Security Now! #617 - 06-20-17

When Governments React

This week on Security Now!

This week we discuss France, Britain, Japan, Germany & Russia each veering around in their Crypto Crash Cars, Wikileaks' Vault7 reveals widespread CIA WiFi router penetration, why we can no longer travel with laptops, HP printer security insanity, how long are typical passwords?, Microsoft to kill off SMBv1, the all-time mega ransomware pay out, Google to get into the whole-system backup business, hacking PCs with "Vape Pens", a bit of miscellany, and a bunch of Closing the Loop feedback with our terrific listeners.

"Lunch Order"

Thanks to the ever-wonderful and clever XKCD: https://xkcd.com/1834/

Security News

Named: The "French-British Action Plan
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/619333/french_british_action_plan_paris_13_june_2017.pdf

Terrorists, and the people they influence, are using the internet, websites, e-mail services and social networks to gather information, organise, spread propaganda and operating methods, send and receive instructions, and claim responsibility for their acts.

At a meeting in Paris on 13 June 2017, Prime Minister May and President Macron agreed to a joint UK/France initiative to ensure the internet cannot be used as a safe space for terrorists and criminals. They stressed that coordination with G7 and EU partners will be sought on these issues.

The following four points were agreed as priorities:

- 1/ Improve methods to remove illegal content from the internet
  While efforts have been observed from companies regarding removing terrorist content, we need industry to move from their current position of reactively removing content when it is notified to them, to proactively identifying content and preventing it from being made available on their platforms in the first place.

- 2/ Support the efforts of civil society organisations to promote alternative and counter-narratives. This will include efforts to:
  - Train and support those civil society actors that promote relevant counter narratives, including through the EU Internet Forum or the European Radicalisation Awareness Network (RAN);
  - Promote their web-ranking, while targeting the right audience, and redirect positive content as appropriate;
  - Better protect those civil society actors involved in developing counter narratives, including parody accounts, through, amongst other things, certification of their accounts and their inscription on a white list.

- 3/ Work together to ensure our countries can access data for investigative purposes

  - 3.1 Seek to preserve the retention and access to traffic and location data
    Under current terrorist threat levels, the ability to retain data useful to investigations remains essential.

  - 3.2 Enable subscription holders to be identified in all circumstances
    A single Internet Protocol (IP) address can be shared between hundreds of users accessing the internet or social platforms via their smartphones. The capability to identify specific users is important, particularly where suspects have accessed terrorist content.
    Proposals: Share expertise and legislative experience regarding these issues, including with EUROPOL, with a view to intensifying dialogue with industry.

- 3.3 Allow access to encrypted content
  When encryption technologies are used by criminal groups, and terrorists, it must be possible to access the content of communications and their metadata. This is not about backdoors or banning encryption, but ensuring Governments and companies develop shared solutions to this issue.
  Proposals: Share strategies on the challenge of accessing content from encrypted services, and coordinate our engagement with the major Communications Service Providers.

Japanese Prime Minister Shinzo Abe's government has just passed controversial legislation giving prosecutors the power to monitor and arrest people in the planning stages of crimes.
https://www.bloomberg.com/politics/articles/2017-06-15/abe-passes-controversial-bill-boosting-japan-surveillance-powers

After an all-night legislative session in Tokyo, lawmakers, who were deliberately delayed by the bill's opposition, voted to pass the so-called anti-conspiracy bill, controversial legislation that gives prosecutors the power to monitor and arrest people in the ***planning stages*** of crimes. The government claims this is needed to bolster counter-terrorism precautions ahead of the 2020 Tokyo Olympics.

Under the bill, terrorist groups or criminal organizations could be punished for the planning of 277 different crimes, ranging from arson to copyright violation. Critics of the legislation argue that the legislation is vague and could lead to the suppression of civil liberties and excessive state surveillance. This is also seen by many as a preamble to Abe's ambition to revise Japan's constitution.

Commenting about this a professor of political science at Sophia University in Tokyo was quoted: "This fits Abe's agenda in the run-up to a prospective national referendum on constitutional revision, and Japan's possible involvement in future wars. Both of these would require new means to control unruly citizens who object to government decisions."

Russia Stumbles Forth In Quest To Ban VPNs, Private Messenger Apps
https://www.techdirt.com/articles/20170609/09213837550/russia-stumbles-forth-quest-to-ban-vpns-private-messenger-apps.shtml

Last year Russia's parliament had introduced a new surveillance bill promising to deliver greater security to the country. But as with so many countries, the bill's effect was to do the opposite -- not only mandating new encryption backdoors, but also imposing harsh new data-retention requirements on ISPs and VPN providers. And as a result, as we covered at the time, some VPN providers, such as Private Internet Access, pulled their service from the country after being effectively outlawed and having some of their servers seized.

Now, this year, Russia hopes to deliver the killing blow to the use of VPNs and other privacy-protection tools: In part of a crackdown on anonymous journalists who have been

reporting details on many of the sordid occurrences inside the often-corrupt Russian political machinery, Russia's Information and Technology Committee has approved draft legislation that would ban anonymity on messenger apps entirely.

Expected to take effect in 2018, the new law would require messenger users to verify their identities using their phone numbers, with Russian mobile phone operators expected to assist the government with this effort.

In concert, a bill has been submitted attempting to effectively ban VPN use entirely. In Russia, broadband users have increasingly turned to VPNs to avoid the growing-list of censored websites. To help thwart such usage, the bill would not only impose steep fines on VPN providers that don't agree to block blacklisted websites, but would require ISPs to terminate these companies Internet service should they not comply:

The proposed legislation reads: "As it stands, the bill requires local telecoms watchdog Rozcomnadzor to keep a list of banned domains while identifying sites, services, and software that provide access to them. Once the bypassing services are identified, Rozcomnadzor will send a notice to their hosts, giving them a 72-hour deadline to reveal the identities of their operators. After this stage is complete, the host will be given another three days to order the people running the circumvention-capable service to stop providing access to banned domains. If the service operator fails to comply within 30 days, all Internet service providers will be required to block access to the service and its web presence, if it has one."

And... in Germany: (via Ian Beckett (@ianbeckett): photo: The London Times)

Germany to change law on encryption

David Charter Berlin

Laws to enable security services to see messages before they are encrypted by providers such as Whatsapp are being drawn up in Germany because of concerns over secret communications between Islamist terrorists.

Angela Merkel's government believes that the same balance of eavesdropping and privacy should exist in the digital age as in the analogue era of letters and phone calls. Mrs Merkel aims to put digital security on the agenda for the G20 summit that she is hosting in Hamburg next month.

Theresa May has also called for a global approach to regulating digital providers, saying during the election campaign that there should be no "safe space" for terrorist ideologies.

Germany is known as one of the countries most protective of personal privacy because of the legacy of surveillance by the Nazi regime and the Stasi secret police of communist East Germany. However, terrorism in Europe is fuelling calls for change.

British authorities were incensed that they could not access the last Whatsapp message sent by Khalid Masood, the Westminster attacker, minutes before he began his killing spree by driving into pedestrians and fatally stabbing a policeman. The messaging company, owned by Facebook, said that its service was so secure that no one but the sender and recipient could see a message, not even Whatsapp itself.

"We want messenger services to have an end-to-end encryption so that the communication of respectable citizens is undisturbed and secure," said Thomas de Maizière, the German interior minister. "Nevertheless, security authorities need the option of access under certain circumstances." That would allow the authorities to read a suspect's communication before it was encrypted, he said.

Remember: It is the commercial interest of Facebook, WhatsApp, Apple, etc. to claim that they are unable to read messages, because their customers state that they want security. But the actual tradeoff for the convenience of not being burdened with explicit key management and endpoint verification -- for example, as Threema requires its users to do -- is that any of these providers **can** tap into their services' communications.

I am NOT saying that they can do this retrospectively at the moment, though that capability could be added. But we know they can do it prospectively, as with a wiretap, under warrant.

Unfortunately and naturally, law enforcement would like to have the ability to retrospectively decrypt any given individual's communications after the fact… and that is a problem that is much more fraught with technical challenges.

Wikileaks Unveils 'Cherry Blossom' — A WiFi hacking system used by the CIA
http://thehackernews.com/2017/06/cia-wireless-router-hacking-tool.html
The CherryBlossom documents: https://wikileaks.org/vault7/document/#cherryblossom

What is perhaps most breathtaking about this is the breadth of the exploitation possible.

https://wikileaks.org/vault7/document/WiFi_Devices/WiFi_Devices.pdf
The venders of well known and popular WiFi devices include: Belkin, D-Link, Linksys, Aironet/Cisco, Apple AirPort Express, Allied Telesyn, Ambit, AMIT Inc, Accton, 3Com, Asustek Co, Breezecom, Cameo, Epigram, Gemtek, Global Sun, Hsing Tech, Orinoco, PLANET Technology, RPT Int, Senao, US Robotics and Z-Com.

Within this latest batch of leaked Vault7 documents are the details of a WiFi device firmare hacking framework being used by the CIA for monitoring the Internet activity of targeted systems by exploiting vulnerabilities in Wi-Fi devices.

It's called "**Cherry Blossom**," and was reportedly designed by the CIA with the help of SRI International (Stanford Research Institute), a US nonprofit research institute, as part of its 'Cherry Bomb' project.

Cherry Blossom is a remotely controllable firmware-based implant for both wireless routers and access points which exploits router vulnerabilities to gain unauthorized access and then replace firmware with custom Cherry Blossom firmware.

Targeted wireless devices are "implanted" with custom CherryBlossom firmware, and since many devices support over-the-network firmware updates, physical access is not required. Once "implanted" these devices perform man-in-the-middle attacks to monitor and manipulate the Internet traffic of connected users.

Once the implanted firmware takes control on the wireless device, it reports back to a CIA-controlled command-and-control server referred as '**CherryTree**,' from which it receives instructions which include:

- Monitoring network traffic to collect email addresses, chat user names, MAC addresses, and VoIP numbers
- Redirecting connected users to malicious websites
- Injecting malicious content into the data stream to fraudulently deliver malware and compromise the connected systems
- Setting up VPN tunnels to access clients connected to Flytrap's WLAN/LAN for further exploitation
- Copying of the full network traffic of a targeted device

According to an “installation guide”, the CherryTree command & control server must be located in a secure sponsored facility and installed on Dell PowerEdge 1850 powered virtual servers, running Red Hat Fedora 9, with at least 4GB of RAM.

“Why we can't have nice things” (or take our nice things travelling with us)
(We get some interesting details about the increasing restrictions on travelling with electronics.)

Israeli hackers reportedly got into ISIS networks and found they were building laptop bombs...

DAVID E. SANGER and ERIC SCHMITT, for the New York Times:

Top Israeli cyberoperators penetrated a small cell of extremist bombmakers in Syria months ago. That was how the United States learned that the terrorist group was working to make explosives that could pass through airport X-ray machines and other screening by looking exactly like batteries for laptop computers.

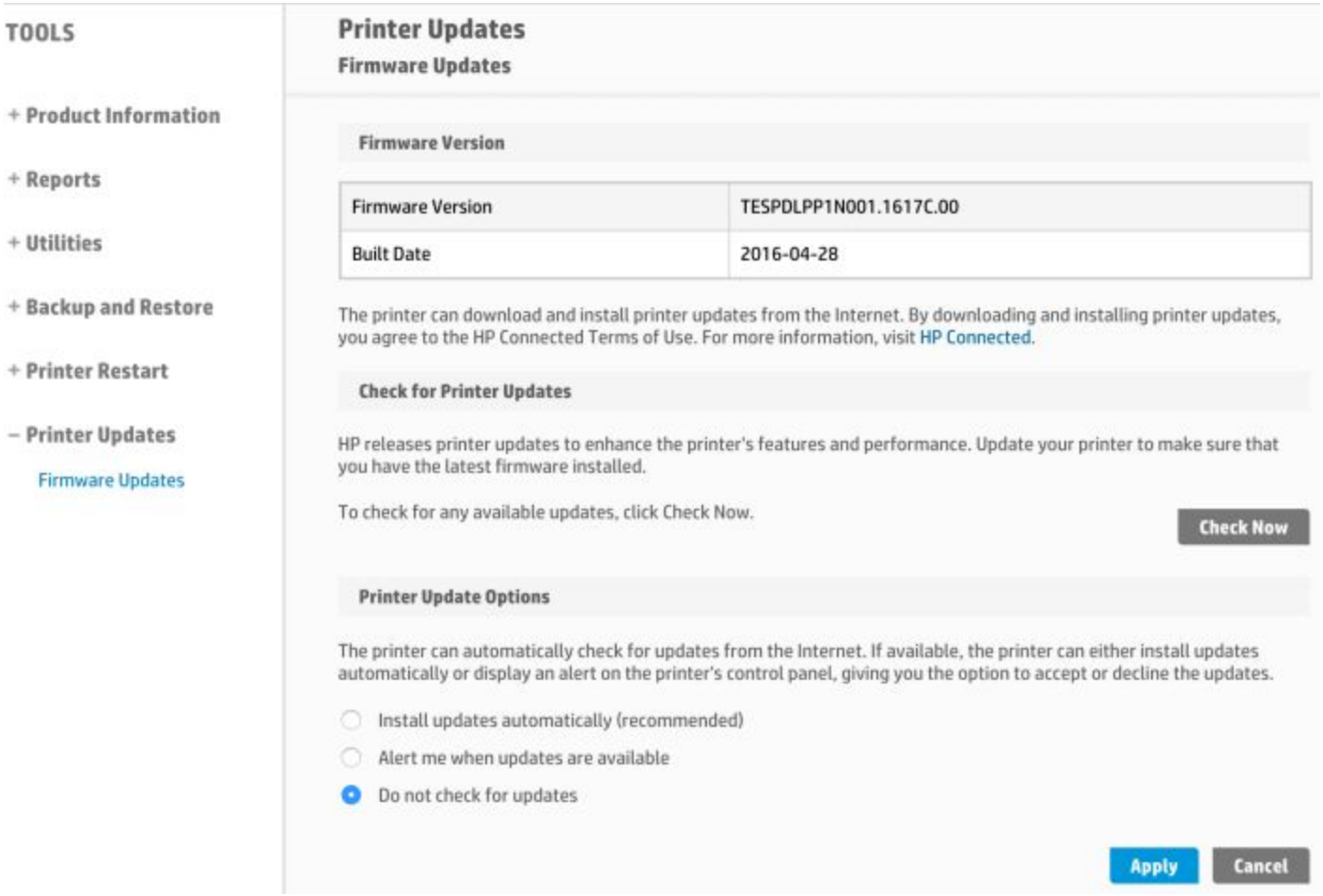
According to two American officials familiar with the operation, the intelligence obtained was so complete that it enabled the United States to understand how the weapons could be detonated. The information helped prompt a ban in March on large electronic devices in carry-on luggage on flights from 10 airports in eight Muslim-majority countries to the United States and Britain.
It was also part of the classified intelligence that President Trump is believed to have revealed to the Russian foreign minister, Sergey V. Lavrov, and the ambassador to the United States, Sergey I. Kislyak. It was the disclosure of this classified intelligence that reportedly infuriated Israeli officials because it revealed the fact that the security surrounding this small cell of extremist Syrian bombmakers had been successfully compromised, thus putting future intelligence gathering at unnecessary risk.

In any event, now we know a bit more about what’s going on. As an engineer, the whole issue of laptops are okay if you can power them on never made any real engineering sense. Only if we were to assume extreme incompetence on the part of all terrorists could would such a weak verification make any sense.

And we know that even innocent lithium batteries in the cargo holds of airplanes can cause problems. (I recently ordered a capacitor from DigiKey and was told that because it contained Lithium it could not be sent through the postal system and needed to to be shipped via UPS or FedEx. Huh???)

HP Printers have NETCAT installed
https://www.tenable.com/blog/rooting-a-printer-from-security-bulletin-to-remote-code-execution

After HP’s detail-lacking April security bulletin, the guys at Tenable decided to take a closer look under the hood of HP printers. So they purchased a pair of HP OfficeJet Pro 8210’s. It turned out that auto-updating firmware was disabled, so most users of HP’s printers will not automatically receive fixes for the problems that have been found.



So they manually updated one of the two identical printer's firmware in order to have before and after patch images… but it turned out that wasn't needed. They used NMAP to scan the printer for open ports and found an unsurprising handful. The "JetDirect" port 9100 turned out to be hosting many problems. By using a PC-based instance of NetCat, which is a common and extremely capable network data tool, they experimenting with various old school path-traversal exploits (/../../..) and they eventually found the linux/bin directory. This demonstrated that it's possible to traverse into the printer's Linux directory.

But how can these directory traversals be turned into remote code execution? It turns out that the Printer Job Language (PJL) commands: FSQUERY, FSUPLOAD, and FSDOWNLOAD will provide read/write access to the printer's filesystems. They demonstrated using the FSQUERY and FSUPLOAD with the directory traversal to retrieve the contents of the printer's /etc/passwd file.

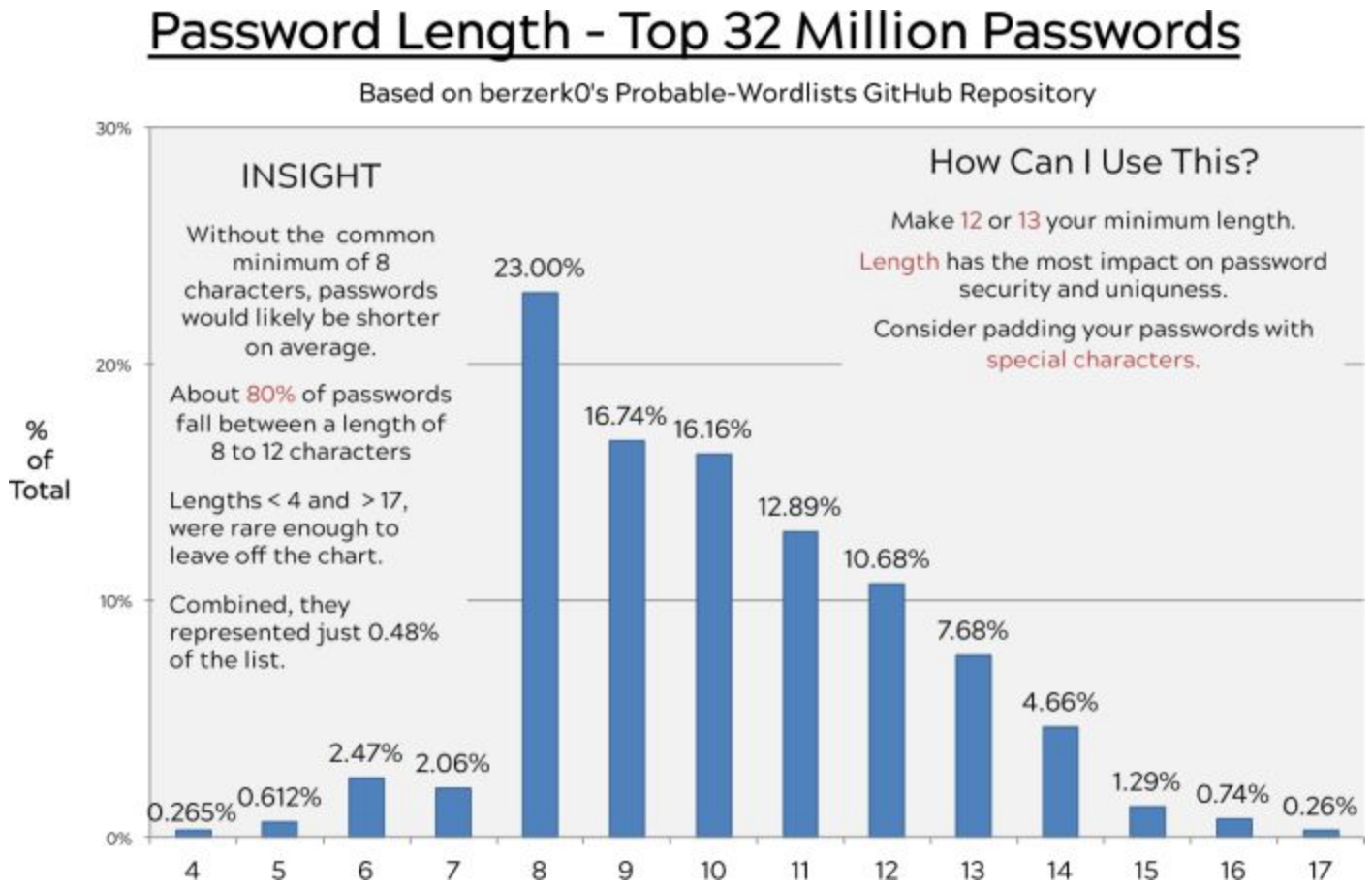
By using the FSDOWNLOAD command, and what they had discovered by surveilling the exposed filesystem, they were able to add a static invocation of the NetCat command upon bootup, which opened a remotely accessible full command shell on any available port of their choosing.

So… we have more details about what we reported two months ago: That the world is now full of remotely network-exploitable HP printers containing seriously vulnerable and exploitable firmware which HP has no ability to remotely update. They make perfect hosts for the insertion of advanced persistent threat (APT) malware within consumer and enterprise networks.

If our experience teaches us anything, we know that these highly vulnerable printers will continue to exist forever, until they die and are decommissioned, and will never go away.

EVERYONE within range of this podcast should proactively update any HP printer firmware within their control and responsibility as soon as possible.

What does the distribution of password length look like?
https://github.com/berzerk0/Probable-Wordlists/blob/master/Trend-Analysis.md
Some interesting and entertaining analysis posted at Github answers this question:



The Github page also has several other very interesting and useful analysis (the characters used and the sequencing of characters.)

Microsoft to disable SMBv1 by default in fall Windows updates
http://searchsecurity.techtarget.com/news/450420885/Microsoft-to-disable-SMBv1-by-default-in-fall-Windows-updates

As we all know… the WannaCry worm malware (whose creation has recently been attributed to a North Korean cyberwarfare group) leveraged the no-longer-mainstream v1 of Microsoft's SMB (Server Message Blocks, aka SAMBA on *nix) protocol. And we also know how difficult it always is to remove support for legacy protocols because there's always something, somewhere, that is no longer supported, cannot be updated, is mission-critical, and only understands the legacy

protocol.

Ned Pyle, who is the principal program manager in the Microsoft Windows Server high availability and storage group, told the guys at BleepingComputer that plans to disable SMBv1 have been in the works at Microsoft for the past five years. Pyle said that the security issues of SMBv1 were the main factor in deciding to disable the protocol, but the fact that SMBv2 was released nine years ago was also a factor. Pyle also said Microsoft would prefer everyone use SMBv3 -- released in 2012 -- as the standard.

However, as we similarly saw with the earlier insecure SSL versions, if SMBv1 is available and enabled, attackers can force a downgrade from the use of the newer and improved protocols to the known-exploitable protocols. Given that running SMBv1 is no longer necessary for modern enterprise users, and having it around opens up a significant security vulnerabilities, it's time for it to be put to rest. Ned Pyle claimed the ubiquity of SMBv1 made taking action more difficult, but confirmed when Windows 10 Redstone 3 is released, SMBv1 will be disabled by default.

A big Pay Day for the bad guys: all-time mega ransomware payout! $1 Million!!
Web host agrees to pay $1m after it's hit by Linux-targeting ransomware
https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/

Nayana, a South Korean Web host, was hit by the Erebus crypto malware. Although Erebus was originally targeted only at computers running Microsoft Windows operating systems, it was later modified to work against Linux systems.

It's unclear how Nayana became infected with Erebus, but an examination of the largely unpatched software the Web hosting service appeared to be running, it's possible the attackers exploited a well-known vulnerability.

In a recent blog post, researchers from security firm Trend Micro wrote:

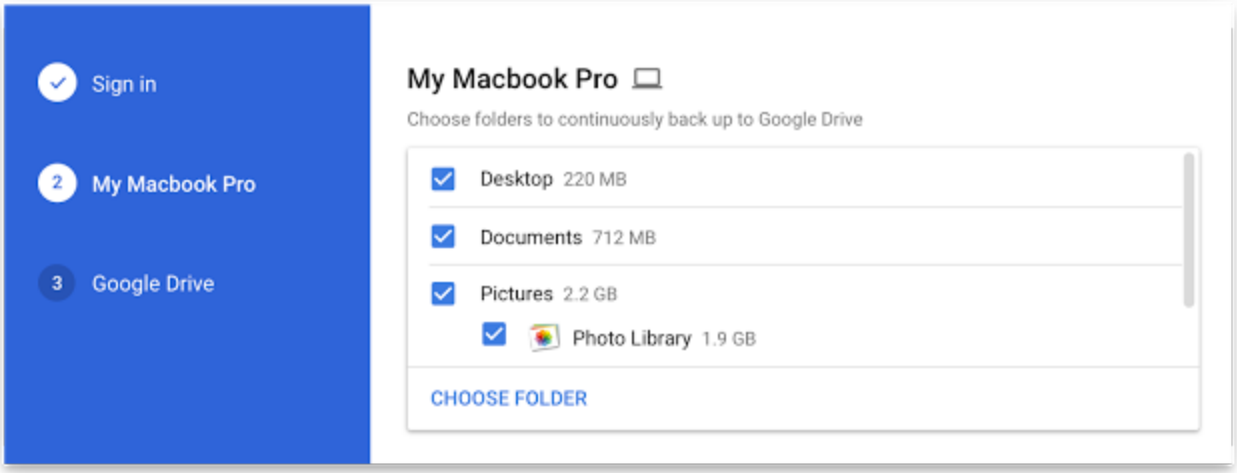
> As for how this Linux ransomware arrives, we can only infer that Erebus may have leveraged vulnerabilities or a local Linux exploit. For instance, based on open-source intelligence, NAYANA's website runs on Linux kernel 2.6.24.2, which was compiled back in 2008. Security flaws like DIRTY COW that can provide attackers root access to vulnerable Linux systems are just some of the threats it may have been exposed to.
>
> Additionally, NAYANA's website uses Apache version 1.3.36 and PHP version 5.1.4, both of which were released back in 2006. Apache vulnerabilities and PHP exploits are well-known; in fact, there was even a tool sold in the Chinese underground expressly for exploiting Apache Struts. The version of Apache NAYANA used is run as a user of nobody(uid=99), which indicates that a local exploit (and subsequent privilege elevation) may have also been used in the attack.

As for the ransom paid to obtain a decryption key, the fee was high due to the fact that all of the data stored on 153 Linux servers and 3,400 customer websites was encrypted.

Nayana's blog posting stated that the initial ransom demands were for five billion won worth of Bitcoin, which is roughly $4.4 million dollars. Company negotiators later managed to get the fee lowered to 1.8 billion won and ultimately landed a further reduction to 1.2 billion won, or just over $1 million. In an update posted last Saturday said Nayana engineers were in the process of recovering the data. The post cautioned that the recovery was difficult and would take time.

Backup and Sync from Google available soon
https://gsuiteupdates.googleblog.com/2017/06/backup-and-sync-from-google-available.html

On June 28th, 2017, we will launch "Backup and Sync from Google", a tool intended to help everyday users back up files and photos from their computers, so they're safe and accessible from anywhere. Backup and Sync is the latest version of Google Drive for Mac/PC, which is now integrated with the Google Photos desktop uploader.



The Backup and Sync tool will replace the current Google Drive uploader client for Mac/PC, and will also be integrated into the desktop Google Photos uploader. So, rather than creating new Google Drive folders on a system, the tool allows users to select standard system drives and folders -- such as Desktop, Documents, Pictures, Photo Library -- and will clone those chosen folders onto Google Drive.

The system is targeted toward regular consumers as a standalone backup solution featuring a simple interface to automatically upload files to the cloud as they are modified and guard against accidental loss.

Since Google's free storage is limited to a total of 15GB, users requiring more storage may be forced to Google's larger paid plans: 10GB of additional storage for $2/month, 100GB additional for $10/month, or 10TB additional for $100 a month.

Note that this would not a replacement for a full system-restoring image backup of the type that TWiT sponsor Carbonite offers. So it won't recover an entire machine. But for seamless background cloud cloning of a user's work product, this could be an effective solution.

From our "but of course it is" department... PC Magazine reports that it's possible (and fairly easy) to hack a PC with a vape pen https://www.pcmag.com/news/354377/its-possible-and-fairly-easy-to-hack-a-pc-with-a-vape-pen

Researchers are warning that USB-rechargeable e-cigarettes can be modified, without much effort, to infect a victim's PC with malware.

Remember, as we've covered here in the past, a USB device is automatically registered as a USB keyboard or, even worse, a network adapter which will be pinged for its DHCP configuration information and can thereby declare itself to be the system's network gateway and reroute all subsequent network traffic through itself.

Our podcast followers should already be highly resistant to allowing anyone to plug anything into their machines' USB ports, but enterprise environments may have less control over such interactions. The takeway here, is that ANY USB THINGY, no matter how apparently benign and innocent could be exchanging more than USB power with any USB port.

The solution, if you must "charge", is a USB Condom which passes only the power and ground lines without allowing the send and receive data signals to pass.

Miscellany

My tweet: "It's unfortunate that this humorous video about using chip cards is not that much of an exaggeration: https://www.youtube.com/watch?v=XD8FjaP78bQ "

The majority of response from my Twitter followers, who are mostly Security Now! Followers, was "What?! Huh?! Chip and Pin works great here! What's wrong with the U.S.?"... which was interesting to me, since my experiences have largely been similar to those in the video. So the conclusions would be that U.S. implementations are much more finicky than in those countries where CC chips have had much more time to mature.

But then we also have:

- Hilarious video! And unfortunately, you're right Steve - it's not that far off the mark. I've witnessed some HORRIFIC implementations!
- PDunn (@pwdunn)
  Pretty much right on. I love Apple Pay.

FWIW, in the US, chip support is not yet ubiquitous.

- Many chip-enabled machines do not accept chips.
- Swiping a chipped card is apparently disallowed.
- Lord help you if you (a) insert the card before instructed to or (b) have the gall to touch it before the system is completely satisfied, finished with whatever-the-hell-its-doing and prompts you to remove it... IMMEDIATELY!!

- And the saddest thing of all is that, as we know and have previously covered, none of this improves the system's operational security enough to be worth all of the hassle. People imagine that some super-power crypto is being done... but we know that's nonsense.

This Week's Darwin Award Winner:
A group of not-too-clever thieves stole a bunch of GPS tracking devices from a tech manufacturer. They were not too difficult to track down.
http://nbc4i.com/2017/06/07/thieves-caught-hours-after-stealing-gps-tracking-devices-from-tech-company/

SpinRite

James Mudd
Location: Oxford UK
Subject: Spinrite Question

Hi Steve + Leo

I really enjoy the podcast and look forward to it every week. I have been listening for years, and just started listening again from the beginning.

I often SpinRite drives before moving then between systems and formatting them. So I have a question, is it better to SpinRite the drive then format, or format first then SpinRite? I usually SpinRite first somehow feeling that having data on the drive is better but, logic tells me it shouldn't make a difference?

Matthew Norton
Location: Northwest, Indiana
Subject: Another random thing that SpinRite fixed!

I had been having an issue with my NumLock not turning on when I booted my computer, even though it was turned on in the BIOS and in windows. I did a SpinRite check of my drives and ever since then, the NumLock has turned on at boot. Thanks for the great product, eagerly awaiting SpinRite's future! Thanks for the podcast, I've been listening since episode 1.

Closing The Loop

Dan Sidor (@DanSidor)

- @SGgrc Ubiquiti EdgeRouter X looks great — do you also have experience with their UniFi access points?

KevN (@KvNa808)

- @SGgrc what was that switch/router you and leo recommended a few months back?

SQRL's Anti-Spoofing

- Eivind Hjertnes (@hjertnes)
  @SGgrc are there any safe guards in sqrl against dns spoofing?
  <<YES>>

- Kjetil Marthinsen (@albusgalea)
  @SGgrc if the malware has taken control of your dns, would your mitigation on MITM attacks still work with #sqrl?

- Martinš Zabarovskis (@MartinsZB)
  @SGgrc listened last SN podcast about dynamic pass and 2F Auth spoof.
  One more reason to use pass manager - it will not recognize wrong addr
  << True... but it will be completely fooled by DNS spoofing noted in the two previous questions.>D>

- Chris Taylor (@TaylorTechLLC)
  @SGgrc could a hacker kill SQRL local host port and run their own hijacker?
  As is possible in Mac OS X. lsof -n -i4TCP:3000 | grep LISTEN |
  << Yes, absolutely! >>

Le French Fab (@lefrenchfab)

- @SGgrc Hi, just listened to SN616. Do you think Apple 2FA is in any way better than the way used by Google/Microsoft? Thanks.
  << Apple has the significant advantage of having their own proprietary closed and encrypted messaging system (iMessage) which allows Apple to get second-factor tokens to their intended recipients without fear of MITM or other on-the-fly interception. >>

Bill (@bigpawzzz)

- @SGgrc Yesterday a friend was asked by TD Bank if they could keep the recording of her voiceprint for security purposes. How unique is it?

Ian Beckett (@ianbeckett)

- @SGgrc tell me why EVERY password interface doesn't have a 3 times and you are locked out for x hours as std ? #bruteforce #cybersecurity
  << GRC's eMail server has a zero-tolerance guessing policy.>>

David Benedict (@bippy_b)

- @SGgrc listening to SN614. Re "DrawOver" issue.
  Google not fixing doesn't mean they won't scrutinize apps more than before.

This week's LAUGH OUT LOUD Tweet:

- courtesy of a retweet by our listener: Morgan Speck (@morganspeck)
- Lesley (@hacks4pancakes)
  Personally I think this Windows 7 thing is overhyped, and shall be switching back to XP since it has a regular security patch cycle again!

~30~