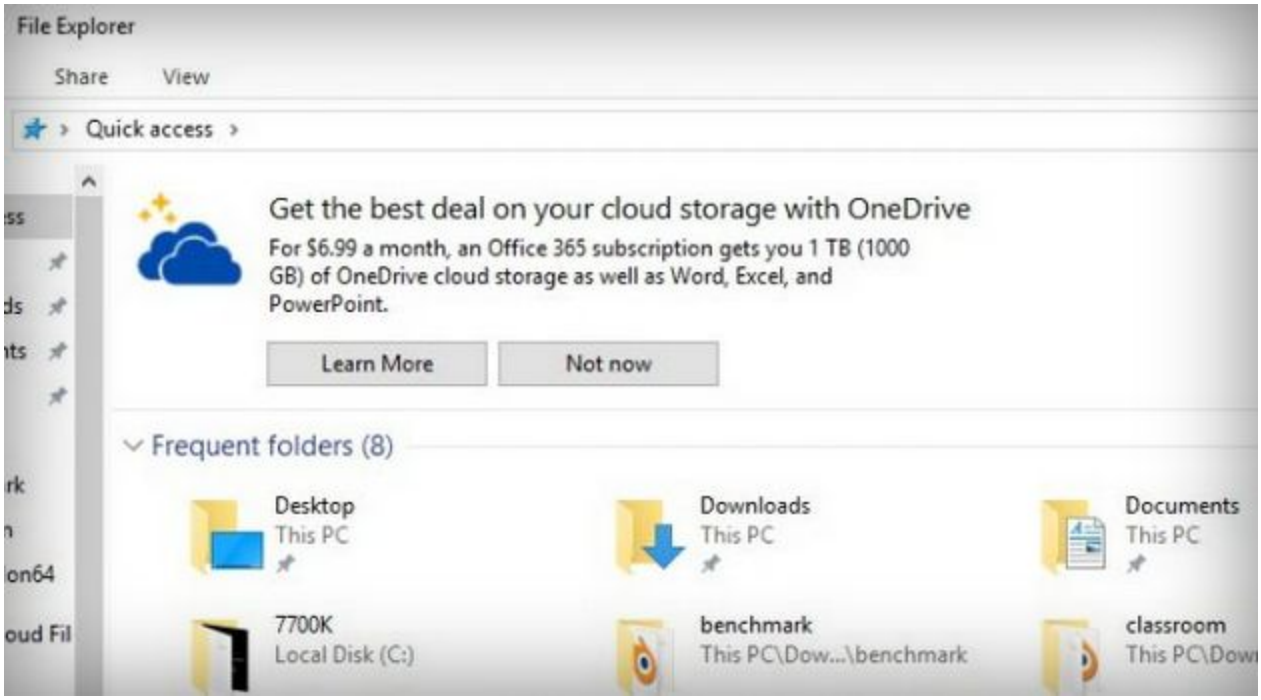
Security Now! #603 - 03-14-17

Vault 7

This week on Security Now!

This week Steve and Leo discuss March's long-awaited patch Tuesday, the release deployment of Google Invisible reCaptcha, getting more than you bargained for with a new Android smartphone, the new "Find my iPhone" phishing campaign, the failure of WiFi anti-tracking, a nasty and significant new hard-to-fix web server 0-day vulnerability, what if your ISP decides to unilaterally block a service you depend upon?, shining some much-needed light onto a poorly conceived end-to-end messaging application, two quick takes, a bit of errata and miscellany... and a look into what Wikileaks revealed about the CIA's data collection capabilities and practices.

Our Picture of the Week



"ExtremeTech: Microsoft now puts ads in Windows 10 File Explorer, because of course"
https://www.extremetech.com/computing/245553-microsoft-now-puts-ads-windows-file-explorer

Security News

The long-awaited March Patch Tuesday???

- Critical:
  - Security Update for Adobe Flash Player
  - Security Update for Microsoft Graphics Component
  - Security Update for Microsoft Windows SMB Server
  - Security Update for Microsoft Windows PDF Library
  - Security Update for Windows Hyper-V
  - Cumulative Security Update for Microsoft Edge
  - Cumulative Security Update for Internet Explorer
- Plus 11 "Important" updates
  - https://technet.microsoft.com/en-us/security/bulletins

Google takes their "Invisible reCaptcha" public

- https://www.google.com/recaptcha/intro/invisible.html
- Tag line: "Tough on bots, Easy on humans"
- Quote: Not just distorted text
- reCAPTCHA doesn't depend solely on text distortions to separate man from machines. Rather it uses advanced risk analysis techniques, considering the user's entire engagement with the CAPTCHA, and evaluates a broad range of cues that distinguish humans from bots.
- https://www.google.com/recaptcha/api2/demo?invisible=true
- https://www.google.com/recaptcha/api2/demo?invisible=false

Pre-Installed Android Malware Found On 36 High-end Smartphones

- http://blog.checkpoint.com/2017/03/10/preinstalled-malware-targeting-mobile-users/
- Last Friday, Check Point disclosed that their Mobile Threat Prevention system had recently detected a severe infection in 36 Android devices belonging to two of their clients: a large tlecommunications company and a multinational technology company. Although the discovery of Android malware is not unusual, what was unusual was that the malware was not downloaded into the devices after the phone's arrival... all of these phones ARRIVED with it pre-installed.

  The malicious apps were not part of the official ROM supplied by the vendor, and were added somewhere along the supply chain. Six of the malware instances were added by a malicious actor to the device's ROM using system privileges, meaning they couldn't be removed by the user and the device had to be re-flashed.

  Several different breeds of malware were discovered, including the well-known "Loki" Trojan which first appeared about a year ago, in February 2016. Loki obtains root privileges ad includes features such as grabbing the list of current applications, browser history, contact list, call history, and location data.

Also found was "SLocker", which is mobile ransomware that uses AES encryption to encrypt all files on the device and demand ransom in return for the decryption key. Slocker uses Tor for its C&C communications.

- The takeaway - "Post-Purchase, Pre-Use Screening": A newly purchased Android smartphone should be scanned once immediately after unboxing to check for any "supply-chain malware" it may have picked up.

- BitDefender Mobile appears to be the highest ranked Android solution. It offers free download and installation with 14 days to try the app before payment. This is perfect for post-purchase, pre-use screening.

The "Find My iPhone" phishing scam

- If an iPhone is lost or stolen, beware of subsequent offers for its recovery. What may be happening (and has been happening) is that organized crime gangs are attempting to phish the owner's Apple logon credentials in order to unlock, examine, wipe and resell the phone.

  Brian Krebs, who follows these sorts of organized incidents has been reporting on this recently and has accumulated several detailed case reports.

- https://krebsonsecurity.com/2017/02/iphone-robbers-try-to-iphish-victims/
- https://krebsonsecurity.com/2017/03/if-your-iphone-is-stolen-these-guys-may-try-to-iphish-you/

WiFi Ethernet MAC randomization -- Not all it's cracked up to be.

- https://arxiv.org/abs/1703.02874v1
- Eight researchers at the US Naval Academy decided to take a close look at WiFi MAC address randomization on Android phones and discovered that it was failing to provide the intended protections:

- ABSTRACT: Media Access Control (MAC) address randomization is a privacy technique whereby mobile devices rotate through random hardware addresses in order to prevent observers from singling out their traffic or physical location from other nearby devices. Adoption of this technology, however, has been sporadic and varied across device manufacturers. In this paper, we present the first wide-scale study of MAC address randomization in the wild, including a detailed breakdown of different randomization techniques by operating system, manufacturer, and model of device. We then identify multiple flaws in these implementations which can be exploited to defeat randomization as performed by existing devices. First, we show that devices commonly make improper use of randomization by sending wireless frames with the true, global address when they should be using a randomized address. We move on to extend the passive identification techniques of Vanhoef et al. to effectively defeat randomization in ~96% of Android phones. Finally, we show a method that can be used to track 100% of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames.

- Review: What's in an Ethernet MAC address?

- What's the WiFi Privacy concern?
  A significant privacy concern arises from the way Ethernet WiFi devices identify and enumerate nearby access points. Devices which are not yet associated with access points perform active scanning to populate their available WiFi lists by broadcasting "probe request frames" which ask nearby APs to identify themselves and respond with 802.11 parameter information required for connection setup.

  These probe request frames require a source MAC address, but if an 802.11 device uses its actual globally unique MAC address then it is broadcasting its unique identity at all times to any wireless receiver that is nearby. Wireless device users can then easily be tracked. To combat this privacy concern, both Android and iOS operating systems allow devices in a disassociated state to use random, locally assigned MAC addresses when performing active scans. Since the MAC address is now random, users gain a measure of anonymity up until they associate with an AP.

- They found several problems:

  - The most glaring observation, while not necessarily a flaw per se, is that the overwhelming majority of Android devices are not implementing the available randomization capabilities built into the Android OS. They suggested that this may be partly due to 802.11 chipset and firmware incompatibilities. However, some non-randomizing devices share the same chipsets as those implementing randomization, so it is not entirely clear why they are not utilizing randomization. Therefore, no effort by an attacker is required to target these devices.

  - The also explored the flaws of the observed MAC address randomization schemes. One such flaw was the inexplicable transmission of the global MAC address in tandem with the use of randomized MAC addresses.

    They observe this flaw across all Android devices. Exploiting this flaw made it trivial to link the global and randomized MAC addresses using device signatures and sequence number analysis. Between probe requests, the sequence numbers increase predictably so an entire series of random addresses can be linked with a global address by just following the chain of sequence numbers. Using sequence numbers has been discussed before in previous work, but the fact that the global MAC address is utilized while in a supposedly randomized scan state has not been.

    This strange behavior is a substantial flaw, and effectively negates any privacy benefits obtained from randomization. In their lab environment they observed that, in addition to periodic global MAC addressed probe requests, they were able to force the transmission of additional such probes for all Android devices. Anytime the user simply turned on the screen, a set of global probe requests were transmitted. An active user, in effect, renders randomization moot, completely eliminating the privacy countermeasure all together.

Additionally, any time the phone receives a call, regardless of whether the user answers the call, global probe requests are transmitted. Although it may not always be practical for an attacker to actively stimulate the phone in this manner, it is worrisome and disconcerting that device activity unrelated to WiFi causes unexpected consequences for user privacy.

    - Discovery and implementation of a control frame attack which exposes the global MAC address (and thus allows tracking/surveillance) for all known devices, regardless of OS, manufacturer, device type, or randomization scheme. Furthermore, Android devices can be susceptible to this attack even when the user disables WiFi and/or enables Airplane Mode.

- Our takeway:
  This is not something end users have any control over. For now, mobile phone and PC users should not expect non-trackability when roaming. We have always been aware that cellular phones are explicitly trackable. But the assumption has been that switching to WiFi would limit tracking exposure. Unfortunately, as it is currently implemented, the protections are weak to nonexistent.

  Hopefully, this research and other like it will focus more attention upon this problem so that future devices give more than passing lip service to anti-tracking privacy.

A new 0-day web server application framework vulnerability is under massive attack.

- "Apache Struts 2" is a decade old, widely used, open-source web application framework.
- A vulnerability exists in the "Jakarta file upload multipart parser", which is a standard part of the framework.

- Get a load of this: Struts supports OGNL -- OGNL stands for Object-Graph Navigation Language, an expression language for getting and setting properties of Java objects -- so it's a type of scripting language for the JVM. Struts would mistakenly execute OGNL that appeared in the Content-Type header. OGNL can be very dangerous, because it offers a means for introducing code-injection vulnerabilities in Java.

- But here's the problem: Struts is not a stand-alone dynamically-linked or invoked separate library. Rather, it is statically linked (compiled into) the service-side JAVA executable. This means that fixing this problem is not just a matter of running apt-get to update a fixed module and rebooting a server. Fixing this could require completely rebuilding the server's web applications, recompiling them with the fixed Struts 2 system. But many of these packages are a decade old and have gone unmaintained for years. Their original authors or subcontractors may be long gone.

  An organization may have tens or hundreds of little Struts-using Web apps, all with their own Struts JAR embedded within them. Many of those apps may be essentially abandoned; the earliest affected version of Struts was released in October 2012, and many of the apps developed since then are "finished". They're still used and deployed, but they're not receiving ongoing maintenance; their developers have moved on to other projects, or even other companies.

- Dan Goodin, writing for ArsTechnica, wrote that researchers at Cisco Systems said they are seeing a "high number of exploitation events" by hackers attempting to carry out a variety of malicious acts. One series of commands that attackers are injecting into webpages stops the firewall protecting the server and then downloads and executes malware of the attacker's choice. The payloads include "IRC bouncers," which allow the attackers to hide their real IP address during Internet chats; denial-of-service bots; and various other packages that conscript a server into a botnet.

- Outside researchers have said the exploits are trivial to carry out, are highly reliable, and require no authentication. It's easy to scan the Internet for vulnerable servers. It's also possible to exploit the bug even if a Web application doesn't implement file upload functionality.

Canada Takes Tax Site Offline After Apache Struts Attacks

- http://www.reuters.com/article/us-canada-cyber-idUSKBN16K2BC
- http://www.darkreading.com/vulnerabilities---threats/canada-takes-tax-site-offline-after-apache-struts-attacks/d/d-id/1328394

- A newly discovered vulnerability in the Apache Struts 2 software has forced the Canadian government to close down the Statistics Canada site used for filing federal taxes, Reuters reports. The site came under attack from hackers but was immediately shut down before any damage could be done.

  The security bug in Apache Struts 2 software, used mostly in websites of government, banks, and retailers, was reported last week after the Apache Software Foundation came out with an update to fix the vulnerability. Users of this software around the world spent the weekend patching up this bug which reportedly was being exploited in the wild.

  Canadian government official John Glowacki said that other countries "are actually having greater problems with this specific vulnerability."

  Chris Wysopal of security software firm Veracode said: "This vulnerability is super easy to exploit. You just point it to the web server and put in the command that you want to run."

TeamViewer stopped working? Let me guess, your ISP is TalkTalk...

- https://hotforsecurity.bitdefender.com/blog/teamviewer-stopped-working-let-me-guess-your-isp-is-talktalk-17781.html

- TeamViewer is a popular remote desktop application frequently used by IT to support remote users.

- Unfortunately, its ease-of-use also allows it to be used by scammers masquerading as helpers.

- TalkTalk:
  - https://community.talktalk.co.uk/t5/Broadband/Teamviewer/m-p/2022946#M665323
  - Hi All,
    Apologies for the confusion, but I can confirm that we have implemented a number of network changes that have blocked a number of applications including Teamviewer.

    We constantly monitor for potentially malicious internet traffic, so that we can protect our customers from phishing and scamming activities. As part of this work, we have recently blocked a number of sites and applications from our network, and we're working hard to minimise the impact on our customers.

    We are working with teamviewer and other 3rd parties on implementing some additional security measures that would enhance the security to all customers of these services but we will continue to block any sites/applications reported by customers to reduce the opportunity for fraud to take place.

- Typical reaction from TalkTalk customers:
  - "but we will continue to block any sites/applications reported by customers to reduce the opportunity for fraud to take place."

    Great !! What about the same consideration for customers who don't report any problems with sites/applications because they haven't had any? I, and no doubt a great many other customers, have been using Teamviewer (via TalkTalk) for many years without any problems, now all of a sudden with no prior warning we can't, and no one is saying how long (if at all) before we can use it again. Corporations, Businesses and IT departments worldwide can use Teamviewer. But Talktalk customers can't. Extremely unsatisfactory customer service IMHO.

- Same problem here, since yesterday. Teamviewer suddenly not connecting at all.

  I'm an IT support engineer. I use Teamviewer to access client's computers to give remote support so this is more than just a little inconvenient. There are other remote support applications out there but what's to say those won't suddenly stop working via TalkTalk at some time in the future ?

  This is completely unsatisfactory. If this can't be resolved then I'll have no alternative but to switch ISP and also recommend that my main clients do also.

Confide -- "Because we say so!"

- https://getconfide.com/
- Super-slick, polished, confidence-inspiring website... offering a piece of junk.

- In mid February, Alan Woodward, a security researcher and professor at the University of Surrey characterized Confide as "a triumph of marketing over substance."

- Home page: "Your Confidential Messenger. Communicate digitally with the same level of privacy and security as the spoken word. With encrypted messages that self-destruct, Confide gives you the comfort of knowing that your private messages will now truly stay that way." (Or not.)

- Matthew Green @matthew_d_green
    - The encryption in Confide looks genuinely bad. Don't use it, people. What's the matter with you. https://arstechnica.com/security/2017/03/unfixed-weaknesses-in-confide-stoke-doubts-about-end-to-end-crypto-claims/

- Matthew Green @matthew_d_green
    - Here's the technical blog post from Quarkslab. In short: no key fingerprinting, bad encryption mechanism, blegh. http://blog.quarkslab.com/make-confide-great-again-no-we-cannot.html

- Matthew Green @matthew_d_green
    - Oh, but Confide does use TLS pinning. That's nice. I'd ask why people keep trying to reinvent their own e2e crypto, but I know the answer. People are just the worst.

- The QuarksLab blog tears it apart with a step-by-step walk through of the way they reverse-engineered and examined the system. In their summary: TL;DR: Confide server can read your messages by performing a man-in-the-middle attack.

- In their FAQ they state:
  "Q: How secure is this and do messages really disappear?"
  "A: We employ end-to-end encryption to ensure conversations remain confidential and are private to you. Even we at Confide cannot decrypt or see any messages. Yes, after messages are read once they disappear."

- Producing a secure end-to-end encrypted messaging system is truly difficult. But it's already been done. If you want maximum security, choose Signal or Threema and verify your contact's key fingerprints. If you're using Signal or WhatsApp, turn on the "notify if the fingerprint changes" feature.

- But, as we'll be discussing as the topic of this podcast... e2e encryption is only secure if both ends are also secure.

Tim Berners-Lee:
"I invented the web. Here are three things we need to change to save it."

- https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet

- Tag: "It has taken all of us to build the web we have, and now it is up to all of us to build the web we want – for everyone"

- Saturday, March 11th: Today marks 28 years since I submitted my original proposal for the worldwide web. I imagined the web as an open platform that would allow everyone, everywhere to share information, access opportunities, and collaborate across geographic and cultural boundaries. In many ways, the web has lived up to this vision, though it has been a recurring battle to keep it open. But over the past 12 months, I've become increasingly worried about three new trends, which I believe we must tackle in order for the web to fulfill its true potential as a tool that serves all of humanity.

  1) We've lost control of our personal data
  2) It's too easy for misinformation to spread on the web
  3) Political advertising online needs transparency and understanding

- My own feeling is… we need a "meta-layer" to wrap and hide the legacy protocol and domain name mess. "Http" "https" hierarchical domains, etc. should all be hidden so that users interact with "Labels" that map can transparently map to an address.
  … So you just have "Amazon" and "Google" and "Apple"

Quick Takes

Tom Elliott (@telliottiv)

- Q:
  I have a dev telling me that storing SSN in SQL using an unsalted SHA1 hash is secure. Isnt this susceptible to a time-memory tradeoff attack (Rainbow tables and some GPUs)?

- A:
  Tom…
  That cannot be secure. SSN's do not contain sufficient entropy to prevent having their hash brute forced. It doesn't matter whether it's SHA-1, SHA-256, salted or unsalted. The search space for a 9-digit all-numeric number is too small.

  Also... storing the hash of an SSN -- putting the SSN behind a one-way function -- suggests that the SSN is being used as an identity authenticating token (since it cannot be decrypted, it can only be verified in the future). This is HORRIBLE design and policy, since SSN's are inherently tied to people's identity -- MUCH WORSE than "your mother's maiden name" or "your first dog's name".

Aaron Watt (@Aussie_Avalon)

- @SGgrc @leolaporte Panasonic hasn't patched their current FireFox OS for their Smart TV's in over a year; should I be worried about it?

Errata

Dan Hankins (@hidannik)

- @SGgrc Mic jack trick won't work on laptops where jack function is software-assignable - there isn't, and can't be, a hardware cutout.

TradMan (@musicasacra62)

- @SGgrc Also, the mic plug hack isn't sufficient. That just activates a software switch. Even with a mic plugged in, software can see int. mic

Miscellany

Last week I believed that I had found the coolest waste of time ever... by someone who built a working digital clock out of Conway's "Game of Life" cellular automata system.

I was wrong.

Thanks to some of our listeners who took were interested and dug around, something even more incredible has come to light: Conways Game of Life... implemented in ITSELF!

https://youtube.com/watch?v=xP5-iIeKXE8

Indicators show potatoes can grow on Mars

- https://phys.org/news/2017-03-indicators-potatoes-mars.html
- Home > Astronomy & Space > Space Exploration > Biology > Biotechnology > March 8, 2017
- In a nod to "Mark Watney"...
  The International Potato Center (CIP) launched a series of experiments to determine whether potatoes can grow under Mars atmospheric conditions and thereby prove they are also able to grow in extreme climates on Earth. The Phase Two effort of CIP's proof of concept experiment to grow potatoes in simulated Martian conditions began on February 14, 2016 when a tuber was planted in a specially constructed CubeSat contained environment built by engineers from University of Engineering and Technology (UTEC) in Lima based upon designs and advice provided by the National Aeronautics and Space Administration in Ames Research Center (NASA ARC), California. Preliminary results are positive.

- Read more at: https://phys.org/news/2017-03-indicators-potatoes-mars.html#jCp

SpinRite

Sean Kloeckner
Location: HB in the OC
Subject: Took your advice on CRC errors

Hi Steve,

I've been a listener for probably a couple years now and I appreciate all the advice you give on the show. I sent in a previous note about Syncthing and what you think of it since I heard you complaining, in a good way, about BTSync previously. Syncthing is totally open source. I have to say it's been functionally everything BTSync is and works great as a dropbox replacement. I no longer need to worry about my data in a company's hands and it replicates to all my other PCs.

Anyway, I wanted to let you know I have been an avid listener and bought SpinRite recently. I am a Linux user and don't really need to buy software, but I know SpinRite would come in handy and thankfully haven't needed it for anything other than testing and maintaining drives in my lab.

I recently bought new PNY drives and use them for a ZFS root system using proxmox and noticed whenever I scan my Zpool, there would be checksum errors that it would correct. Few weeks went by without me touching them and everything works generally OK but everytime I would perform a scrub on my pool, it would still return errors. I learned in more detail that certain drives can return junk when under duress but this is on a fresh install every time with the same result.

Anyway, long story short after seeing CRC errors in the syslog and then running SpinRite confirmed the CRC errors, I took your advice and replaced the cables. I ran some further benchmark and dummy data tests on my pool and SpinRite ... and lo and behold, no more checksum errors!
Love the show and wanted to pitch in my 2 cents for other listeners out there who may be in the same situation. What you do is a public service.

- NOTE: A checksum error will force a repeat of the failed operation. So the guaranteed consequence will be somewhat reduced performance. But the BIG WORRY is that checksums are small and fast and are therefore NOT guaranteed to catch every error. If cables are throwing a lot of errors, some WILL get past the checksum test... resulting in corrupted data being read from or written to the drive.

Vault 7

WikiLeaks released 8,761 documents and files which allegedly (and believably) exposes and discloses the tactics and technologies the US Central Intelligence Agency uses to hack into secure devices, systems and communications.

These include Android & iOS devices, Routers, Windows, Mac and Linux PCs, and many IoT devices including Smart lightbulbs and televisions.

Vault7 - Home / https://wikileaks.org/ciav7p1/

Both "The Gibson" and "SQRL" appear as accidental name collisions within the document dump.
https://wikileaks.org/ciav7p1/cms/page_9535963.html

But... there really was nothing hugely new here.
Imagine is someone where to listen to all previous 602 weeks of Security Now and so find and collect everything that we have discussed on this podcast. That's about that the CIA would then have, and does apparently have.

As I reading through everything I found nothing that we haven't already discussed -- often many times -- on this podcast.

This clearly demonstrates one of the fundamental distressing realities of today's computing and communication technologies which this podcast has often highlighted: When your defenses are inherently somewhat soft and porous, placing PRESSURE upon them will cause them to leak. Well funded and highly motivated state actors, such as the NSA and CIA can bring significantly resources -- and thus a great deal of pressure -- to bear against the many technologies we use in our daily lives.

Perhaps the most controversial aspect of this is the notion that not a malicious hacker, but a taxpayer funded organization would be discovering and concealing zero-day vulnerabilities in these systems. Keeping them for their own purposes and not disclosing them to their devices' manufacturers.

Apple says it's already patched 'many' Wikileaks iOS exploits
https://www.engadget.com/2017/03/08/apple-ios-wikileaks-cia-exploits/
Apple said in a statement: "Apple is deeply committed to safeguarding our customers' privacy and security. The technology built into today's iPhone represents the best data security available to consumers, and we're constantly working to keep it that way. Our products and software are designed to quickly get security updates into the hands of our customers, with nearly 80 percent of users running the latest version of our operating system. While our initial analysis indicates that many of the issues leaked today were already patched in the latest iOS, we will continue work to rapidly address any identified vulnerabilities. We always urge customers to download the latest iOS to make sure they have the most recent security updates."

Notepad++ Fix CIA Hacking Issue
https://notepad-plus-plus.org/news/notepad-7.3.3-fix-cia-hacking-issue.html
"v 7.3.3 - Fix CIA Hacking Notepad++ Issue"
https://wikileaks.org/ciav7p1/cms/page_26968090.html
Notepad++ DLL Hijack
The following DLL hijack works for both the portable and non-portable variants of Notepad++
The issue of a hijacked DLL concerns scilexer.dll (needed by Notepad++) on a compromised PC, which is replaced by a modified scilexer.dll built by the CIA. When Notepad++ is launched, the modified scilexer.dll is loaded instead of the original one.
It doesn't mean that CIA is interested in your coding skill or in your sex message content typed in Notepad++, but rather it prevents raising any red flags while the DLL does data collection in the background.

It's not a vulnerability/security issue in Notepad++, but for remedying this issue, from this release (v7.3.3) forward, notepad++.exe checks the certificate validation in scilexer.dll before loading it. If the certificate is missing or invalid, then it just won't be loaded, and Notepad++ will fail to launch.

Checking the certificate of DLL makes it harder to hack. Note that once users' PCs are compromised, the hackers can do anything on the PCs. This solution only prevents from Notepad++ loading a CIA homemade DLL. It doesn't prevent your original notepad++.exe from being replaced by modified notepad++.exe while the CIA is controlling your PC.

The Bottom Line:
As I once indicated back at the time of the Sony APT breach, I would have a nervous breakdown if I was responsible for securing something as lumbering and massive as Sony Pictures. It's simply impossible.

The NSA/Snowden and CIA/WikiLeaks disclosures demonstrate conclusively, if nothing else, that, despite all of their best efforts, those high-end government intelligence agencies are unable to secure their own working assets.

So... how could they possibly be trusted with any explicit "Golden Key" which would allow them to access our encrypted communications?

Past is prologue, and ALL of the evidence demonstrates that even with the best of intentions, US Law Enforcement cannot be trusted with any sort of carte blanche backdoor access to the Internet's encrypted communications. OF COURSE THEY WANT THAT. It's fine for them to ask. "You can ask." But we must not capitulate. As our experience with OpenSSL vulnerabilities continues to demonstrate, any sort of cryptographic monoculture is inherently dangerous. The system we have now, where a court order search warrant must be obtained and served creates a heterogenous system with distributed responsibility and built-in checks and balances. Even requiring companies to be able to decrypt their customers' data subjects customers to unnecessary risks.

And besides... if the CIA has all of this, now demonstrated technology, they clearly don't need to ask for permission.

Other Links:

The Truth About the WikiLeaks C.I.A. Cache - The New York Times
https://www.nytimes.com/2017/03/09/opinion/the-truth-about-the-wikileaks-cia-cache.html

WikiLeaks and the CIA's hacking secrets, explained - CNET
https://www.cnet.com/how-to/wikileaks-cia-hack-phone-tv-router-vault-7-year-zero-weeping-angel/

Compromise of CIA Cyber Weapon Cache Leaves Most Computing Devices Vulnerable
http://www.integrasurety.com/cia-cyber-weapons-compromise/

Wikileaks: CIA has tools to snoop via TVs - BBC News
http://www.bbc.com/news/technology-39193008

WikiLeaks: The CIA is using popular TVs, smartphones and cars to spy on their owners
https://www.washingtonpost.com/news/the-switch/wp/2017/03/07/why-the-cia-is-using-your-tvs-smartphones-and-cars-for-spying/

WikiLeaks publishes docs from what it says is trove of CIA hacking tools | Ars Technica
https://arstechnica.com/security/2017/03/wikileaks-publishes-what-it-says-is-trove-of-cia-hacking-tools/

The CIA Didn't Break Signal or WhatsApp, Despite What You've Heard
https://theintercept.com/2017/03/07/the-cia-didnt-break-signal-or-whatsapp-despite-what-youve-heard/