

Security Now! #568 - 07-12-16

Q&A #237

This week on Security Now!

- Facebook Messenger, Russia's President Putin, the fate of Russian-based VPN endpoints, Russian hackers compromising iOS devices, my promised follow-up on that Lenovo SMM hack which suddenly looked a lot more worrisome, the apparent illegality of password sharing, post-quantum crypto testing in Chrome, reconsidering antivirus add-ons, Pokemon Go woes, a possible defense against CryptoMalware, news from the "Of course someone had to try this" department, miscellany including the return of Mr. Robot, Leo moves to FreeBSD, a recent pfSense facelift, Apollo assembly language source, even more... and FIVE questions from Twitter.

Their Fearless Leader (*nice shades*)



Security News

Facebook Messenger adds "Secret Conversations" -- end-to-end encryption.

https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper.pdf

- "Secret Conversations" can be selectively enabled.
- This will preclude some other features such as "chatbot" which depend upon visibility into conversations.
- Secret Conversations resides within the common Messenger App, but they use a different transport protocol, specialized on-device storage, and separate back-end infrastructure.
- The Secret Conversations threat model considers the compromise of server and networking infrastructure used by Messenger — Facebook's included. Attempts to obtain message plaintext or falsify messages by Facebook or network providers result in explicit warnings to the user. However the implicit assumption is that endpoint clients are working as designed, e.g. that they are not infected with malware.
- SC uses Signal Protocol's common open source implementation.
- Secret Conversations also incorporates new abuse-reporting features which are not present other platforms which use the Signal Protocol.
- White Paper: Key Verification
- For every secret conversation Messenger exposes in its interface both participants' identity keys (i.e. IKpk). Users may optionally verify these keys in order to ensure no man-in-the-middle attack is compromising their secret conversations. Messenger displays the 256-bit IKpk values in hexadecimal format.
- Next Week: A close look at two additional aspects: "Abuse Reporting" and "Secure Storage."

Putin vs The Internet

- Last Thursday, Russia's president Putin ordered the Federal Security Service Bureau (FSB) to produce "encryption keys" capable of decrypting all data on the internet. No one is really sure what this means exactly.
- That's just one part of the Russian government's new plan for internet surveillance, signed into law under the "anti-terrorist" bill and going into effect on July 20th.
- Some highlights are:
 - Telecom providers and "organizers of information distribution" (basically, any website) must store copies of the content of all information they transmit (including phone calls and text messages) for six months and store the metadata for three years so they can give the Kremlin whatever it wants, whenever.
 - Not only do "organizers of information distribution" have to store all transmitted information, they have to turn over "any information necessary to decrypt those messages." So, "additional coding" has to be added to all electronic messages which will function as instructions for the FSB to "decode" them.
- In announcing Mr. Putin's decision to sign the amendments into law Thursday, spokesman Dmitry Peskov told reporters that the president instructed the government to make adjustments if the measures indeed pose any "financial risks." Dmitry said: "The government will keep a close eye on how this law is implemented, and if some unpleasant consequences are discovered, the president will ask [the government] to take steps."

Private Internet Access VPN provider closing down Russian operations.

- "We Are Removing Our Russian Presence"

- To Our Beloved Users,

The Russian Government has passed a new law that mandates that every provider must log all Russian internet traffic for up to one year. We believe that due to the enforcement regime surrounding this new law, some of our Russian Servers were recently seized by Russian Authorities, without notice or any type of due process. We think it's because we are the most outspoken and only verified no-log VPN provider.

Luckily, since we do not log any traffic or session data, period, no data has been compromised. Our users are, and will always be, private and secure.

Upon learning of the above, we immediately discontinued our Russian gateways and will no longer be doing business in that region.

To make it clear, the privacy and security of our users is our number one priority. For preventative reasons, we are rotating all of our certificates. Furthermore, we're updating our client applications with improved security measures to mitigate circumstances like this in the future, on top of what is already in place. In addition, our manual configurations now support the strongest new encryption algorithms including AES-256, SHA-256 and RSA-4096.

All Private Internet Access users must update their desktop clients and our Android App at Google Play. Manual OpenVPN configurations users must also download the new config files from the client download page.

We have decided not to do business within the Russian territory. We're going to be further evaluating other countries and their policies.

In any event, we are aware that there may be times that due notice and due process are foregone. However, we do not log and are default secure against seizure.

Russian Hackers Targeting iOS Device Users with Ransom Attacks

- <http://appadvice.com/post/russian-hackers-targeting-ios-device-users-with-ransom-attacks/717660>
- A number of iOS device users in the United States and Europe have recently become victim of a scary ransom scam. Their device is placed into "lost mode", and the scammers demand a payment – anywhere from \$30 to \$50 – to unlock their iPhone or iPad.
- Compromised Apple IDs obtained through phishing or online exchanges.
- Extortion demands in Russian.
- A full factory reset and restore from backup will restore function.
- This may be another downstream consequence of the recent mega-breaches.

Lenovo...

- System Management Mode (SMM) BIOS Vulnerability
 - From a malicious app with admin privilege:
 - Firmware write protection can be disabled.
 - Safe Boot Mode can be bypassed.
 - Affected machine firmware can be altered to install permanent malicious pre-boot rootkit code.
- <https://support.lenovo.com/us/en/solutions/LEN-8324>
- Execution of code in SMM by an attacker with local administrative access
- Lenovo's Product Security Incident Response Team (PSIRT) is fully aware of the uncoordinated disclosure by an independent researcher of a BIOS vulnerability located in the System Management Mode (SMM) code that impacts certain Lenovo PC devices. Shortly after the researcher stated over social media that he would disclose a BIOS-level vulnerability in Lenovo products, Lenovo PSIRT made several unsuccessful attempts to collaborate with the researcher in advance of his publication of this information.

Since that time, Lenovo has actively undertaken its own investigation, which remains ongoing. At this point, Lenovo knows that vulnerable SMM code was provided to Lenovo by at least one of our Independent BIOS Vendors (IBVs). Independent BIOS vendors (IBVs) are software development firms that specialize in developing the customized BIOS firmware that is loaded into the PCs of original equipment manufacturers, including Lenovo. Following industry standard practice, IBVs start with the common code base created by chip vendors, such as Intel or AMD, and add additional layers of code that are specifically designed to work with a particular computer. Lenovo currently works with the industry's three largest IBVs.

The package of code with the SMM vulnerability was developed on top of a common code base provided to the IBV by Intel. Importantly, because Lenovo did not develop the vulnerable SMM code and is still in the process of determining the identity of the original author, it does not know its originally intended purpose. But, as part of the ongoing investigation, Lenovo is engaging all of its IBVs as well as Intel to identify or rule out any additional instances of the vulnerability's presence in the BIOS provided to Lenovo by other IBVs, as well as the original purpose of the vulnerable code.

- Some Yoga's -- LOTS of Thinkpads
- <http://blog.cr4.sh/>
- <https://github.com/Cr4sh/ThinkPwn>
- 07/02 - One of my followers confirmed that vulnerable code is present in his HP Pavilion laptop
- 07/05 - Alex James found vulnerable code on motherboards from GIGABYTE (Z68-UD3H, Z77X-UD5H, Z87MX-D3H, Z97-D3H and many others)
- 07/06 - Japanese researcher known as 173210 found vulnerable code in firmware of Fujitsu LIFEBOOK A574/H, other Fujitsu computers probably affected as well
- 07/07 - Dell Latitude E6430 is also vulnerable, it means that other computers from Dell might be affected as well

Share your password, go to jail:

(From the "somewhat overblown by the media" department)

- Ruling could make sharing passwords for subscription services a federal crime
- <http://www.foxnews.com/politics/2016/07/11/ruling-could-make-sharing-passwords-for-subscription-services-federal-crime.html>
- A recent federal court ruling from the 9th Circuit Court of Appeals could make sharing your passwords for subscription services -- covering everything from Netflix to HBO GO -- a federal crime punishable by prison time, wrote a judge who opposed the decision.

The ruling, pertained to a trade-secrets case, found that certain instances of sharing passwords are prosecutable under the Computer Fraud and Abuse Act (CFAA) – predominantly concerned with hacking.

The case involved David Nosal, a headhunter who left his former company Korn/Ferry and later used the password of a still-employee assistant to access the company's database and use that information at his new competing firm. According to Fusion, the defendant was convicted of hacking charges in 2013 and sentenced to one year and one day in prison. The appeals court upheld the conviction by 2-1.

One of the two judges upholding the lower court decision, Margaret McKeown, wrote: "This access falls squarely within the CFAA's prohibition on access 'without authorization,' and thus we affirm the conviction for violations under the CFAA."

However, in his minority dissenting opinion, Judge Stephen Reinhardt, argued that the case was not about hacking, but password sharing. Consequently, he argued, the ruling jeopardizes password sharing for the general public: He wrote: "[The ruling] loses sight of the anti-hacking purpose of the CFAA, and despite our warning, threatens to criminalize all sorts of innocuous conduct engaged in daily by ordinary citizens. The majority does not provide, nor do I see (writes Reinhardt), a workable line which separates the consensual password sharing in this case from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners. There simply is no limiting principle in the majority's world of lawful and unlawful password sharing."

- The concern??... If Reinhardt is right, it could place users of popular streaming sites like HBO GO and Netflix, who share their passwords, in breach of the CPAA -- and open to federal prosecution.

"HTTPS crypto's days are numbered" (?) Here's how Google wants to save it

- Coming to a browser near you, new, post-quantum crypto.
- <http://arstechnica.com/security/2016/07/https-crypto-is-on-the-brink-of-collapse-google-has-a-plan-to-fix-it/>
- "Quantum Nervousness" <https://www.cecpq1.com/>
- EC = Elliptic Curve (the Bernstein 25519) + PQ (Post-Quantum) - "New Hope" Key Agreement
- Remember... this is ONLY for asymmetric key (public key) crypto.
- <https://cryptojedi.org/papers/newhope-20160328.pdf>

Reconsidering AntiVirus

- Yahoo! News: Antivirus software is 'increasingly useless' and may make your computer less safe
- <https://ca.news.yahoo.com/antivirus-software-increasingly-useless-may-090000827.html>
- Backlash from the recent sweeping Symantec kernel filter flaw evoked a reappraisal of the cost/benefit ratio of anti-virus add-on software.
- As this news item appearing on Yahoo! News hints, the notion that perhaps the benefits no longer accrue significantly is beginning to go mainstream. What may have once been a "no brainer" for most people may be changing.
- Criminals are increasingly pursuing the weakest link in the chain... which is no longer the computer's technology... it's the end user themselves.

Pokemon Go Home

- Pokemon Go: I saw the effect for the first time during lunch today. One Verizon employee whacked his head on a tree branch while walking and staring at his screen. Another lunch party of eight "tech yuppies" all had their phone out and "up" while walking (slowly) and never put them away throughout the meal. One of the servers came out to the patio where I had eaten and was then reading and said to me "I already HATE this new stupid Pokemon thing!! EVERYONE in the restaurant is obsessed with whatever it is."

This might be a good time to audit your Google App Permissions:

- <https://security.google.com/settings/security/permissions>
- Bit.ly link of the week: <http://bit.ly/sn-568>

From: "Anonymous Sender" <anon@grc.com>

- Subject: Pokemon go app spreads droidjack malware
- Date: Mon, 11 Jul 2016 16:50:56 -0000
- See: <https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoor-pokemon-go-android-app>

A bunch of news sites can be found talking about the subject simply by Googling. I believe I have been a victim. After realizing that I was infected I factory reset my phone. However, it seems that DroidJack remains in place after a factory reset (with an asterix next to the item, why?)

See the "more" section at <http://droidjack.net/features.html>

This is a poor judgement on my part; installing an app from a third party. I should have known better.

I hope this will help anyone who listens to security now in the future.

- DroidJack is a malicious RAT (Remote Access Trojan) The DroidJack RAT is well known and has been described in the past by Symantec, Kaspersky and others. It was uploaded to a malicious file repository service at 09:19:27 UTC on July 7, 2016, less than 72 hours after the game was officially released in New Zealand and Australia.

Probably because the game had not yet been officially released globally, many wishing to access the game before it was released in their region resorted to downloading the APK from third parties. Many large media outlets provided instructions on how to download the game from third parties. Some even went further, providing instructions and encouragement for installing the APK downloaded from a third party:

"To install an APK directly you'll first have to tell your Android device to accept side-loaded apps. This can usually be done by visiting Settings, clicking into the Security area, and then enabling the "unknown sources" checkbox." <sigh>

- The Security Now lesson: When people WANT SOMETHING they will ignore the risks.
- FoMO: Fear of Missing Out.

CryptoDrop: Researchers develop a way to stop ransomware

- <http://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf>
- Researchers from the University of Florida and Villanova University claim to have found an "obvious" solution to the Encrypting Malware problem dubbed "CryptoDrop."
- <quote> "Our system is more of an early-warning system. It doesn't prevent the ransomware from starting ... it prevents the ransomware from completing its task ... so you lose only a couple of pictures or a couple of documents rather than everything that's on your hard drive, and it relieves you of the burden of having to pay the ransom."

From the "Of course someone had to try this department"... (thanks to Jeff Arthur)

- BBC News: 'Dalek' commands can hijack smartphones
 - <http://www.bbc.com/news/technology-36763902>
 - (Yes... the evil Dr. Who robots.)
- Researchers from UC Berkeley and Georgetown University have demonstrated that garbled speech commands hidden in radio or video broadcasts could be used to control smartphones without their owners being aware of what's going on.

The clips, which sound like the Daleks from Doctor Who, can be difficult for humans to understand but still trigger a phone's voice control functionality. The commands could make a smartphone share its location data, make calls and access compromised websites.

They took a series of voice commands, such as: "OK Google, call 911," and heavily distorted the audio so that it was difficult for human listeners to understand... but the Android phone still understood it loud and clear. Such low-pitched speech could be hidden among background noise and still trigger smartphone features.

One of the researchers from Georgetown said: "Our research was mostly geared towards

answering the theoretical question: is it possible to leverage the differences in how computers and humans understand speech to produce commands that could be understood by the former and not by the latter? We found that the answer to this question is yes - but there's certainly a lot more work to be done to investigate what it would take to make these attacks more practically deployable. While the attack should be considered seriously - especially given the growing popularity of voice-only interfaces such as Amazon Echo, Apple Watch and Android Wear - we aren't trying to make the case that these attacks are easy to conduct."

Miscellany

Mr. Robot returns TOMORROW!!!

Want to see more? The critically acclaimed series, which won the Golden Globe for Best Drama after its first season, returns Wednesday, July 13 at 10pm. And want to keep talking? The "Hacking Robot" post show, hosted by Andy Greenwald, premieres right afterwards on USA. Episode One was early-released... may still be floating around

Leo moves to FreeBSD.

Packages vs Ports (Binary vs Source Compilation)
"pkg upgrade"

pfSense just got a VERY nice facelift upgrade!

If you haven't logged in recently and checked... do so!! :)

Assembly Code That Took America to the Moon Now Published On GitHub

AGC - Apollo Guidance Computer

The Great North Road ... or ... the ENDLESS North Road?

A wonderful fun and engaging read... but, sheesh!

Twitter dialog with someone who just finished the Rho Agenda prequel trilogy.

SpinRite

Dave Jones / @DVJones89

Hi Steve,

I wanted to drop you a quick message to add yet another success story to your ever-growing pile of SpinRite testimonials. I'm a Software Engineer living in Edinburgh, Scotland, though I'm originally from England, where my folks still live. As I suspect will be the case for many of your listeners, I provide Tech Support for my friends and family.

On my latest visit to my parents, my Dad asked me to look at his Windows 7 laptop that, over the previous months, had slowly ground to a crashing, unresponsive halt.

Over the course of a few hours, I followed your advice to upgrade Windows Update, install Never 10 and replace 3rd party AV with Microsoft Windows Defender. All of this knowledge accumulated over many years listening to Security Now - a valuable resource, not only for security, but also for staying abreast of Windows issues (not easy when you develop exclusively in OS X).

After auditing the laptop's software, I pulled out my copy of SpinRite and set it running at Level 4 on the laptop's hard-drive. SpinRite ran for almost exactly 24 hours and, though the status screen reported no faulty sectors, I rebooted the system feeling quietly optimistic. Sure enough, SpinRite had forced the hard-drive to take a long, hard look at itself and the laptop is now running like a dream.

Thank you for your brilliant suite of tools, library of podcasts and methodical approach to problem solving.

Give my regards to Leo and his wonderful podcast network, I'll visit that studio some day! :)

Kind regards,
Dave Jones (dvjones89 in the chatroom)

P.S. Please feel free to share this on a future SN podcast, infact, I'd love it if you did :)

Q&A:

[1] - Hans Dekker / @hansdekker

@SGgrc If I keep an internet exposed web server (or e.g. a minecraft server) on a wifi guest network with limited access, am I safe?

[2] - Kyle Day / @kyleday

Hi Steve- love your SN Podcast. Highlight of my week. I have a question about Corporate Spying via inserting a certificate into a Windows user's root certificate store. I understand that I.E. and Chrome use Window's built-in certificate store, but Mozilla's Firefox uses its own. If I install FireFox on my work machine and use it for personal browsing, does that mean that it's impossible for my employer to decrypt that traffic because they don't have a certificate to MITM my FireFox traffic? Would that be a good workaround for corporate spying? Thanks!

[3] - Scott Ericsson in Milwaukee, Wisconsin posed a tricky SQL question:

Steve, SQL sounds amazing, but I think there's a problem: As I understand it, SQL auto-magically creates a unique identity for each of its users for each website they visit. But what if I want to appear as a different user at the same website? Under the Internet's present (horrific) eMail and password scheme, I can create a Gmail alias, or use another eMail account to create a second independent identity at any site I wish. But SQL would appear to lock us in to our SQL identity for each site?? Isn't this a potential problem??

[4] - "docop" / @docop29

@sggrc Steve, I have a guest wifi network at work that I use with my iPad for doing (mostly) work tasks. I have an iPhone that I never connect to the network so my private information isn't going through corporate servers. The wifi password changes every 2 weeks so I have to reconnect with my iPad...I have noticed recently though, that my iPhone also connects to the network...it seems that iOS is automatically updating the password across iCloud. Given your recent discussions about corporate appliances breaking SSL and being able to access ALL of your traffic...is this inadvertently opening up the private traffic on my phone to my corporate overlords?!?!?

[5] - Jared / @nuclear_eye

Security now question: What is the big push behind cloud computing/storage? For these services to be off site makes us more dependent on internet connectivity and puts our data at a great security risk, so it seems. I don't like the idea of depending on someone else to access my data, securing it and having access to it. I get that it is nice to be able to access from anywhere in the world but sometimes that isn't necessary. So why put stuff in the cloud? Thanks for Sprinrite - Love it. Listen to the podcast every week and love it!