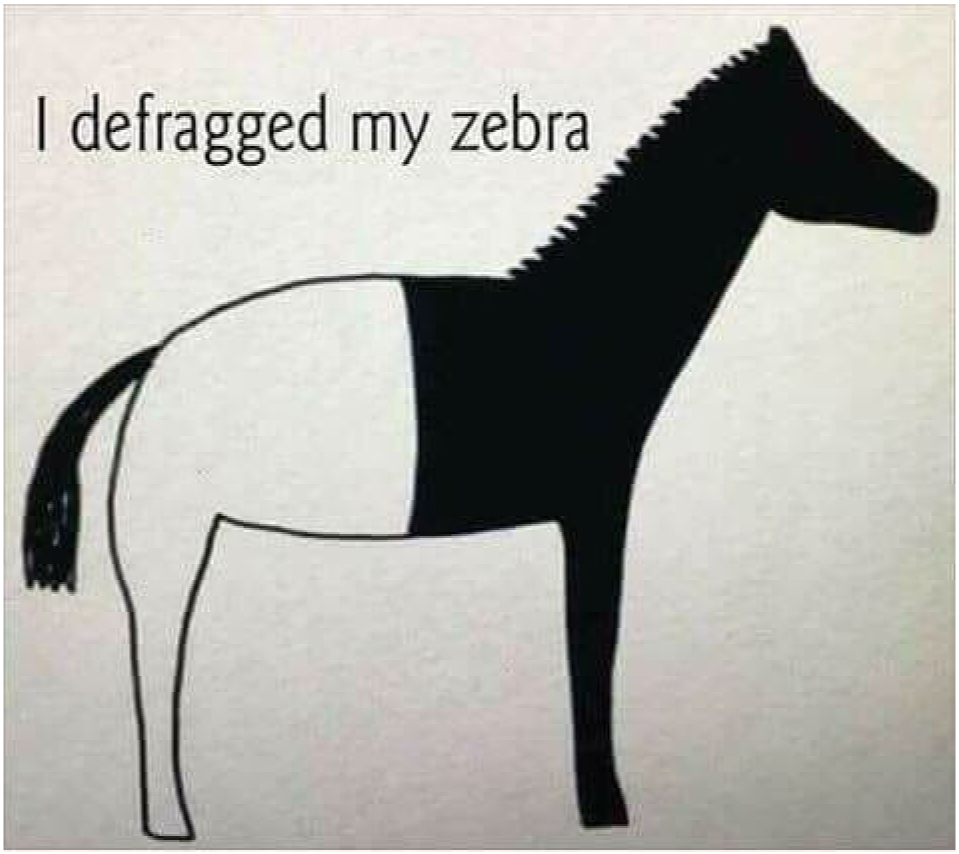
Security Now! #637 - 11-14-17

Schneier on Equifax

This week on Security Now!

This week we discuss why Steve won't be relying upon FaceID for security, a clever new hack of longstanding NTFS and Windows behavior, the Vault8 WikiLeaks news, the predictable resurgence of the consumer device encryption battle, a new and clever data exfiltration technique, new anti-Malware features coming to Chrome, an unbelievable discovery about access to the IME in Skylake and subsequent Intel chipsets, a look at who's doing the unauthorized cryptomining, WebAssembly is ready for prime time, a bit of miscellany, some closing the loop feedback with our listeners... an then we share Bruce Schneier's congressional testimony about the Equifax breach.

Our Picture of the Week



Security News

iPhone X's face recognition stories are beginning to surface

- https://hackernoon.com/my-younger-brother-can-access-my-iphone-x-face-id-is-not-secure-376c904f88bc
- http://www.bkav.com/d/top-news/-/view_content/content/103968/face-id-beaten-by-mask-not-an-effective-security-measure
- https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask
- https://www.wired.com/story/hackers-say-broke-face-id-security/

I will not use FaceID alone. Since I have my authenticator app there, the phone creates a portal into all of my other accounts. And since it receives my eMail and text messages, which are currently used as last-line account recovery, I cannot afford to have anyone get access to them.

Apple has done SO MUCH to shore up the internal security of their platform... but the insecurity of FaceID seems as through it should be quite worrisome.

A clever use of NTFS file system links...

https://bogner.sh/2017/11/avgater-getting-local-admin-by-abusing-the-anti-virus-quarantine/

If a user is allowed to move a quarantined file out of quarantine, the A/V is most likely vulnerable to this attack.

The Windows NTFS file system has a feature known as "Directory Junctions" which are similar to Unix symbolic links. This abuse of directory junctions can cause the quarantine directory to appear in the system's DLL search path... which will cause the system to load the malicious software -- named as a DLL -- in preference to the actual DLL it is searching for.

The following vendors who have been contacted and have already released fixes are: Trend Micro, Emsisoft, Kaspersky Lab, Malwarebytes, Ikarus, and Zone Alarm. Others have been notified are should be updated soon.

Furthermore, as "#AVGator" can only be exploited if the user is allowed to restore previously quarantined files. The researcher who discovered this problem recommends that everyone within a corporate environment block normal users from restoring identified threats -- which should already be the default configuration.

Keep your A/V up to date since we can predict that bad guys will begin exploiting this soon.

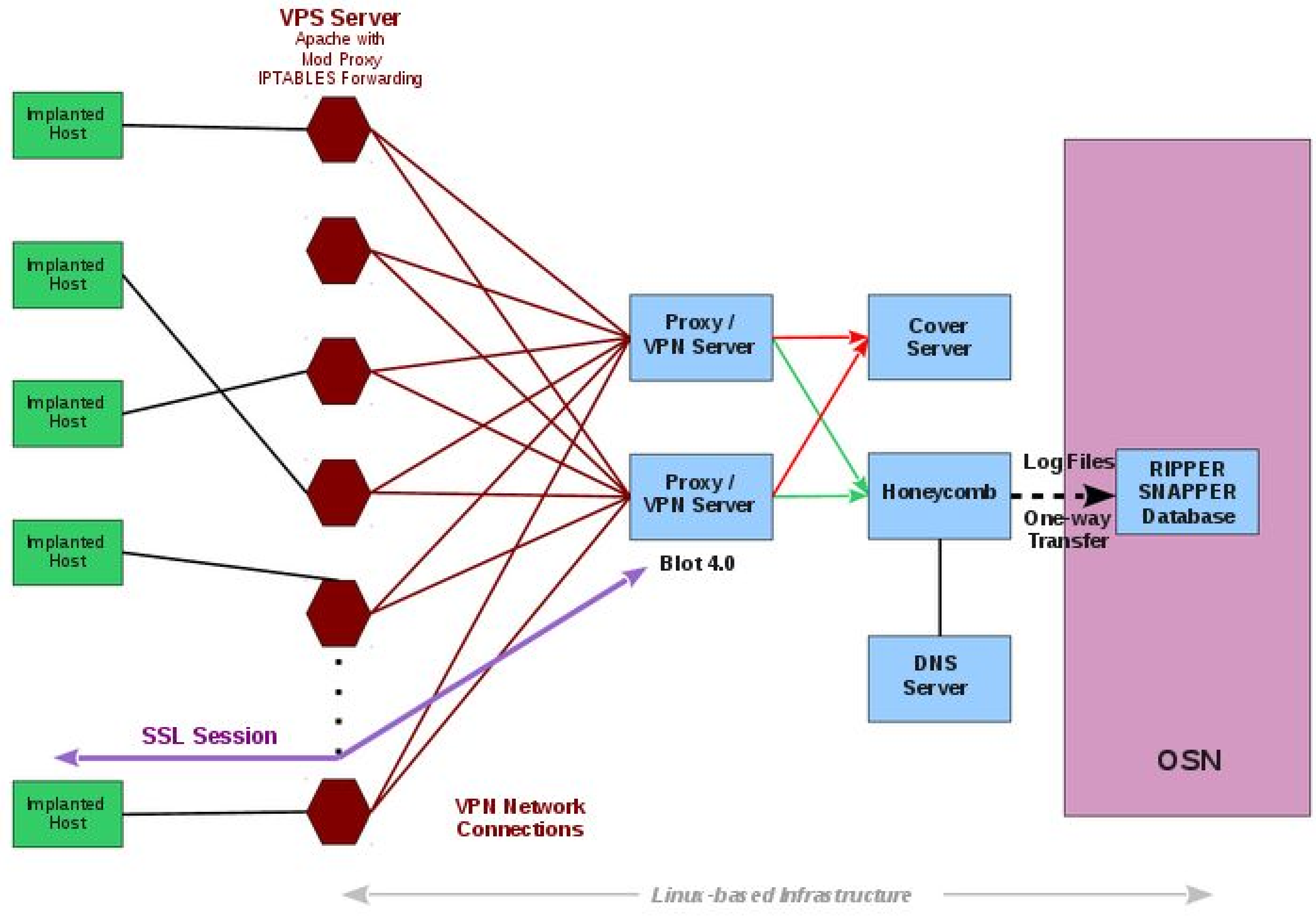
Vault 8: WikiLeaks Releases Source Code For Hive - CIA's Malware Control System

https://wikileaks.org/vault8/
https://thehackernews.com/2017/11/cia-hive-malware-code.html

WikiLeaks has released, under the name "Vault 8" the source code for what they claim to be, and what appears to be, a command-and-control system for use by the US Central Intelligence

Agency for managing remotely located surveillance implants.

It's known, somewhat dramatically, as "the Hive" and consists of a system for hiding the communications of CIA implants in plain sight...



Apple says it immediately contacted FBI about unlocking Texas shooter’s iPhone
Apple is refuting the FBI’s official account
https://www.theverge.com/2017/11/8/16626452/apple-fbi-texas-shooter-iphone-unlock-encryption-debate
http://www.zdnet.com/article/texas-shooter-fbi-cannot-access-texas-gunman-iphone/

Immediately upon learning that an encrypted iPhone might contain evidence useful to the FBI's investigation, Apple proactively reached out to the FBI offering assistance, but Apple's assistance was never accepted.

And a clock was ticking, since, if the alleged shooter had used a fingerprint to unlock the phone, any delay might thwart the FBI's chance of gaining easy access to the iPhone since, as we know, the fingerprint sensor cannot be used for easy entry after 48 hours.

Tim Cushing, writing for TechDirt: "If everything alleged by the Reuters report is true, the FBI's "struggles" are of its own making. It could have sought immediate assistance from Apple but chose not to. It also, apparently, turned down Apple's offer to help. If so, the FBI doesn't actually want cooperation from tech companies. It wants to be able to tell companies what features they can and can't have. It wants to dictate all the terms of these engagements, which is very much in line with the DOJ's views on tech company "partnerships." "

Diane Feinstein has also been dusting off her legislation which died for lack of support near the end of the previous administration.

There is an entirely safe, though burdensome-for-Apple, solution to this:

- Apple already maintains a connection to every one of their devices.
- Ultimately, there is a single master 256-bit symmetric key super-guarded by layers of security.
- During the device setup process, when that high-entropy key is created, it could be encrypted by a very long and very safe master Apple "Master Key Transport" public key. It could then be safely sent to Apple for storage and all trace of it removed from the iPhone.
- At that point, Apple has the ability to INDIVIDUALLY decrypt any specific phone upon receipt of a court order.
- There is no "master key", no "golden key", no backdoor, side door or unlocked front door. There is nothing for law enforcement to be trusted with. t that point, Apple, and Apple alone, can, if and when they choose, decrypt any specific phone upon lawful demand.
- Apple clearly does not want that responsibility, and I salute them for that. But it may be that they're going to be left with little choice.

Exfiltration by encoding data in pixel colour values
https://www.pentestpartners.com/security-blog/exfiltration-by-encoding-data-in-pixel-colour-values/

Hackers are endlessly clever: The exfiltration of a mobile device's data by displaying a band of "static" along the bottom edge of the screen during a video conference.

The encoding of the data would need to be robust against compression, which would tend to alter individual pixel values. But clever design of the data's representation could get the data through.

Google Adds New Features in Chrome to Fight Malvertising
https://www.bleepingcomputer.com/news/security/google-adds-new-features-in-chrome-to-fight-malvertising/

Starting with release 64 (January 2018) Chrome will block iframe redirects:
Due to a history of abuse by embedded malvertising, Chrome will no longer accept URL redirections triggered by JavaScript code residing within iframes.

Two months later with release 65 in early March 2018, Chrome will begin blocking JavaScript-driven "Tab Under" behavior. A "tab under" is the act of a web page bypassing

Chrome's built-in pop-up blocker by opening links in new tabs and redirecting the old tab to a new URL. From Chrome 65 on, that redirect attempt will be blocked and will display a notice at the bottom of the page.

The last of the three new features is called "Abusive Experiences Report" and will take the form of a blacklist of sites known to be using misleading user-interface elements -- such as Play or Pause buttons... or even invisible transparent overlays -- that redirect users without their consent. Browsers make a CLEAR DISTINCTION between what users do and what any scripting does.

Website owners who register their site with Google will receive warnings about these type of misleading UI elements in the new Abusive Experiences Report section part of their Google Console account. Then, beginning next January website owners who do NOT address these reports will have any redirections triggered by these misleading elements blocked via Chrome's built-in popup blocker.

Intel’ Management Engine Tech Just Got Exposed Through USB Ports
https://www.hackread.com/intel-management-engine-technology-just-got-exposed-through-usb-ports/

JTAG: Joint Test Action Group

The JTAG specification is, without question, the most widely used serial protocol for communicating with embedded devices. Those hacks of hardware drive firmware use a JTAG interface. Once the JTAG communication pins have been located, a JTAG programmer can be attached to literally take over the embedded device through that serial interface. The embedded processor can be halted, single-stepped, any of its internal registers can be read or written, including the program counter. And of its RAM or ROM programming code can be extracted and modified. It is, essentially, a full remote debugging interface... which is exactly what it is used for.

It is typically implemented as a 4-wite interface with a clock, a mode, data-in and data-out.

Now get a load of this: Starting with the Platform Controller Hub used with all Skylake and subsequent Intel chipsets, Intel began offering an external JTAG interface to the IME through the motherboard's USB ports!! ... referring to this as Direct Connect Interface or DCI.

Known as the "God-mode Hack", next month, in December 2017, researchers from Positive Technologies intend to demonstrate that they have identified a way to run unsigned code in the Platform Controller Hub on any given motherboard from Skylake and after.

Positive Technologies has revealed that the latest IME versions are equipped with JTAG (Joint Test Action Group) debugging ports, which can be accessed through USB. These ports allow a user low-level access to the code running on a chip. This potentially means that anyone who can obtain brief USB access can exploit the firmware responsible for running the Intel Management Engine.

"Cryptojacking" craze that drains your CPU now done by 2,496 sites
https://arstechnica.com/information-technology/2017/11/drive-by-cryptomining-that-drains-cpus-picks-up-steam-with-aid-of-2500-sites/
https://gwillem.gitlab.io/2017/11/07/cryptojacking-found-on-2496-stores/

Independent security researcher Willem de Groot examined many websites and found 2,496 containing the coinhive monero cryptocurrency mining JavaScript... with a very interesting distribution:

85% of them are linked to just two mining accounts, while the remaining 15% are spread out over unique CoinHive accounts... though the ID tags for that third class, while different, all have the same format and pattern, suggesting that virtually the ENTIRE recent surge in cryptocurrency mining is due to the actions of a grand total of just THREE individuals or groups.

It's not that legitimate sites are jumping on the bandwagon to mint a bit of extra coinage at their visitor's expense, but that bad guys have found another revenue stream.

CoinHive could clearly shutdown, or change their embedded script to advise and seek consent... but there's a weird Hobbesian bargain here, since this permissionless mining is also HUGELY profitable for CoinHive, who retains the bulk of the mining proceeds. So, in effect, the few malicious actors are serving as agents of CoinHive.

HOST file to the rescue:
add 127.0.0.1 coin-hive.com coinhive.com

Web-based CryptoCurrency Mining, brought to you courtesy of: "WebAssembly"
As we mentioned at the time, just over two and a half years ago, the work on WebAssembly began in April 2015, when browser makers joined forces to create a binary (bytecode) format for browser-based web applications.

And, in a surprisingly short time, as of last month, all major browsers today support WebAssembly.

Over this past summer, Firefox and Chrome were the first major browsers to place WebAssembly into their stable development branches.

Then the Chromium-based browsers, like Opera and Vivaldi, inherited the feature as soon as it was added to the Chromium stable version.

And Apple's Safari 11.0 recently obtained WebAssembly, as did Microsoft Edge (EdgeHTML 16), the version that was recently included in the Windows 10 Fall Creators Update.

As it is today, JavaScript SOURCE is loaded into the browser and must then be compiled down into JavaSCript bytecode by "Just In time" (JIT) or other means. This takes time, wastes resources, and does not result in super-fast execution.

By comparison, WebAssembly is pre-compiled once and delivered FAR more compactly and is able to run from the moment it arrives... since all major browsers now understand how to interpret its bytecode.

And, WebAssembly also allows developers to write code in C, C++, or Rust, and then compile to wasm directly, without having to trans-compile (transpile) the code into JavaScript for distribution.

The precompiled format is dense and designed to be both fast to parse (~20 times faster than JS) and screamingly fast to execute.

The compiled bytecode has a well-defined format as well as a comfortable textual representation, so "Vide Source" on a webpage can show something meaningful.

http://webassembly.org/

Efficient and fast
The wasm stack machine is designed to be encoded in a size- and load-time-efficient binary format. WebAssembly aims to execute at native speed by taking advantage of common hardware capabilities available on a wide range of platforms.

Safe
WebAssembly describes a memory-safe, sandboxed execution environment that may even be implemented inside existing JavaScript virtual machines. When embedded in the web, WebAssembly will enforce the same-origin and permissions security policies of the browser.

Open and debuggable
WebAssembly is designed to be pretty-printed in a textual format for debugging, testing, experimenting, optimizing, learning, teaching, and writing programs by hand. The textual format will be used when viewing the source of wasm modules on the web.

Part of the open web platform
WebAssembly is designed to maintain the versionless, feature-tested, and backwards-compatible nature of the web. WebAssembly modules will be able to call into and out of the JavaScript context and access browser functionality through the same Web APIs accessible from JavaScript. WebAssembly also supports non-web embeddings.

Miscellany

Interactive C to Assembly instruction display
https://gcc.godbolt.org/

Asus RT-AC68U router firmware updated to v3.0.0.4.382.18547, fixing:

Security fixed
- Fixed KRACK vulnerability
- Fixed CVE-2017-14491: DNS - 2 byte heap based overflow
- Fixed CVE-2017-14492: DHCP - heap based overflow
- Fixed CVE-2017-14493: DHCP - stack based overflow
- Fixed CVE-2017-14494: DHCP - info leak
- Fixed CVE-2017-14495: DNS - OOM DoS
- Fixed CVE-2017-14496: DNS - DoS Integer underflow
- Fixed CVE-2017-13704 : Bug collision
- Fixed predictable session tokens, logged user IP validation, Logged-in information disclosure (special thanks for Blazej Adamczyk contribution)
- Fixed web GUI authorization vulnerabilities.
- Fixed AiCloud XSS vulnerabilities

New features
- HDD Hibernation
- URL filter black/white list
- Bandwidth limiter on guest network
- URL filter support https website

Authenticating myself to HOVER:

- Received a PIN via eMail.
- Because I have a time-based 2FA, we needed to talk and I needed to provide the authentication in real time.

SpinRite

Dave L in San Rafael, CA
Subject: SpinRite on Hybrid Hard Drives
Date: 05 Nov 2017 14:37:45
:

My new laptop has a hybrid hard drive on which I have been afraid to run SpinRite in fear that the solid state portion will be degraded by heavy read/writes.

Can you advise listeners of the best way to run SpinRite on such a drive?

Closing The Loop

Christopher Ursich @chrisursich
@SGgrc The installer I downloaded today (Nov 11) from LastPass was signed on Oct 3 but with a cert that expired Oct 29. Is good practice to trust or not? Continually concerned about LastPass becoming sloppy.

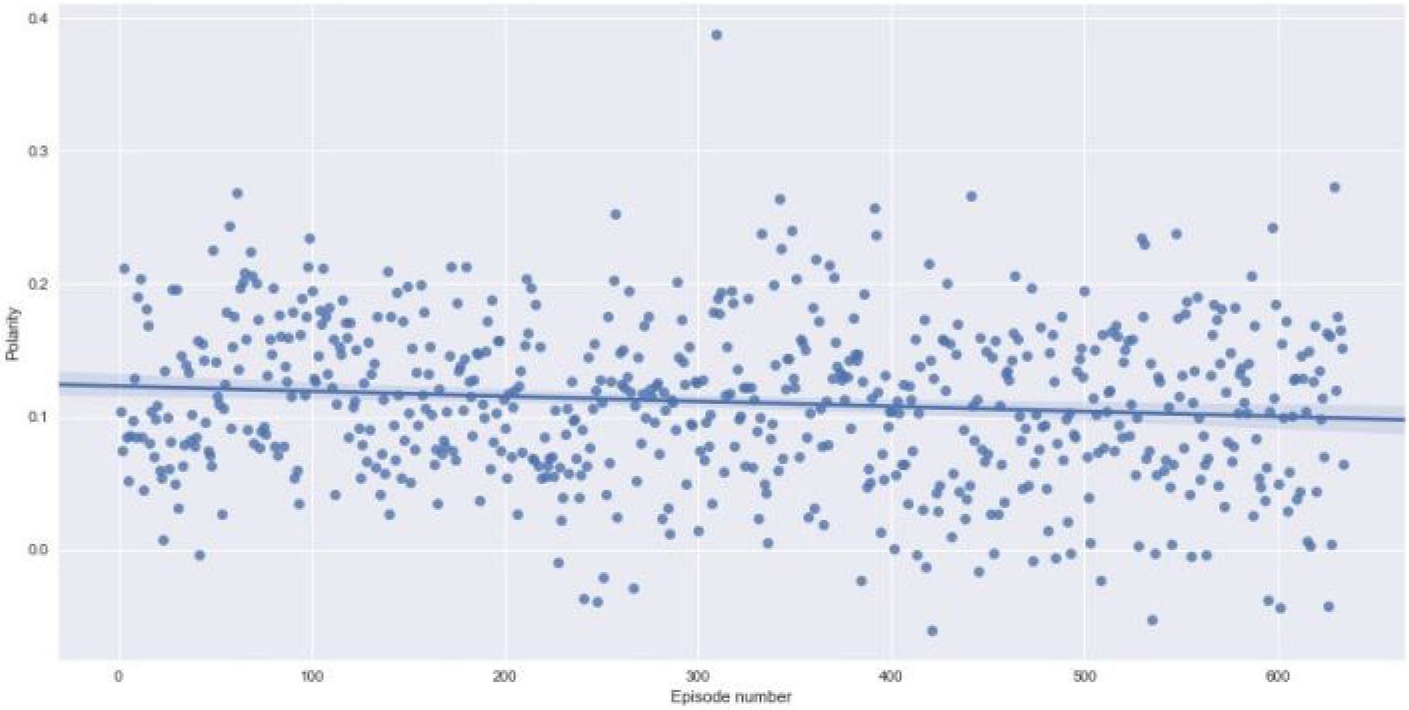
James Nahrgang @JamesNahrgang
@SGgrc Steve, I've wondered for some time now, how do you respond when talking to the average person and they say something like, "I don't have anything to hide, therefore, I don't need security"?

David Lemire @dlemire60
@SGgrc, discussion of disabling Intel ME in SN-636 created a terminology question. If killing a phone is "bricking", is killing a motherboard "planking"?

Damashe Thomas @Damashe
@SGgrc When Generating new ssh keys, what is your recommended key type & size? i.e ECDSA or ed25199

Marc Boorshtein @mlbiam
@SGgrc not sure favicon.ico is a good login test, usually anonymous since it's displayed on login pages. Tested that it's accurate?

Luis Zepeda @_Xepe
@leolaporte Hey Leo!, I remember you asked @SGgrc if He believed that security was getting better across all these years of Security Now! Well, I ran some natural language processing and sentiment analysis tools, and found: (spoiler: it's been getting slightly worse)



Ronald A. Suchland @RSuchland
@GibsonResearch I cannot find anything to stop Leak Test. Win7 64 bit. Lavasoft locks up the computer.

Pete Aitch @PeteAitch
Hi @SGgrc on yr podcast you’ve referred several times to keeping a laptop in the freezer - wouldn’t the cold damage the battery etc? Thanks!

Chris in Germany
Subject: Comment on Steve's comment last episode
Date: 04 Nov 2017 11:24:06
Hello Leo and Steve!
Steve, you commented in the last episode, that users should never download anything, even from trusted sources. Does that include the show notes you and Leo upload to your show? /s
To be fair, I don't think this advice is feasible for the average user and sounds stallman-esque. Could you elaborate on that further? How am I supposed to use the internet without downloading anything.

Thanks a lot, I appreciate the podcast and your experience!

Schneier on Equifax

https://www.schneier.com/blog/archives/2017/11/me_on_the_equif.html

“Me on the Equifax Breach”

Last week, I testified before the House Energy and Commerce committee on the Equifax hack. You can watch the video here. And you can read my written testimony below.

Testimony and Statement for the Record of Bruce Schneier
Fellow and Lecturer, Belfer Center for Science and International Affairs, Harvard Kennedy School Fellow, Berkman Center for Internet and Society at Harvard Law School
Hearing on "Securing Consumers' Credit Data in the Age of Digital Commerce"
Before the Subcommittee on Digital Commerce and Consumer Protection Committee on Energy and Commerce United States House of Representatives
1 November 2017
2125 Rayburn House Office Building
Washington, DC 20515

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the security of credit data. My name is Bruce Schneier, and I am a security technologist. For over 30 years I have studied the technologies of security and privacy. I have authored 13 books on these subjects, including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your* World (Norton, 2015). My popular newsletter Crypto-Gram and my blog *Schneier on* Security are read by over 250,000 people.

Additionally, I am a Fellow and Lecturer at the Harvard Kennedy School of Government -- where I teach Internet security policy -- and a Fellow at the Berkman Klein Center for Internet and Society at Harvard Law School. I am a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of Electronic Privacy Information Center and VerifiedVoting.org. I am also a special advisor to IBM Security and the Chief Technology Officer of IBM Resilient.

I am here representing none of those organizations, and speak only for myself based on my own expertise and experience.

I have eleven main points:

1. The Equifax breach was a serious security breach that puts millions of Americans at risk.
Equifax reported that 145.5 million US customers, about 44% of the population, were impacted by the breach. (That's the original 143 million plus the additional 2.5 million disclosed a month later.) The attackers got access to full names, Social Security numbers, birth dates, addresses, and driver's license numbers.

This is exactly the sort of information criminals can use to impersonate victims to banks, credit card companies, insurance companies, cell phone companies and other businesses vulnerable to fraud. As a result, all 143 million US victims are at greater risk of identity theft, and will remain at risk for years to come. And those who suffer identify theft will have problems for months, if not years, as they work to clean up their name and credit rating.

2. Equifax was solely at fault.
This was not a sophisticated attack. The security breach was a result of a vulnerability in the software for their websites: a program called Apache Struts. The particular vulnerability was fixed by Apache in a security patch that was made available on March 6, 2017. This was not a minor vulnerability; the computer press at the time called it "critical." Within days, it was being used by attackers to break into web servers. Equifax was notified by Apache, US CERT, and the Department of Homeland Security about the vulnerability, and was provided instructions to make the fix.

Two months later, Equifax had still failed to patch its systems. It eventually got around to it on July 29. The attackers used the vulnerability to access the company's databases and steal consumer information on May 13, over two months after Equifax should have patched the vulnerability.

The company's incident response after the breach was similarly damaging. It waited nearly six weeks before informing victims that their personal information had been stolen and they were at increased risk of identity theft. Equifax opened a website to help aid customers, but the poor security around that -- the site was at a domain separate from the Equifax domain -- invited fraudulent imitators and even more damage to victims. At one point, the official Equifax communications even directed people to that fraudulent site.

This is not the first time Equifax failed to take computer security seriously. It confessed to another data leak in January 2017. In May 2016, one of its websites was hacked, resulting in 430,000 people having their personal information stolen. Also in 2016, a security researcher found and reported a basic security vulnerability in its main website. And in 2014, the company reported yet another security breach of consumer information. There are more.

3. There are thousands of data brokers with similarly intimate information, similarly at risk. Equifax is more than a credit reporting agency. It's a data broker. It collects information about all of us, analyzes it all, and then sells those insights. It might be one of the biggest, but there are 2,500 to 4,000 other data brokers that are collecting, storing, and selling information about us -- almost all of them companies you've never heard of and have no business relationship with.

The breadth and depth of information that data brokers have is astonishing. Data brokers collect and store billions of data elements covering nearly every US consumer. Just one of the data brokers studied holds information on more than 1.4 billion consumer transactions and 700 billion data elements, and another adds more than 3 billion new data points to its database each month.

These brokers collect demographic information: names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of things we've purchased, when we've purchased them, and how we paid for them. They keep track of deaths, divorces, and diseases in our families. They collect everything about what we do on the Internet.

4. These data brokers deliberately hide their actions, and make it difficult for consumers to learn about or control their data.

If there were a dozen people who stood behind us and took notes of everything we purchased, read, searched for, or said, we would be alarmed at the privacy invasion. But because these companies operate in secret, inside our browsers and financial transactions, we don't see them and we don't know they're there.

Regarding Equifax, few consumers have any idea what the company knows about them, who they sell personal data to or why. If anyone knows about them at all, it's about their business as a credit bureau, not their business as a data broker. Their website lists 57 different offerings for business: products for industries like automotive, education, health care, insurance, and restaurants.

In general, options to "opt-out" don't work with data brokers. It's a confusing process, and doesn't result in your data being deleted. Data brokers will still collect data about consumers who opt out. It will still be in those companies' databases, and will still be vulnerable. It just won't be included individually when they sell data to their customers.

5. The existing regulatory structure is inadequate.
Right now, there is no way for consumers to protect themselves. Their data has been harvested and analyzed by these companies without their knowledge or consent. They cannot improve the security of their personal data, and have no control over how vulnerable it is. They only learn about data breaches when the companies announce them -- which can be months after the breaches occur -- and at that point the onus is on them to obtain credit monitoring services or credit freezes. And even those only protect consumers from some of the harms, and only those suffered after Equifax admitted to the breach.

Right now, the press is reporting "dozens" of lawsuits against Equifax from shareholders, consumers, and banks. Massachusetts has sued Equifax for violating state consumer protection and privacy laws. Other states may follow suit.

If any of these plaintiffs win in the court, it will be a rare victory for victims of privacy breaches against the companies that have our personal information. Current law is too narrowly focused on people who have suffered financial losses directly traceable to a specific breach. Proving this is difficult. If you are the victim of identity theft in the next month, is it because of Equifax or does the blame belong to another of the thousands of companies who have your personal data? As long as one can't prove it one way or the other, data brokers remain blameless and liability free.

Additionally, much of this market in our personal data falls outside the protections of the Fair Credit Reporting Act. And in order for the Federal Trade Commission to levy a fine against

Equifax, it needs to have a consent order and then a subsequent violation. Any fines will be limited to credit information, which is a small portion of the enormous amount of information these companies know about us. In reality, this is not an effective enforcement regime. Although the FTC is investigating Equifax, it is unclear if it has a viable case.

6. The market cannot fix this because we are not the customers of data brokers.
The customers of these companies are people and organizations who want to buy information: banks looking to lend you money, landlords deciding whether to rent you an apartment, employers deciding whether to hire you, companies trying to figure out whether you'd be a profitable customer -- everyone who wants to sell you something, even governments. Markets work because buyers choose from a choice of sellers, and sellers compete for buyers. None of us are Equifax's customers. None of us are the customers of any of these data brokers. We can't refuse to do business with the companies. We can't remove our data from their databases. With few limited exceptions, we can't even see what data these companies have about us or correct any mistakes.

We are the product that these companies sell to their customers: those who want to use our personal information to understand us, categorize us, make decisions about us, and persuade us.

Worse, the financial markets reward bad security. Given the choice between increasing their cybersecurity budget by 5%, or saving that money and taking the chance, a rational CEO chooses to save the money. Wall Street rewards those whose balance sheets look good, not those who are secure. And if senior management gets unlucky and the a public breach happens, they end up okay. Equifax's CEO didn't get his $5.2 million severance pay, but he did keep his $18.4 million pension. Any company that spends more on security than absolutely necessary is immediately penalized by shareholders when its profits decrease.

Even the negative PR that Equifax is currently suffering will fade. Unless we expect data brokers to put public interest ahead of profits, the security of this industry will never improve without government regulation.

7. We need effective regulation of data brokers.
In 2014, the Federal Trade Commission recommended that Congress require data brokers be more transparent and give consumers more control over their personal information. That report contains good suggestions on how to regulate this industry.

First, Congress should help plaintiffs in data breach cases by authorizing and funding empirical research on the harm individuals receive from these breaches.

Specifically, Congress should move forward legislative proposals that establish a nationwide "credit freeze" -- which is better described as changing the default for disclosure from opt-out to opt-in -- and free lifetime credit monitoring services. By this I do not mean giving customers free credit-freeze options, a http://money.cnn.com/2017/09/15/pf/warren-schatz-equifax/index.html proposal by Senators Warren and Schatz, but that the default should be a credit freeze.
The credit card industry routinely notifies consumers when there are suspicious charges. It is obvious that credit reporting agencies should have a similar obligation to notify consumers when

there is suspicious activity concerning their credit report.

On the technology side, more could be done to limit the amount of personal data companies are allowed to collect. Increasingly, privacy safeguards impose "data minimization" requirements to ensure that only the data that is actually needed is collected. On the other hand, Congress should not create a new national identifier to replace the Social Security Numbers. That would make the system of identification even more brittle. Better is to reduce dependence on systems of identification and to create contextual identification where necessary.

Finally, Congress needs to give the Federal Trade Commission the authority to set minimum security standards for data brokers and to give consumers more control over their personal information. This is essential as long as consumers are these companies' products and not their customers.

8. Resist complaints from the industry that this is "too hard."
The credit bureaus and data brokers, and their lobbyists and trade-association representatives, will claim that many of these measures are too hard. They're not telling you the truth.
Take one example: credit freezes. This is an effective security measure that protects consumers, but the process of getting one and of temporarily unfreezing credit is made deliberately onerous by the credit bureaus. Why isn't there a smartphone app that alerts me when someone wants to access my credit rating, and lets me freeze and unfreeze my credit at the touch of the screen? Too hard? Today, you can have an app on your phone that does something similar if you try to log into a computer network, or if someone tries to use your credit card at a physical location different from where you are.

Moreover, any credit bureau or data broker operating in Europe is already obligated to follow the more rigorous EU privacy laws. The EU General Data Protection Regulation will come into force, requiring even more security and privacy controls for companies collecting storing the personal data of EU citizens. Those companies have already demonstrated that they can comply with those more stringent regulations.

Credit bureaus, and data brokers in general, are deliberately not implementing these 21st-century security solutions, because they want their services to be as easy and useful as possible for their actual customers: those who are buying your information. Similarly, companies that use this personal information to open accounts are not implementing more stringent security because they want their services to be as easy-to-use and convenient as possible.

9. This has foreign trade implications.
The Canadian Broadcast Corporation reported that 100,000 Canadians had their data stolen in the Equifax breach. The British Broadcasting Corporation originally reported that 400,000 UK consumers were affected; Equifax has since revised that to 15.2 million.
Many American Internet companies have significant numbers of European users and customers, and rely on negotiated safe harbor agreements to legally collect and store personal data of EU citizens.

The European Union is in the middle of a massive regulatory shift in its privacy laws, and those agreements are coming under renewed scrutiny. Breaches such as Equifax give these European regulators a powerful argument that US privacy regulations are inadequate to protect their citizens' data, and that they should require that data to remain in Europe. This could significantly harm American Internet companies.

10. This has national security implications.
Although it is still unknown who compromised the Equifax database, it could easily have been a foreign adversary that routinely attacks the servers of US companies and US federal agencies with the goal of exploiting security vulnerabilities and obtaining personal data.

When the Fair Credit Reporting Act was passed in 1970, the concern was that the credit bureaus might misuse our data. That is still a concern, but the world has changed since then. Credit bureaus and data brokers have far more intimate data about all of us. And it is valuable not only to companies wanting to advertise to us, but foreign governments as well. In 2015, the Chinese breached the database of the Office of Personal Management and stole the detailed security clearance information of 21 million Americans. North Korea routinely engages in cybercrime as way to fund its other activities. In a world where foreign governments use cyber capabilities to attack US assets, requiring data brokers to limit collection of personal data, securely store the data they collect, and delete data about consumers when it is no longer needed is a matter of national security.

11. We need to do something about it.
Yes, this breach is a huge black eye and a temporary stock dip for Equifax -- this month. Soon, another company will have suffered a massive data breach and few will remember Equifax's problem. Does anyone remember last year when Yahoo admitted that it exposed personal information of a billion users in 2013 and another half billion in 2014?

Unless Congress acts to protect consumer information in the digital age, these breaches will continue.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.