacy rights, but they also want their privacy rights to be protected by their own privacy laws. That won't happen if a foreign government unilaterally can reach across a border and simply obtain email and demand that it be brought back."

- Microsoft has also been pushing back, along with Google, arguing that the U.S. constitution's first amendment give companies the right to publish more information about how many U.S. National Security Letters and orders they receive and how many user accounts are affected.

(((VIDEO 2:07))) Grace Hopper explains "nano" and "micro" seconds.
http://youtu.be/JEpsKnWZrJ8
(Thanks Mementh!)

pfSense updated to v2.3.2
https://blog.pfsense.org/?p=2108
This release includes fixes for 60 bugs, 8 features and 2 todo items completed.
Details: https://redmine.pfsense.org/projects/pfsense/issues?query_id=53

Doing it wrong?... or "Doing it weird!" (either way, not on my network)
CUJO - "How does CUJO get access to all the packets by just plugging in to my router?"
https://support.getcujo.com/support/solutions/articles/9000037417-how-does-cujo-get-access-to-all-the-packets-by-just-plugging-in-to-my-router-
https://www.getcujo.com/

Q: I have a highly customized router based on WRT, so I am curious how it is going to get access to all the packets on my switched network without me having to make changes to my router settings?

A: The CUJO appliance works in one of two modes. Our "Gateway" mode, where you plug it into your router with a single ethernet cable or our Bridge mode, where it sits between your modem/router and switch. Our Gateway mode works by intercepting packets via an ARP mechanism. This is how we achieve our "simple, plug-n-play" goal, for the average Joe. Our Bridge mode works as you would expect - because it sits in the middle of a modem/router and a switch, it's physically in the middle.
Once the CUJO is logically or physically in the middle, we sample metadata from your network's

connections (using NetFlow). The metadata is strictly src/dest IPs and ports, bandwidth, packet count and connection states. We do NOT perform Deep Packet Inspection as it is too intrusive and has a pretty big performance penalty for us. These samples are hashed and sent to the CUJO cloud over an encrypted channel. In the cloud is where we do the heavy lifting.

Errata

Ubiquity EdgeRouter DOES support OpenVPN from the CLI.
(It's reportedly running Debian Linux.)
https://help.ubnt.com/hc/en-us/articles/217569187-EdgeRouter-OpenVPN-Server-with-TLS-and-Multiple-WAN

Mark (mark) / 7/20/16, 9:25 AM
Hi Steve. Correction? For SpinRite to fix raid 6 array. Wouldn't it need to repair last drive that failed?? Data on previous failed would be out of date. Mark

Martin Yirrell / 7/20/16, 3:59 AM
The Daleks are not robots but malevolent aliens that use a machine to live/travel

Gary Marriott / @ramriot
Hi Steve,
Facebook messenger. Because Facebook is the custodian of the remote key that recovers the local decryption key for message logs, this opens them up to being compelled by deception or court order to release that key to expose a person's local message logs. Even if the message logs included e3e encrypted messages.

SQRL

(end of a GRC newsgroup post)
> All right - sounds good. It could get annoying to have to enter the entire SUPER LONG
> COMPLICATED password every time my wife and I switch active SQRL user, X times a day!

Remember that the classic "SUPER LONG/COMPLICATED" password logic requirement is ***significantly*** changed with SQRL...

In the traditional non-SQRL model, your remote web account is inherently exposed to the entire public Internet. So it's only the secret of your username and password that prevents ANYONE in the world from obtaining free reign to your online account. So THAT is what sets the requirement for strong password protection.

But none of that remains true with SQRL.

With SQRL, physical access to your SQRL cryptographic identity is the FIRST requirement which CANNOT be bypassed. NOTHING other than a distant derivative of your SQRL identity ever transits the wire. So unlike with passwords, your SQRL identity cannot be obtained from monitoring your logon traffic.
This is an underappreciated aspect of SQRL: The fact that we are authenticating LOCALLY to our

encrypted identity, by briefly decrypting it, rather than globally to a publicly accessible service, represents a HUGE difference in threat models.

Consequently, our SQRL passwords ONLY need to prevent the *use* of our local SQRL identity by someone who can also first obtain *access* to it.

A 2" x 2" SQRL Sticker from "StickerMule" ($2.70)
http://bit.ly/2anI6lP
Credit Card or PayPal

Miscellany

"Bob in Santa Barbara"
Niacinamide: Search "UPC 021078005063" and "021078005063"

StarTrek "Beyond"
IMDB 7.8/10
A straight-up action movie set in our rebooted Star Trek universe.

Eric Ebert (@EricEbert13) tweeted:
@SGgrc How do you feel about season 2 of Mr. Robot so far?
After thinking about how to best describe my feelings, I replied: "Put it this way… I'm only still watching because season 1 was so amazing."

SpinRite

Ralph Griesenbeck / @RandomGravy
In a recent SN episode you recommended looking at the SMART screen in SpinRite. However that only works if it's supported in BIOS. In my experience the systems supporting SMART in BIOS are not that common. Even if SMART data is available interpretation is a bit of an art as each drive maker has different implementations. Am I missing something?

Hey Ralph,
Some BIOSes can and do support SMART probing. But SpinRite does its own directly to the hardware, continuously during operation. So it does have access to the drive's SMART data even when the BIOS is "not so SMART"

SpinRite also performs some SMART interpretation for the user and succeeds in eliminating some of the drive-to-drive variations, though you're right that differences between drives can be confusing.

https://www.grc.com/sr/smart.htm
https://www.grc.com/sr/smart-studymode.htm