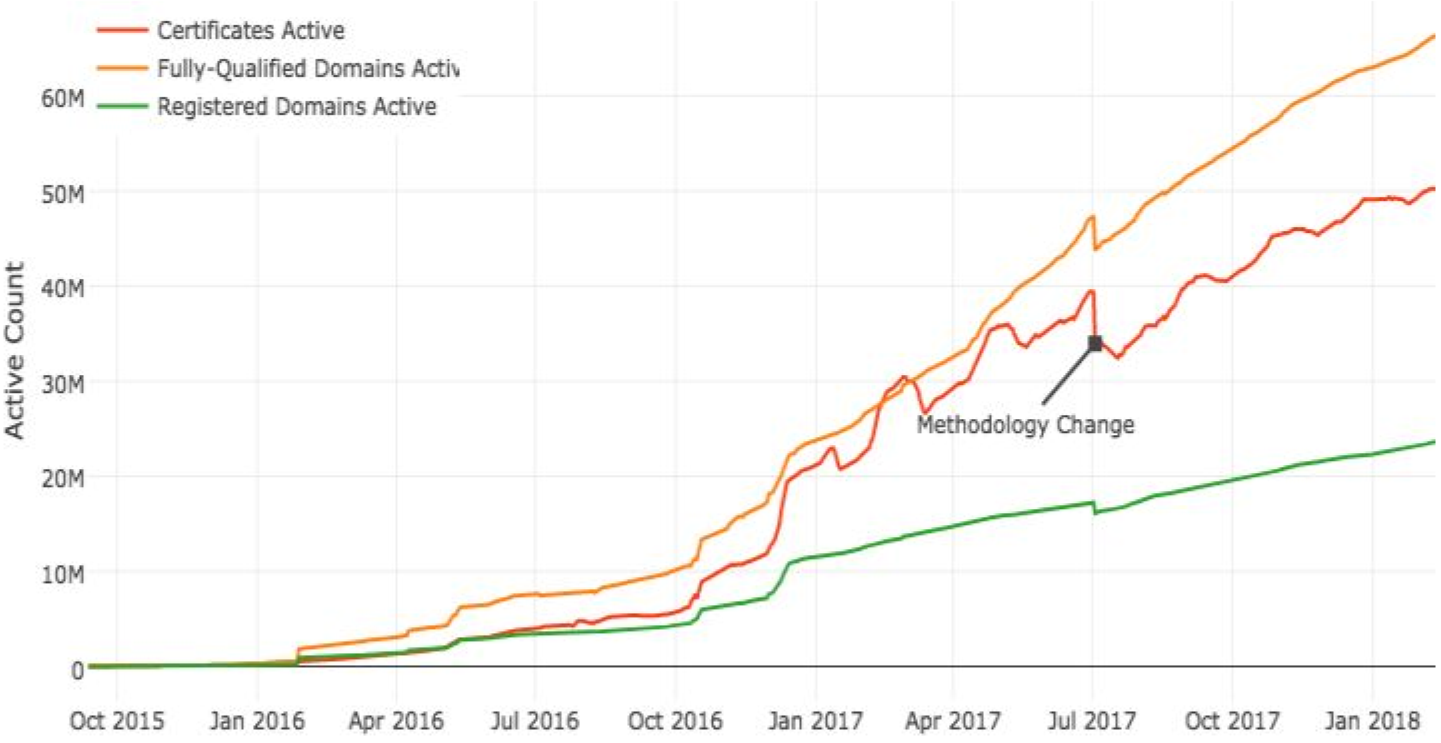
Security Now! #651 - 02-20-18
Russian Meddling Technology

This week on Security Now!

This week we examine and discuss the appearance of new forms of Meltdown and Spectre attacks, the legal response against Intel, the adoption of new cybersecurity responsibility in New York, some more on Salon and authorized cryptomining, more on software cheating auto emissions, a newly revealed instance of highly profitable mal-mining, checking in on Lets Encrypts steady growth, the first crack of Windows uncrackable UWP system, Apple' whacky Telugu Unicode attacks, a frightening "EternalBlue" experiment, another aspect of cryptomining annoyance, a note now that Chrome's new advertising controls are in place, a bit of closing the loop with our listeners. And then we conclude with a look into the technology that was revealed in last week's indictment of election meddling Russians... and from a practical technology standpoint, the feasibility of anything changing.

Lets Encrypt Domain Growth



Let's Encrypt Hits 50 Million Active Certificates and Counting
One way to count is by “fully qualified domains active”—in other words, different names covered by non-expired certificates. This is now at 66 million. This metric can overcount sites; while most people would say that eff.org and www.eff.org are the same website, they count as two different names here.

Security News

From the "attacks never get worse they only ever get better" department...

The proud Princeton professor's tweet:

> My PhD student @carolinetrippel developed research tools/techniques to synthesize security exploits. Yes, her tools find #Spectre & #Meltdown. But they've also discovered 2 new related-but-distinct vulnerabilities using cache coherence protocols!
> https://arxiv.org/abs/1802.03802

The new research paper by researchers at Princeton and Nvidia, titled: "MeltdownPrime and SpectrePrime: Automatically-Synthesized Attacks Exploiting Invalidation-Based Coherence Protocols"

The researchers developed a tool to formalize the underlying architectural characteristics which enabled the creation of the Meltdown and Spectre side-channel attacks. Although Intel may NOW have such tools at their disposal (one would hope) it's clear that they have not, previously. There is some speculation that this research may lead CPU designers such as Intel to re-verify their recently developed hardware mitigations. The new tool allowed the researchers to synthesize a [new] software-attack based on a description of a CPU's microarchitecture and an execution pattern that could be attacked. Though the software attack is specific to a microarchitecture and represent exploits "in their most abstracted form", they can be used to develop fully fledged attacks.

And, in fact, the researcher did develop new but different related attacks which they named "MeltdownPrime" and "SpectrePrime".

Abstract:

> The recent Meltdown and Spectre attacks highlight the importance of automated verification techniques for identifying hardware security vulnerabilities. We have developed a tool for automatically synthesizing microarchitecture-specific programs capable of producing any user-specified hardware execution pattern of interest. Our tool takes two inputs: (i) a formal description of a microarchitecture in a domain-specific language (almost identical to mspec from recent work), and (ii) a formal description of a microarchitectural execution pattern of interest, e.g. a threat pattern. All programs synthesized by our tool are capable of producing the specified execution pattern on the supplied microarchitecture.

:(Intel has had 32 Spectre and Meltdown class action suits filed against it.
From Intel's 10-K Annual Report filing with the US Securities and Exchange Commission (SEC)

(PDF page 124 of 201) Litigation related to Security Vulnerabilities:
In June 2017, a Google research team notified us and other companies that it had identified security vulnerabilities (now commonly referred to as “Spectre” and “Meltdown”) that affect many types of microprocessors, including our products. As is standard when findings like these are presented, we worked together with other companies in the industry to verify the research and develop and validate software and firmware updates for impacted technologies.

On January 3, 2018, information on the security vulnerabilities was publicly reported, before software and firmware updates to address the vulnerabilities were made widely available. Numerous lawsuits have been filed against Intel and, in certain cases, our executives and directors, in U.S. federal and state courts and in certain courts in other countries relating to the Spectre and Meltdown security vulnerabilities.

As of February 15, 2018, 30 customer class action lawsuits and two securities class action lawsuits have been filed. The customer class action plaintiffs, who purport to represent various classes of end users of our products, generally claim to have been harmed by Intel's actions and/or omissions in connection with the security vulnerabilities and assert a variety of common law and statutory claims seeking monetary damages and equitable relief. The securities class action plaintiffs, who purport to represent classes of acquirers of Intel stock between July 27, 2017 and January 4, 2018, generally allege that Intel and certain officers violated securities laws by making statements about Intel's products and internal controls that were revealed to be false or misleading by the disclosure of the security vulnerabilities. Additional lawsuits and claims may be asserted on behalf of customers and shareholders seeking monetary damages or other related relief. We dispute the claims described above and intend to defend the lawsuits vigorously. Given the procedural posture and the nature of these cases, including that the proceedings are in the early stages, that alleged damages have not been specified, that uncertainty exists as to the likelihood of a class or classes being certified or the ultimate size of any class or classes if certified, and that there are significant factual and legal issues to be resolved, we are unable to make a reasonable estimate of the potential loss or range of losses, if any, that might arise from these matters.

<<sigh>>

New York cybersecurity laws begin to take effect
https://www.cyberscoop.com/new-york-financial-cybersecurity-law-deadline-february-2018/

Last week the senior executes -- the chairman of the board of directors or a senior officer like the CEO -- of over 3,000 banks, insurers and other financial services organizations doing business in New York were required to personally certify that their computer networks are protected by a cybersecurity program appropriate to their organization's risk profile.

The new regulations from New York’s Department of Financial Services (DFS) are designed to drive accountability and oversight of the organization's cybersecurity to the top of the organization's power structure.

The new rules came into force in March 2017, with a series of staggered implementation deadlines that stretch into next year.

Last week's certification which covers calendar year 2017, includes the half-dozen most straightforward elements of the new rules — those which came into force in August last year. Since then, financial institutions covered by the rules are required to have:

- Adopted a cybersecurity program appropriate to the bank’s risk profile.

- Adopted cybersecurity policies designed to protect the bank’s information systems and the customer data they hold.

- Appointed a chief information security officer “responsible for overseeing and implementing the [bank’s] cybersecurity program and enforcing its cybersecurity policy.”

- Engaged qualified cybersecurity personnel (either staff or contractors) to work with the CISO managing the company’s risk.

- Developed an incident response plan.

- Taken steps to control privileged access to its IT network.

DFS has scheduled the next tier of more onerous requirements further out along the two year transition timetable. Just two weeks away, March 1 is the second implementation deadline, when a further set of provisions come into force, requiring regulated banks and other financial service providers to:

- Implement either continuous monitoring or periodic penetration testing and vulnerability assessments of its IT network.

- Conduct a full scale risk assessment of its information systems, to inform its cybersecurity program.

- Implement multi-factor authentication for remote access; and more widely as indicated by its risk assessment.

- Provide regular cybersecurity awareness training for staff.

- Begin annual reporting from the CISO to the board of directors.

Salon's and Cryptomining

I've read several interviews of Jordan Hoffner, CEO of Salon Media Group.

The most curious and disingenuous thing he/they have said is about CPU usage percentage... with people complaining about their processor being pinned.

JavaScript based cryptomining is going to be atrociously low yield.

It's going to be incredibly wasteful of the system's resources... so that even if/when the user's CPU is pinned the site will still not be generating useful revenue.

So, we should not base too much on this first generation of JavaScript mining. What we need is low-level mining built into browsers with access to the system's GPU resources.

Authorized Mining by Coinhive: https://authedmine.com/

> A Note to Adblock and Antivirus Vendors
>
> There is no need to block AuthedMine.com or any scripts hosted on this domain.
>
> AuthedMine.com offers a Monero miner that can be embeded into other Websites. This miner will only ever run after an explicit opt-in from the user. The miner never starts without this opt-in.
>
> We implemented a secure token to enforce this opt-in on our servers. It is not circumventable by any means and we pledge that it will stay this way. The opt-in token is only valid for the current browser session (at max 24 hours) and the current domain. The user will need to opt-in again in the next session or on a different domain.
>
> The opt-in notice is hosted on our servers and can not be changed by website owners. There's no way a website owner can start mining without the user knowing.
>
> Click here to see how the Opt-In looks like: [start mining].
>
> A detailed and technical explanation of the Opt-In can be found in our documentation.
>
> We believe that browser based mining can be a viable alternative for intrusive and annoying ads if used honestly and with consent by the user. We kindly ask Adblock and Antivirus Vendors to support us.
>
> Please help us build a better web.
>
> Cheers,
> Coinhive

https://coinhive.com/documentation/authedmine

> AuthedMine - A Non-Adblocked Miner
>
> Shortly after the launch of Coinhive, several Adblockers have begun blocking our miner. This is unfortunate because we intended Coinhive to be an alternative to ads, precisely for users with adblockers.
>
> However, we have to acknowledge that the decision to block Coinhive was understandable as it was possible to run the miner on a webpage without asking the visitor for consent or even informing them. Even some antiviruses now consider our JavaScript miner as a threat, which makes it difficult for website owners to use Coinhive at all.
>
> We implemented AuthedMine as a solution to these problems. The JavaScript Miner, Simple UI and Captcha, when loaded from authedmine.com, will never start without asking for consent from the user or (for the Simple UI and the Captcha) letting them explicitly start mining through a click.

> We realize this opt-in may be clunky and not fit all too well with your use case, but we strongly believe that being honest with the user will ultimately be beneficial - for users and website owners alike.
>
> Neither the JavaScript files on authedmine.com nor the domain names are currently blocked by any adblockers or antiviruses. We will talk to adblock and antivirus vendors so it will hopefully stay this way.

Reuters reports that a German newspaper, citing confidential documents...
... reported Sunday that the U.S. investigators probing Mercedes maker Daimler have found that its cars were equipped with software which may have help them to pass diesel emissions tests.

Daimler, which faces ongoing investigations by U.S. and German authorities into excess diesel emissions, has said investigations could lead to significant penalties and recalls.

- The German newspaper wrote that the documents showed that U.S. investigators had found several software functions that helped Daimler cars pass emissions tests, including one which switched off emissions cleaning after 26 km of driving.

- Another function under scrutiny allowed the emissions cleaning system to recognize whether the car was being tested based on speed or acceleration patterns.

- The paper also cited emails from Daimler engineers questioning whether these software functions were legal.

Hackers make $3.4 Million after installing Monero mining software on Jenkins servers
On Friday, Israeli security firm Check Point announced it uncovered the footprint of a large hacking operation targeting Jenkins servers left connected to the Internet...
(of which there are ~25,000!... but more on that in a minute!)

First a bit of Java terminology: Serialization and Deserialization in Java

> Serialization is a process of converting an object into a sequence of bytes which can be persisted to a disk or database or can be sent through streams. The reverse process of creating object from sequence of bytes is called deserialization.

April 26th of 2017: SECURITY-429 / CVE-2017-1000353
CLI: Unauthenticated remote code execution

An unauthenticated remote code execution vulnerability allowed attackers to transfer a serialized Java SignedObject object to the remoting-based Jenkins CLI, that would be deserialized using a new ObjectInputStream, bypassing the existing blacklist-based protection mechanism.

SignedObject has been added to the remoting blacklist.

In Jenkins 2.54, the remoting-based CLI protocol was deprecated and a new, HTTP based protocol introduced as the new default, in addition to the existing SSH-based CLI. This feature has been backported to Jenkins 2.46.2. It is strongly recommended that users upgrading Jenkins disable the remoting-based CLI, and use the one of the other modes (HTTP or SSH) instead

Despite having been fixed over a year ago, attackers are leveraging CVE-2017-1000353, a vulnerability in the Jenkins Java deserialization implementation that allows attackers to run malicious code remotely without needing to authenticate first.

Check Point says hackers used this vulnerability to make Jenkins servers download and install a Monero miner (minerxmr.exe).

The miner was being downloaded from an IP address located in China. It is unclear if this is the attacker's server, or a compromised server used to host the miner on behalf of the hackers.

The attackers have been active for months. This has allowed them to mine and already cash out over 10,800 Monero, which is over $3.4 million, at the time of writing.

Note that with a remote code execution vulnerability bad guys could have gotten up to all sorts of very serious mischief. But what did they choose to do with this remote execution vulnerability? They mined cryptocurrency.

Bleeping Computer had some terrific summary reporting on this. Get a load of this (from Bleeping Computer)

<quote> Over 25,000 Jenkins servers left exposed online

Attackers aren't the only ones who've noticed the large number of Jenkins servers available online. In mid-January, security researcher Mikail Tunç published research highlighting that there were over 25,000 Jenkins servers left exposed to Internet connections at the time of his research.

Also on Friday, FireEye released new research on other hackers leveraging the CVE-2017-10271 flaw to infect Oracle WebLogic servers with malware. This vulnerability has been under active exploitation since early December 2017, and one group has already made more than $226,000.

Besides Jenkins and Oracle WebLogic servers, hackers are also targeting Ruby on Rails, PHP, and IIS servers, also deploying Monero-mining malware. Trend Micro fears that two recently disclosed CouchDB vulnerabilities will also soon be exploited in the same way.

Monero-mining malware is already this year's biggest malware trend/problem, with numerous malware distribution campaigns spreading such payloads on any unsecured computer/server crooks can get their hands on.

Perhaps we should begin referring to all of these as "Willie Sutton Attacks" -- going where the money is. Whereas Willie famously robbed banks to steal money, today's hackers are increasingly stealing processing power and turning it into money.

From the "Some secrets cannot be kept" department:
https://torrentfreak.com/pirates-crack-microsofts-uwp-protection-five-layers-of-drm-defeated-180215/

The first "Uncrackable" Windows 10 Universal Windows Platform (UWP) game has reportedly been liberated from its captivity.

The game is "Zoo Tycoon Ultimate Animal Collection" which the cracking group CODEX says they cracked by successfully penetrating five separate layers of DRM protection. It's not absolutely clear whether some specific flaw in this particular game's protection may have allowed a way in. But what is clear is that, as this podcast has often observed, the task of protecting something which needs to be autonomously used by an endpoint is inherently impossible.

The CODEX group notes that it would probably be a good idea to keep this executable from phoning home (or phoning anywhere) by blocking its access to the Internet.

iOS and macOS both got updates:
The folks making the AlohaBrowser for iOS and Android discovered the a heap corruption could be triggered by exposing either OS to two specific Unicode characters. This is one of those "crash on view" bugs.

Known as the "Telugu character bug" (Telugu is a language native to south India and its 3rd most spoken language), it affected devices running the latest public version of Apple's software across many device technologies. So updates available today include iOS 11.2.6 for iPhone and iPad, tvOS 11.2.6 for Apple TV, watchOS 4.2.3 for Apple Watch, and macOS 10.13.3 supplemental update for Mac.

Apple referred to these two magically endowed characters as a “maliciously crafted string.”

According to Apple, the iOS update also fixes “an issue where some third-party apps could fail to connect to external accessories,” so that may be welcome news to some folks may have that fixed.

The Unicode foreign language symbol is NOT present in beta versions of iOS 11.3, so it was on the road to being fixed when Apple was forced to push out an interim fix because it was being actively exploited in the wild.

All the techie details:
https://manishearth.github.io/blog/2018/02/15/picking-apart-the-crashing-ios-string/

"EternalGlue": A rebuilt NotPetya gets its first execution outside of the lab
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/february/eternalglue-part-two-a-rebuilt-notpetya-gets-its-first-execution-outside-of-the-lab/

EternalBlue uses the NSA's leaked SMBv1 exploit.

In June 2017, we were asked by a client to rebuild NotPetya from scratch.

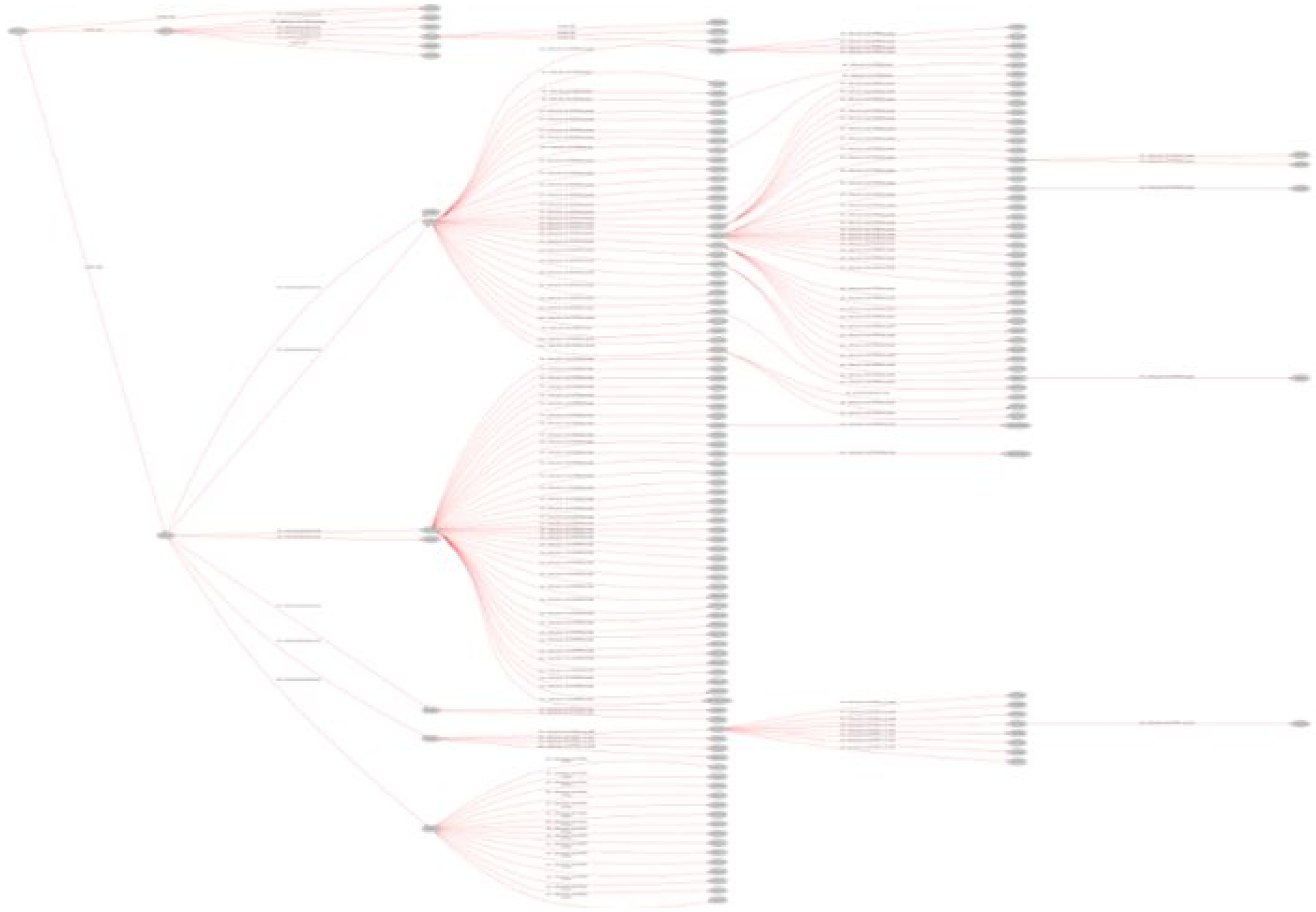
Instead of the data destruction payload, they asked for telemetry and safeguards. Why? Because they wanted to measure what the impact of NotPetya would have been.

Since part one of this story (which you can read here), we've completed the first phase of live testing in a secure environment deployed by our client.
It has been a marathon, not a sprint

By the time we emerged from testing the code and the associated safeguards in December 2017, we had already been working with our customer in the lab for a number of months.

This slow and steady approach has ensured everything works as intended and the quality of telemetry is sufficient to answer the client's questions.

Christmas comes early: EternalGlue's first outing



On 7 December, EternalGlue got its first outing on the customer's engineering network i.e. live but not corporate.

The result? More data than one could have imagined and interesting insights as to propagation in live environments.

The headlines were from phase one of the experiment were:

- The customer ran it on one machine in their engineering network with no privileges.
- It found three machines unpatched.
- It exploited those three machines to obtain kernel level access.
- It infected those three machines.
- Within ten minutes it had gone through the entire engineering network using recovered/stolen credentials.
- It then took the domain about two minutes later.
- 107 hosts were owned in roughly 45 minutes before the client initiated the kill and remove switch.

Another annoyance from BitCoin mining: RF Interference.
https://thenextweb.com/hardfork/2018/02/16/fcc-threatens-arrest-hardware-seizure-for-those-using-popular-bitcoin-miner/
T-Mobile complained that massive RF interference emanating from a local residence at 700 Mhz was significantly interfering with the delivery of the companies cellular services. The FCC's enforcement bureau said continued use of the "Antminer s4" — or, presumably others that interfered with the same 700 MHz frequency — would be subject to fines, criminal prosecution or seizure of the equipment.

"BrowseAloud" breach injected Monero/Coinhive mining into 4,275 websites.
Remember last week's coverage...

A large proportion of the sites hosting the illicit Coinhive injection were governmental a browser-based cryptomining is extremely inefficient. So in something of a funny quip, it was noted that browser-based cryptomining relies upon placing the mining code on sites people actually visit: The culprits behind the widespread attack only minted a grand total of $24.

Under the hood: How Chrome's ad filtering works
https://blog.chromium.org/2018/02/how-chromes-ad-filtering-works.html

Chrome's new "intrusive ad blocking" went live last Thursday.

A survey of 40,000 Internet users in North America was taken by the "Coalition for Better Ads".

The most intrusive ads were "prestitial" page covering ads with a countdown and flashing animated ads.

Google notes that while some problematic ads are sourced by the advertising supplier, the majority of problematic as experiences are under the control of and at the specification of the site's owner -- such as high ad density and the prestitial page covers.

Google writes: "This result led to the approach Chrome takes to protect users from many of the intrusive ad experiences identified by the Better Ads Standards: evaluate how well sites comply with the Better Ads Standards, inform sites of any issues encountered, provide the opportunity for sites to address identified issues, and remove ads from sites that continue to maintain a problematic ads experience."

Evaluating sites for violations
Sites are evaluated by examining a sample of pages from the site. Depending on how many violations of the Better Ads Standards are found, the site will be evaluated as having a status of Passing, Warning, or Failing. The evaluation status of sites can be accessed via the Ad Experience Report API. Site owners can also see more detailed results, such as the specific violations of the Better Ads Standards that were found, via the Ad Experience Report in Google’s Search Console. From the Report site owners can also request that their site be re-reviewed after they have addressed the non-compliant ad experiences.

Filtering on sites at the network level
At a technical level, when a Chrome user navigates to a page, Chrome’s ad filter first checks if that page belongs to a site that fails the Better Ads Standards. If so, network requests on the page — such as those for JavaScript or images — are checked against a list of known ad-related URL patterns. If there is a match, Chrome will block the request, preventing the ad from displaying on the page. This set of patterns is based on the public EasyList filter rules, and includes patterns matching many ad providers including Google’s own ad platforms, AdSense and DoubleClick.

What this looks like in Chrome
Chrome will automatically block ads on sites that fail the Better Ads Standards, using the approach described above. When at least one network request has been blocked, Chrome will show the user a message indicating that ad blocking has occurred as well as an option to disable this setting by selecting “allow ads on this site.” For desktop users, the notification in Chrome's address bar will look similar to Chrome's existing pop-up blocker. Android users will see message in a small infobar at the bottom of their screen, and can tap on “details” to see more information and override the default setting.

Early results show positive progress for users
While the result of this action is that Chrome users will not see ads on sites that consistently violate the Better Ads Standards, our goal is not to filter any ads at all but to improve the experience for all web users. As of February 12, 42% of sites which were failing the Better Ads Standards have resolved their issues and are now passing. This is the outcome we are were hoping for — that sites would take steps to fix intrusive ads experiences themselves and benefit all web users. However, if a site continues to maintain non-compliant ad experiences 30 days after being notified of violations, Chrome will begin to block ads on that site. We're encouraged by early results showing industry shifts away from intrusive ad experiences, and look forwarding to continued collaboration with the industry toward a future where Chrome's ad filtering technology will not be needed.

SpinRite

Scott Napier / @ssnapier
@SGgrc SpinRite has quite literally helped to keep the physical security of the Smithsonian intact, and I have convinced some skeptics of it's power. Looking forward to 6.1!

Closing The Loop

Nico de Smidt / @CryptoMike365
How about "speckdown"

Life Cream Scoop / @JAbramSloan
@SGgrc how about Smeltdown?

Matt Fenton / @FCrypt01001101
Hi Steve, what about calling it Melspec? A twist on the word Milspec. For meltdown and spectre. Thanks, Matt

eat78 / @iantwitter
@SGgrc SpecMelt

Carol Saye / @sayepetsitting
@SGgrc meltspec?

.... **bcrypt.c / @bcrypt_c**
@SGgrc Spectre + meltdown = DownSpec'd

Doug White / @cpuguru
Aloha Steve!

Just a FYI that I upgraded my Comcast internet service to 1Gig speed last week. Trying to run the SpeedTest resulted in about a 460MB+ throughput even though the technician showed 1Gig at the port. I remembered an earlier podcast about the EdgeRouter X & that the internal throughput would only be about half a Gig. So I purchased an EdgeRouter 4 replaced the EdgeRouter X - now I have my 1Gig throughput!

Figured I'd mention my experience as I imagine there are other home routers that will be likewise speed limited even though they advertise 1Gig ports.

Cheers!
Doug

Doug White / @cpuguru
If you're running a Ubiquiti Edgerouter - looks like new firmware dropped last week:
https://www.ubnt.com/download/edgemax/edgerouter-x/default/edgerouter-er-xer-x-sfpep-r6-firmware-v1100

Chip Steiner / @steiner_cci
Hey @SGgrc, When your ISP DNS has the best performance (using DNSBench) over GoogleDNS, Quad9, OpenDNS but uses DNS Filtering what's your advice?

Chris Ryan / @4given_p8ntblr
@SGgrc I saw this link for an IoT checker to see if your devices are on Shodan and thought I'd share iotscanner.bullguard.com

---

Russian Meddling Technology

Indictments reveal how Russia's 2016 election information warfare worked
https://www.cyberscoop.com/how-russias-2016-election-information-warfare-worked/

Last Friday, Special Counsel Robert Muller's investigation into Russian interference with the 2016 US presidential election released an indictment naming 13 Russian individuals and three Russian companies, accusing them of violating U.S. criminal law. The indictment charged the defendants with conspiracy to defraud the United Stated, wire fraud and identity theft.

This is a technical, not a political, podcast... so what interests me and us here, is not and should not be the election politics aspect of the effort, but the technical side of what was done to pull this off. And this is relevant not only for its pure technical content, but because we're hearing that Google, Facebook, Instagram and others were, at least to some degree be determined, responsible for and negligent and "should have known better" and done something about it.

But as I have looked into this, in many ways it's reminiscent of US law enforcement and our FBI complaining about the use of encryption and the "Internet going dark" problem... and demanding to have a golden key for access. My point is... it all comes down to technology... and that's a world we're competent to judge.

The indictment alleges that Russians purchased servers located in the United States in order to obfuscate their origins and then created and established hundreds of fake personas on social media which they carefully developed into “leaders of public opinion.”

They used virtual private networks (VPNs) to open and operate the social media accounts -- exactly as any US citizen might.

Muller's prosecutors also said that the Russians stole U.S. identities to open accounts with PayPal to further support their false identities and purchase advertisements on social media sites.

Russian agents, thus convincingly posing as American citizens, recruited and paid real Americans to engage in political activities, promote political campaigns and stage political rallies. And those Americans had no idea, nor any reason to suspect, that they were communicating with Russian agents.

Interestingly, the indictment alleges that in some cases the Russians fomented unrest on both sides of the US political divide at the same time: "After the election, the defendants allegedly staged rallies to support the president while simultaneously staging rallies to protest his election. In one instance the Russian defendants organized one rally to support the president-elect and another rally to oppose him... both in New York on the same day."

We here in the U.S. invented the Internet. It was our technology. And we are collectively profiting mightily from its existence -- largely because it is such a wide open communications platform. What happened is that an adversarial country very cleverly used our own technologies -- even our own U.S. bandwidth -- against our nation's interest.

Mike Masnick writing for TechDirt: "DOJ Russia Indictment Again Highlights Why Internet Companies Can't Just Wave A Magic Wand To Make Bad Stuff Go Away"

https://www.techdirt.com/articles/20180216/14052839251/doj-russia-indictment-again-highlights-why-internet-companies-cant-just-wave-magic-wand-to-make-bad-stuff-go-away.shtml

This was not just some run-of-the-mill "pretend to be Americans," this was a hugely involved process to make it very difficult to determine that they were not Americans.

I've seen some people online claiming that this shows why the platforms have to take more responsibility for who is using their platform:

> While you read the Mueller #Indictment remember the tech CEO mantra: “We don’t want to be the arbiters of truth.” These platforms were used *exactly as they were designed to be used*. Here we are a year later, and still no accountability or governance.
>
> — Renee DiResta (@noUpside) February 16, 2018

But my read on it is exactly the opposite. It shows just how ridiculous such a demand is. Would any of us be using these various services if we were all forced to go through a detailed background check just to use a social media platform? That seems excessive and silly. Part of the reason why these platforms are so useful and powerful in the first place is that they're available for nearly everyone to use with [few] hurdles in the way. That obviously has negative consequences -- in the form of trolling and scams and malicious behavior -- but there's also a ton of really good stuff that has come out of it.

(I'll note that many people who stir controversy have a great deal of trouble with Twitter specifically because it is such a completely wide open low-bar messaging platform.)

We should be pretty cautious before we throw away all of the value of these platforms just because some people used them for nefarious purposes. People are always going to be able to hide their true intentions from the various platforms -- and the response to that shouldn't be "put more blame on the platforms" -- it should be a recognition of why it's so silly to blame the tools and services for the actions of the users.

Yes, we should be concerned about foreign attempts to influence our elections (while noting that the US, itself, has a long history of doing the same damn thing in other countries -- so this is a bit of blowback). But blaming the technology platforms the Russians used seems to be totally missing the point of what happened -- and risks making the internet much worse for everyone else.

~30~