Security Now! #616 - 06-13-17

Things are getting worse

This week on Security Now!

This week we discuss clever malware hiding its social media communications, the NSA documents the Russian election hacking two-factor authentication bypass, meanwhile, other Russian attackers leverage Google's own infrastructure to hide their spoofing, Tavis finds more problems in Microsoft's anti-malware protection, a cryptocurrency stealing malware, more concerns over widespread Internet-connected camera design, malware found to be exploiting Intel's AMT motherboard features, the new danger of mouse-cursor hovering, Apple's iCloud sync security claims, Azure changes their CA, a bunch of catch-up miscellany and a bit of closing the loop feedback from our listeners.

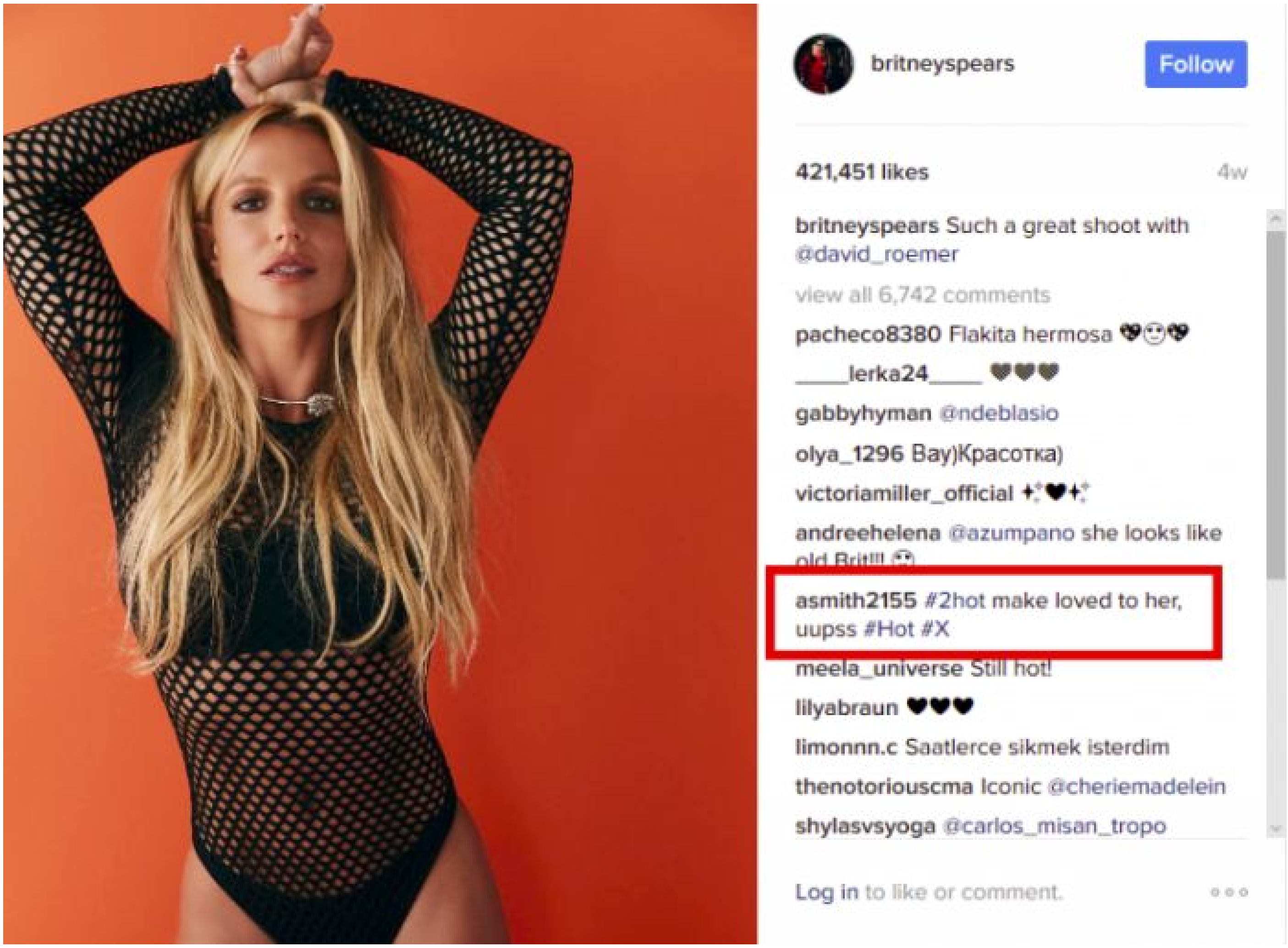
Our Picture of the Week

Windows for Warships

Security News

Social media sites are being used as stealthy malware forwarding points
https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

Check this out…



britneyspears

421,451 likes 4w

britneyspears Such a great shoot with @david_roemer

view all 6,742 comments

pacheco8380 Flakita hermosa ♥☺♥

____lerka24____ ♥♥♥

gabbyhyman @ndeblasio

olya_1296 Вау)Красотка)

victoriamiller_official ✨♥✨

andreehelena @azumpano she looks like old Brit!!! 😲

asmith2155 #2hot make loved to her, uupss #Hot #X

meela_universe Still hot!

lilyabraun ♥♥♥

limonnn.c Saatlerce sikmek isterdim

thenotoriouscma Iconic @cheriemadelein

shylasvsyoga @carlos_misan_tropo

Log in to like or comment.

The malware examines each photo's comment. It computes a custom hash value. If the hash matches 183, it then runs a regular expression on the comment to obtain the path of the bit.ly URL:

```
(?:\\u200d(?:#|@)(\\w)
```

Looking at the photo's comments, there was only one for which the hash matches 183. This comment was posted on February 6, while the original photo was posted in early January.

Taking the comment and running it through the regex, you get the following bit.ly URL:
http://bit.ly/2kdhuHX

Looking a bit more closely at the regular expression, we see it is looking for either `@|#` or the Unicode character `\200d`. This character is actually a non-printable character called 'Zero Width Joiner', normally used to separate emojis.

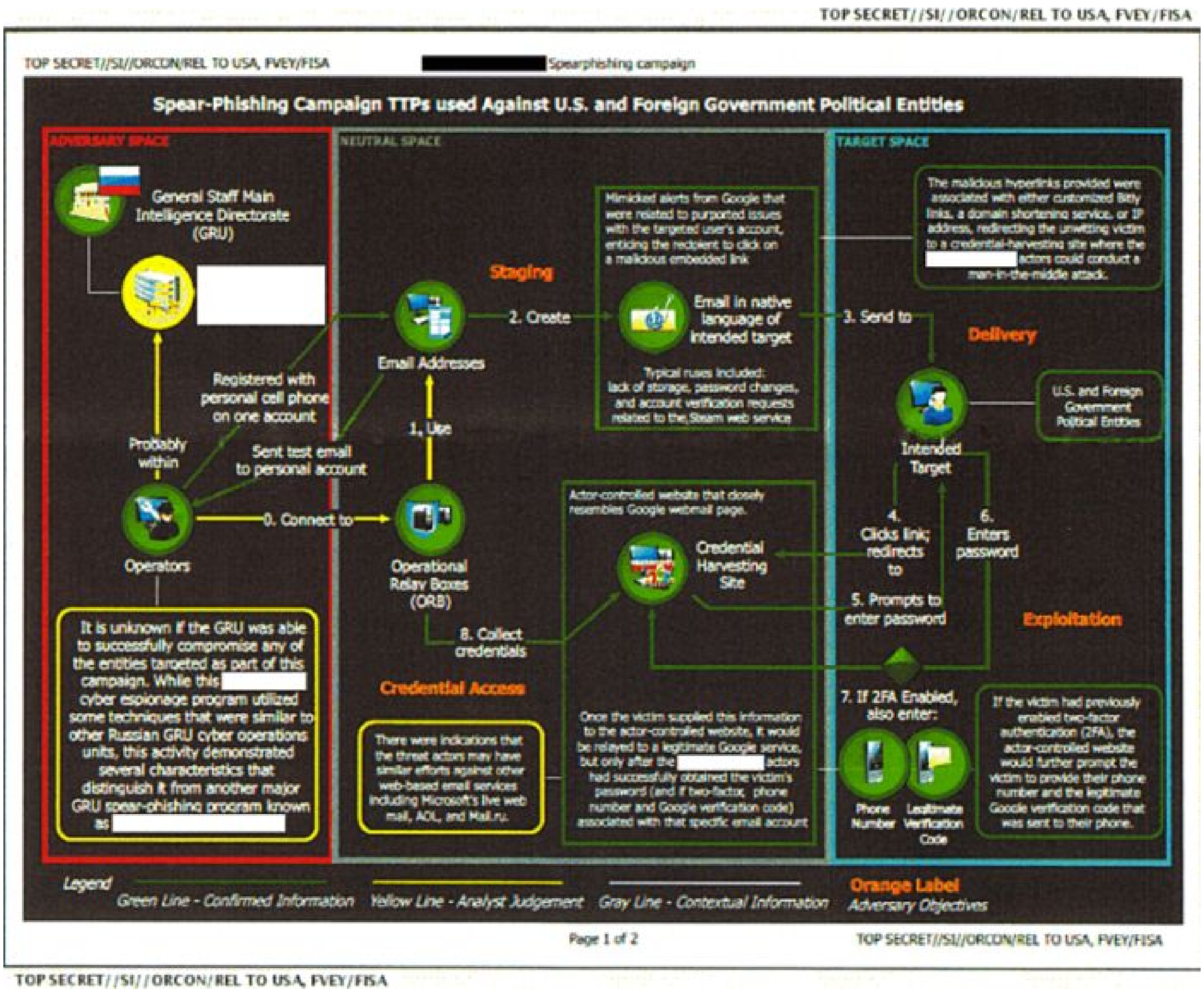
Pasting the actual comment or looking at its source, you can see that this character precedes each character that makes the path of the bit.ly URL:

```
smith2155<200d>#2hot ma<200d>ke lovei<200d>d to <200d>her, <200d>uupss
<200d>#Hot <200d>#X
```

When resolving this shortened link, it leads to `static.travelclothes.org/dolR_1ert.php` , which was used in the past as a watering hole C&C by the Turla crew.

The moral of this story?... As with other forms of steganography, it is not be feasible to attempt to examine public media for hidden meaning. It will only only be possible to find the hidden content by discovering the endpoints that access the content and then look where they are pointing.

The leaked NSA report detailing the way Russian attackers attempted to attack the 2016 US election revealed an interesting bypass for Two Factor Authentication: Just Ask...



TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA [redacted] Spearphishing campaign

Spear-Phishing Campaign TTPs used Against U.S. and Foreign Government Political Entities

ADVERSARY SPACE
NEUTRAL SPACE
TARGET SPACE
General Staff Main Intelligence Directorate (GRU)
[redacted]
Probably within
Registered with personal cell phone on one account
Sent test email to personal account
Operators
0. Connect to
Operational Relay Boxes (ORB)
1. Use
Email Addresses
Staging
2. Create
Email in native language of intended target
3. Send to
Delivery
Intended Target
U.S. and Foreign Government Political Entities
4. Clicks link; redirects to
Credential Harvesting Site
5. Prompts to enter password
6. Enters password
Exploitation
7. If 2FA Enabled, also enter:
Phone Number
Legitimate Verification Code
8. Collect credentials
Credential Access

Mimicked alerts from Google that were related to purported issues with the targeted user's account, enticing the recipient to click on a malicious embedded link

Typical ruses included: lack of storage, password changes, and account verification requests related to the,Steam web service

The malicious hyperlinks provided were associated with either customized Bitly links, a domain shortening service, or IP address, redirecting the unwitting victim to a credential-harvesting site where the [redacted] actors could conduct a man-in-the-middle attack.

Actor-controlled website that closely resembles Google webmail page.

It is unknown if the GRU was able to successfully compromise any of the entities targeted as part of this campaign. While this [redacted] cyber espionage program utilized some techniques that were similar to other Russian GRU cyber operations units, this activity demonstrated several characteristics that distinguish it from another major GRU spear-phishing program known as [redacted]

There were indications that the threat actors may have similar efforts against other web-based email services including Microsoft's live web mail, AOL, and Mail.ru.

Once the victim supplied this information to the actor-controlled website, it would be relayed to a legitimate Google service, but only after the [redacted] actors had successfully obtained the victim's password (and if two-factor, phone number and Google verification code) associated with that specific email account

If the victim had previously enabled two-factor authentication (2FA), the actor-controlled website would further prompt the victim to provide their phone number and the legitimate Google verification code that was sent to their phone.

Legend
Green Line - Confirmed Information
Yellow Line - Analyst Judgement
Gray Line - Contextual Information
Orange Label
Adversary Objectives

Page 1 of 2

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

The slide in the NSA report says: “If the victim had previously enabled two-factor authentication (2FA) the actor-controlled website would further prompt the victim to provide their phone number and their legitimate Google verification code that was sent to their phone."

In other words, after tricking victims into entering their email and password into a fake Google site, the hackers would find that some victims had 2FA set up on their accounts. As we know, this meant that even armed with the username and password, attackers were unable to gain access to the Gmail accounts in question — that is… unless they could get the verification codes as well. So they just straight up asked for them.

The NSA slide states: "Once the victim supplied this information to the actor-controlled website, it would be relayed to a legitimate Google service, but only after the attackers had successfully obtained the victim's password (and if two-factor, phone number and Google verification code) associated with that specific email account."

Once access was gained to the accounts, which reportedly belonged to an electronic-voting vendor, the hackers would then email election officials from the hacked accounts and attempt to trick those same officials into opening script-laden Word docs that would compromise their computers.

It's an elaborate bit of spear phishing, and it reminds us that no matter what digital security practices we put in place, we can all still slip up.

This is the class of worrisome site spoofing / MITM attacks I’ve just spent a month working on in SQRL. A SQRL feature was redefined from optional and maybe to be used in the future to “mandatory in v1.0” in the spec. And it COMPLETELY prevents ALL of these sorts of attacks.

Russian Hackers Are Using Google's Own Infrastructure to Hack Gmail Users
https://motherboard.vice.com/en_us/article/russian-hackers-are-using-googles-own-infrastructure-to-hack-gmail-users

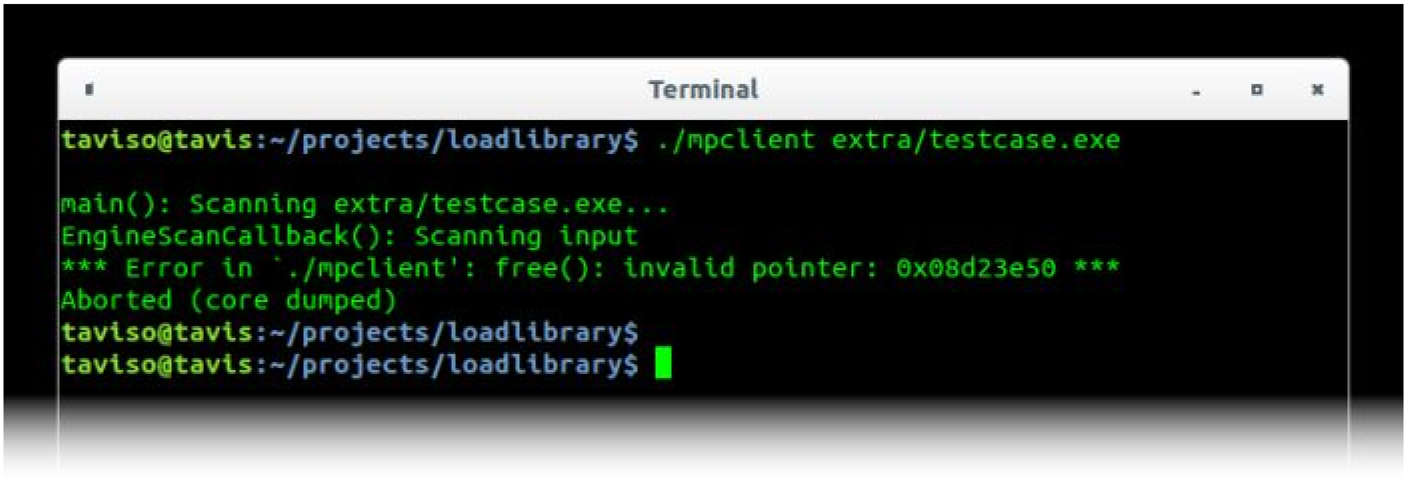
Google's Accelerated Mobile Pages -- AMP -- is a Google service originally designed to speed up web pages on mobile, especially for publishers. It operates by caching a copy of a website's page on Google's servers.

The attackers, using a spear phishing campaign, sent extremely well-formed and authentic appearing eMail, apparently from Google. The eMail explained that someonehad attempted to logon with the user’s password and they would need to change their password.

The eMail contained a big friendly Googleish “Change Your Password” button… and if even a savvy user were to hover their mouse over the button to display its underlying link URL, they would see: https://www.google.com/amp/tiny.cc/63q6iy   In other words, a totally legitimate looking, secure (https://) link to within Google. However, the page that link redirects to is another forgery -- being unwittingly hosted by Google themselves -- thanks to the clever abuse of Google’s Accelerate Mobile Pages facility.

Whoops.

Tavis Ormandy (@taviso) 9:55am · 7 Jun 2017 · Twitter Web Client
Sigh, more critical remote mpengine vulns. Found on Linux then reproduced on Windows, full report on the way. This needs to be sandboxed.



```
taviso@tavis:~/projects/loadlibrary$ ./mpclient extra/testcase.exe

main(): Scanning extra/testcase.exe...
EngineScanCallback(): Scanning input
*** Error in `./mpclient': free(): invalid pointer: 0x08d23e50 ***
Aborted (core dumped)
taviso@tavis:~/projects/loadlibrary$
taviso@tavis:~/projects/loadlibrary$
```

Previously, on three separate occasions Tavis found problems in Microsoft's Malware Protection Engine, which is common to all of their platforms. He found:

- Windows MsMpEng Type Confusion
    - MPEngine MsMpEng in Microsoft Windows 8, 8.1, 10, Windows Server, SCEP, Microsoft Security Essentials, and more suffers from a remotely exploitable type confusion.

    - Remenber that the "Type Confusion" bug was remotely wormable and Microsoft issued an emergency out-of-cycle patch to fix it.

- Microsoft MsMpEng UIF Decoder Denial Of Service
    - Microsoft MsMpEng suffers from an issue where the UIF decoder will spin forever processing sparse blocks.

- Microsoft MsMpEng Privilege Escalation
    - Microsoft MsMpEng suffers from multiple privilege escalation vulnerabilities

All of this has come about after Tavis wrote "LoadLibrary" -- a tool to allow Windows DLLs to be loaded into Linux for examination. It is NOT a WINE replacement. But it did allow Tavis to port the Microsoft Windows Defender DLLs to Linux, where he then used fuzzing tools to locate previously unknown vulnerabilities.

As Tavis writes: "The intention is to allow scalable and efficient fuzzing of self-contained Windows libraries on Linux. Good candidates might be video codecs, decompression libraries, virus scanners, image decoders, and so on."

As to "why", Tavis writes: "Distributed, scalable fuzzing on Windows can be challenging and inefficient. This is especially true for endpoint security products, which use complex interconnected components that span across kernel and user space. This often requires spinning

up an entire virtualized Windows environment to fuzz them or collect coverage data.
This is less of a problem on Linux, and I've found that porting components of Windows Antivirus products to Linux is often possible. This allows me to run the code I'm testing in minimal containers with very little overhead, and easily scale up testing.

This is just personal opinion, but I also think Linux has better tools. ¯_(ツ)_/¯

"LoadLibrary" is up on Github: https://github.com/taviso/loadlibrary

---

Bitcoin Malware Changes Destination Wallet To Steal 13 BTC
https://cointelegraph.com/news/bitcoin-malware-changes-destination-wallet-to-steal-13-btc

Another timely lesson in crypto security comes as a user reports malware stealing 13 Bitcoins by automatically replacing their destination address.

<paraphrasing from the report>
"I copy/pasted a BTC address into electrum and confirmed the bitcoin transaction. A few minutes later I checked with the recipient to verify that it had appeared in his wallet. It hadn't. Somehow it was sent to the wrong address."

"I checked all browser windows, private messages, chat histories. I do not know this address that grabbed the 13 BTC."

When this mystery wa shared with knowledgeable users on Reddit, they pointed out that the address was almost certainly changed by malware… Specifically a clipboard-altering program that has been in production for several years. This malware surreptitiously monitors the system clipboard the the appearance of a destination bitcoin address and immediately and silently replaces it with its own.

The 13 BTC transaction to the presumed malware operators has since been confirmed, despite petitions to major mining pools.

(And note that these days, 13 BTC is no small bit of change! $35,555 currently. Gone!!)

F-Secure report documents 18 different vulnerabilities in a line of Internet cameras
(Including hard-coded default login credentials that cannot be changed.)
http://images.news.f-secure.com/Web/FSecure/%7B43df9e0d-20a8-404a-86d0-70dcca00b6e5%7D_vulnerabilities-in-foscam-IP-cameras_report.pdf

Researchers at F-Secure documented 18 vulnerabilities that the manufacturer has not fixed despite being alerted to them several months ago. All of the flaws were confirmed in a camera marketed under the Opticam i5 HD brand. A smaller number of the vulnerabilities were also found in the Foscam C2.

The report noted that the weaknesses are likely to exist in many other camera models Foscam manufactures and sells under other brand names.

F-Secure wrote: “The sheer number of vulnerabilities offers an attacker multiple alternatives in compromising the device. Among the discovered vulnerabilities are insecure default credentials and hard-coded credentials, both of which make it trivial for an attacker to gain unauthorized access. Other vulnerabilities allow for remote command injection by an attacker. World-writeable files and directories allow an attacker to modify the code and to gain root privileges. Hidden Telnet functionality allows an attacker to use Telnet to discover additional vulnerabilities in the device and within the surrounding network. In addition, the device’s “firewall” doesn’t behave as a firewall, and it also discloses information about the validity of credentials.

Dan Goodin’s excellent reporting in ArsTechnica…
The flaws allow for a wide range of hacks, including using the Internet-connected cameras to participate with other infected devices in distributed denial-of-service attacks, accessing private videos, and compromising other devices connected to the same local network. The vulnerabilities are compounded by the ability to permanently replace the normal firmware controlling the camera with malicious firmware that can survive restarts without being detected.

One example of three vulnerabilities disclosed in the report: the cameras have (1) a built-in file transfer protocol server that contains a hard-coded account password (an empty password, by the way) that can't be changed by the user, (2) a hidden and undocumented telnet function that allows attackers to expand the device capabilities, and (3) incorrect permissions assigned to programming scripts that run each time the device starts.

Hackers could exploit all three of these flaws in a way "to allow the attacker persistent remote access to the device," the report explained. "The empty password on the FTP user account can be used to log in. The hidden Telnet functionality can then be activated. After this, the attacker can access the world-writable (non-restricted) file that controls which programs run on boot, and the attacker may add his own to the list. This allows the attacker persistent access, even if the device is rebooted. In fact, the attack requires the device to be rebooted, but there is a way to force a reboot as well."

The researchers went on to say that they notified Foscam representatives of the vulnerabilities several months ago and that, to date, the manufacturer hasn't fixed any of them. With no security updates, F-Secure declined to release proof-of-concept exploits. Besides the Foscam and Opticam brands, F-Secure said it was aware of 14 other brands used to market Foscam-made devices. They include:

- Chacon / Thomson / 7links / Opticam / Netis / Turbox / Novodio
- Ambientcam / Nexxt / Technaxx / Qcam / Ivue / Ebode / Sab

People who running one of these devices should strongly consider running them inside a dedicated local network that doesn't have access to other connected devices and can't be reached from the outside Internet. More generally speaking, all Internet-of-things users should be sure to change all default passwords and regularly check for security updates, although sadly, in this case, those precautions will provide little protection.

http://www.foscam.com/
Foscam’s website is currently offering a “Happy Fathers Day Giveaway” -- That’s right, give your old man something serious to worry about!

Microsoft's security team have discovered advanced malware using the Serial-Over-LAN (SOL) technology of the Active Management Technology (AMT) built into Intel motherboards to bypass all system firewalls and security. (Bringing new meaning to the abbreviation "SOL".)
https://www.bleepingcomputer.com/news/security/malware-uses-obscure-intel-cpu-feature-to-steal-data-and-avoid-firewalls/

As we have been increasingly covering on this podcast recently, Intel's AMT SOL is part of the Intel ME (Management Engine), an independent processor embedded within the Intel support chipsets of enterprise and other high-end motherboards.

This Intel ME runs even when the main processor is powered off. As we know, Intel incorporated their ME to provide operating system independent remote administration capability allowing companies to manage large networks of enterprise machines.

The AMT SOL is a Serial-over-Lan interface for the Intel AMT remote management feature that exposes a virtual serial interface via TCP. And because it's running inside the Intel ME, the AMT SOL interface remains up and functional even if the PC is turned off, allowing the Intel ME engine to send or receive data via TCP.

Fortunately, this Serial Over LAN functionality is NOT enabled by default. It must have previously been administratively enabled.

But Microsoft has discovered malware created by the high-end cyber-espionage group "PLATINUM" that is able to leverage Intel's AMT SOL interface to exfiltrate data from infected machines.

Microsoft hasn't indicated whether these state-sponsored hackers have found a way to enable this feature on infected hosts, or whether they just found it active and decided to use it.

When contacted by Microsoft, Intel said the PLATINUM group wasn't using any vulnerability in the Intel AMT SOL interface, but this was another case of bad guys using a technology developed for legitimate purposes to do bad things.

Thanks to the "PowerPoint Mouseover Based Downloader" which leverages Windows Powershell, simply HOVERING over a malicious link is now sufficient to takeover your computer.
https://www.dodgethissecurity.com/2017/06/02/new-powerpoint-mouseover-based-downloader-analysis-results/

This newly discovered attack does not rely upon macros, Javascript or VBA for its execution.

When the user opens the document they are presented with the text "Loading…Please wait" which is displayed as a blue hyperlink to the user. When the user mouses over the text (which is the most common way users would check the destination of a hyperlink) the underlying Powerpoint document, which defines a hover action for the link, executes PowerShell.

Now, get this: The Powershell command connects to domain "cccn.nl" to retrieve and save a file named c.php to disk as "ii.jse" in the temp folder. That file is then executed by wscript.exe and then that drops a file named “168.gop”. JavaScript then executes certutil.exe with the -decode parameter and the 168.gop as the file to decode. The result is saved in the temp folder as “484.exe”. Then “484.exe” is executed, spawning mstsc.exe to allow RDP access to the system.

After this, 484.exe was observed being renamed and saved to AppData\Roaming\Microsoft\Internet Explorer\sectcms.exe by mstsc.exe, where it gets re-executed from the new location.

Furthermore, a .bat file was written to disk then executed in cmd.exe. This bat file changes the attributes of the sectcms.exe program to hidden, read-only, system. It also deletes any of the files with extensions .txt/.exe/.gop/.log/.jse from the temp folder, thus cleaning up after itself and removing most of its obvious tracks.

All this… from the historically safe practice of simply hovering over a link in a received document.

(If anyone is interested in further exploration and experimentation, the link in the show notes is to the author’s original writeup and in one of his responses to his posting he offers a link to the entire exploit kit.)

Motherboard: Apple Is Trying To Make Your iMessages Even More Private
https://motherboard.vice.com/en_us/article/apple-is-trying-to-make-your-imessages-even-more-private

It seems to me that “Trying” is the operative word, and a bit of misdirection...

During an interview with Daring Fireball's John Gruber, Craig Federighi said that the company has figured out a way to do [cross-iDevice] syncing while still remaining unable to read your iMessages.

He said: "Our security and encryption team has been doing work over a number of years now to be able to synchronize information across your, what we call your circle of devices—all those devices that are associated with the common account—in a way that they each generate and share keys with each other that Apple does not have."

"And so, even if they store information in the cloud, it is encrypted with keys that Apple doesn't have. So [users] can put things in the cloud, they can pull stuff down from the cloud, so the cloud still serves as a conduit—and even ultimately kind of a backup for them—but only they can read it."

Motherboard writes: It is unclear exactly how Apple is able to pull this off, as there's no explanation of how this works other than from those words from Craig. The company didn't respond to a request for comment asking for clarifications. It's possible that we won't know the exact technical details until iOS 11 officially comes out later this year.

Meanwhile, cryptographers are already scratching their heads and holding their breath. Kenn White, a security and cryptography researcher, told Motherboard in an online chat: “The $6 million question: how do users recover from a forgotten iCloud password? If the answer is they cannot, that's a major [user experience] tradeoff for security. If you can, maybe via email, then it's [end-to-end] with Apple managed (derived) keys. If recovery from a forgotten iCloud password is possible *without access* to keys on a device's Secure Enclave, it's not truly e2e. It's encrypted, but decryptable by parties other than the two people communicating. In that sense, it's closer to the default security model of Telegram than that of Signal."

And… irrespective of all of that, I continue to contend that unless the user is explicitly managing (receiving and verifying) their communicating co-party’s encryption keys (as, for example, is the case with Threema), Apple remains ENTIRELY FREE to insert an additional party-line key into any or all communications. I’m not suggesting that they ARE doing so… but they DO have the capability of responding to wiretap warrants. iMessage is “many-to-many” messaging, not just one-to-one, and user’s have no visibility into precisely WHO those “many” co-parties are.

The Official Azure Key Vault Team Blog
https://blogs.technet.microsoft.com/kv/2017/04/20/azure-tls-certificates-changes/

Microsoft writes: “We know security is a top priority for you, and so is uptime of your applications. To give you additional assurance of the authenticity of Azure services, most Azure services get their SSL/TLS certificates from a known set of intermediate certificate authorities (CAs) that Microsoft operates. Microsoft publishes details of these CAs in its Certificate Practice Statement (CPS).

Some organizations configure their applications with specific CAs, using a security practice called certificate pinning. Since CAs expire and get replaced, this practice requires that the applications be updated periodically to use the latest CAs. If this is not done in time, the application may get interrupted. To make this process easy for you, Microsoft publishes new CAs well in advance of using them.

The current intermediate CAs used by Azure are due to expire in May 2018. Microsoft published a new set of CAs last year in the July 2016 revision of the CPS. Azure services will begin using these new CAs from July 27, 2017. If your organization configures your application with specific CAs, then you must ensure your applications are updated by July 27, 2017 to prevent interruption.

/////

Microsoft Azure services were previously signed by either of two intermediate certificates. They are adding four additional intermediates… and

Endpoint changes are

Original CRL distribution point:	http://cdp1.public-trust.com/CRL/Omniroot2025.crl
New CRL distribution point:	http://crl3.digicert.com/Omniroot2025.crl
OCSP	http://ocsp.digicert.com

You must ensure your app can connect to all of the above.

SpinRite

From: James Campbell
Subject: Thank you!

I upgraded one of my NAS's and decided to use the old one to setup a server at my church. The problem was, I had 13 hard disks laying around. I knew that some of them were laying around because I outgrew their capacity, and some had failed... but, alas, post it notes don't stick forever!

So... SpinRite to the rescue! Today, 13 disks fully tested, 4 with catastrophic failures that wouldn't even mount. And the remaining 9 have now all been fully verified by SpinRite. The old NAS is now stuffed with 4 matching drives and has been installed at the church.

Thanks Steve!
Jim C.

Miscellany

The Frontiers Saga:

- Andrey Hardy (@andreyhardy)
  @SGgrc Congratulations, Gibson. After years of life- and productivity-enhancing recommendations, you've ruined me with the Frontiers Saga!

- Jason Egan (@beguil3d)
  Thank you @SGgrc for introducing me to Ryk Brown's Frontiers Saga.
  I was in a serious sci-fi rut and am thoroughly enjoying the books!

Tom Cruise's "The Mummy" -- awful!

- Jack Reacher
- Mission Impossible's
- Oblivion
- Edge of Tomorrow

Ben Affleck's "The Accountant" -- awesome!

And...

- Orphan Black as started its 5th and final season
- Sense8 season 2 is out on Netflix.

Monument Valley II

- Monday before last, Monument Valley II, the sequel to the 2014 iPad game of the year.
- $5 for iOS (Android release coming soon) by Ustwo Games
- More than 30 Million downloads of the first version.
- The success of the first release put huge pressure on the original 8-person team to give the world more. But until yesterday they had only managed to create the small "Forgotten Shores" extension to the original.

- After that, the 8-person company felt burned out on the concept and wanted to do something else. But today, three years later, the company is 20 people and ALL of the new hires came to the company because they loved Monument Valley. They brought a ton of new ideas and reinvigorated the entire concept.
- Our listeners know that I most enjoy relaxing, thoughtful, cerebral and non-temporal (reflexes optional) puzzle games . Monument Valley I was wonderful and I look forward to taking my time to move through Monument Valley II.

"Flow Batteries"

- New “Instantly Rechargeable” Battery Deals a Fatal Blow to Fossil Fuels
- https://futurism.com/new-instantly-rechargeable-battery-deals-a-fatal-blow-to-fossil-fuels/

Closing The Loop

Jonathan Lloyd (@jondlloyd)

- @SGgrc Question regarding SQRL: How might a user share their credentials for a single site with someone else? Is this possible?

  I ask because MANY websites don't have robust permission systems. I still need to send or receive login info AT LEAST a few times per year.

  In any case, I thought I'd ask. I don't recall hearing this mentioned on SN before. Love the show! I try not to miss an episode.

  (((Many-to-One Mapping)))

Carl Green (@gystservices)

- @SGgrc re: travel mode for 1Password manager.
  Q: can it be en/disabled from your phone? Seems to me, they would ask you to do that...