Security Now! #630 - 09-25-17

The Great DOM Fuzz-Off

This week on Security Now!

This week, Father Robert and I follow more Equifax breach fallout, look at encryption standards blowback from the Edward Snowden revelations, examine more worrisome news of the CCleaner breach, see that ISPs may be deliberately infecting their own customers, warn that turning off iOS radios doesn't, look at the first news of the FTC's suit against D-Link's poor security, examine a forthcoming Broadcom GPS chip features, warn of the hidden dangers of high-density barcodes, discuss Adobe's disclosure of their own private key, close the loop with our listeners, and examine the results of DOM fuzzing at Google's Project Zero.

Security News

Re: Equifax -- An interesting bit of gossip I picked up at a recent private security conference

The conference itself was under NDA, so I'm not a liberty to share any of that material, nor have I any need or interest in doing so. But there were a lot of very smart and well-connected people there. And an interesting point was made over breakfast of the second day: There's a quiet and firm belief among those in the know that the Equifax penetration was likely not a "random opportunistic hacker", but much more likely a highly skilled and targeted state-sponsored cyber intrusion. Specifically: China.

The goal, of course, was not and was never those 143 million mostly-American citizens. We were all caught up in the same net. The target were specific high-value corporate and government individuals whose personal identity information might be used to further and support additional targeted intrusions.

Experian Credit Lock PIN Security Fail!

https://krebsonsecurity.com/tag/credit-freeze/

The recent Equifax focus and attention has resulted in increased scrutiny of all credit processing firms, which somewhat disturbing and distressing results. Many of these systems at Equifax and others have been found to be unable to handle the sudden focus of attention, and as a result of that attention, previously unappreciated problems have been identified.

An example is experian's credit locking PIN recovery.

Experian's "Request your PIN" web service page reads: "If you have a security freeze on your credit report and wish to obtain your forgotten or misplaced PIN, you may request it here. A PIN is needed to remove a freeze from your credit report and to provide a creditor access to your credit report."

The first hurdle for instantly revealing anyone’s freeze PIN is to provide the person’s name, address, date of birth and Social Security number (which, Brian notes, is all data that has been jeopardized in breaches 100 times over — including in the recent Equifax breach — and which is broadly for sale in the cybercrime underground).

After that, one just needs to input an email address to receive the PIN and swear that the information is true and belongs to the submitter.

As Brian puts it: "I’m certain this warning would deter all but the bravest of identity thieves!"

When, 20 months ago after the Anthem breach we talked about this and I locked all of my credit reports we were strongly cautioned that we must NOT LOSE those PINS. But apparently asking consumers to be sufficiently responsible turned out to be impractical. So the system has been softened to make it both more practical and much less robust and secure.

Reuters: "Distrustful U.S. allies force spy agency to back down in encryption fight"
http://mobile.reuters.com/article/amp/idUSKCN1BW0GV

After a three-year process, the US ANSI standards organization, which was proposing the standardization of several strengths of two new encryption algorithms "Speck" and "Simon" have agreed to remove the weaker variants from the future standard following a backlash from international cryptographers who, frankly, no longer feel able to trust the US NSA's role in this process.

The ISO has decided not to approve two NSA-designed block encryption algorithms: Speck and Simon. It's because the NSA is not trusted to put security ahead of surveillance:

This distrust was evidenced throughout the communications among members. Not surprisingly, the suspicions stem from the nature of the internal NSA documents disclosed by Edward Snowden which revealed that the agency that previously focused upon the manipulation of standards and to promote technologies it could penetrate. Recall that budgetary documents, for example, sought funding to "insert vulnerabilities into commercial encryption systems."

More than a dozen of the experts involved in the approval process for Simon and Speck feared that if the NSA was able to crack the encryption techniques, it would gain a "back door" into coded transmissions, according to the interviews and emails and other documents seen by Reuters.

One Israeli computer science professor involved in the process said: "I don't trust the designers. There are quite a lot of people in NSA who think their job is to subvert standards. My job is to secure standards."

Bruce Schneier, who blogged about this Reuters reporting concluded his short entry saying: "I don't trust the NSA, either."

- https://www.schneier.com/blog/archives/2017/09/iso_rejects_nsa.html

CCleaner malware appears to be significantly worse that it first appeared to be.
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

Recap:

> The 32-bit installer of the v5.33 of CCleaner was maliciously modified to install a backdoor which reached out to a remote C2 (Command & Control) server. The backdoor malware was able to receive commands and download additional malware payloads.
>
> Significantly more than two million downloads of that maliciously modified download are believed to have occurred.

Cisco's Talos security division obtained files ostensibly from the malware's C2 server. Talos was careful about trusting the files, but was able to authenticate them by finding traces of Talos' own previous activity within the server's files. Thus they were authentic.

What Talos subsequently discovered was that the server code contained an array of 20 public domain names, including "cisco.com". They wrote:

"Interestingly the array specified contains Cisco's domain (cisco.com) along with other high-profile technology companies. This would suggest a very focused actor after valuable intellectual property.

These new findings raise our level of concern about these events, as elements of our research point towards a possible unknown, sophisticated actor. These findings also support and reinforce our previous recommendation that those impacted by this supply chain attack should not simply remove the affected version of CCleaner or update to the latest version, but should restore from backups or reimage systems to ensure that they completely remove not only the backdoored version of CCleaner but also any other malware that may be resident on the system."

Selected systems -- those appearing in the 20-domain list -- were delivered a secondary (Stage 2) payload consisting of 32-bit or 64-bit shellcode, though it appears that only the 32bit x86 shellcode was active and deliverable.

Later, Talos wrote: "The use of domain-based filtering further indicates the targeted nature of this attack. While we have confirmed that the number of systems affected by the backdoor was large based upon beacon information stored within the MySQL database, the attackers were specifically controlling which infected systems were actually delivered a Stage 2 payload. While it was reported that no systems executed a Stage 2 payload, this is not accurate. In analyzing the database table storing information on the systems that were delivered a Stage 2 payload, we identified 20 unique hosts that may have been affected by this payload. The functionality present within Stage 2 is documented in the "Stage 2 Payloads" section of this post."

The C2 MySQL database held two tables: one describing all machines that had reported to the server and one describing all machines that received the second-stage download, both of which had entries were dated between Sept. 12th and Sept. 16th. Over 700,000 machines reported to the C2 server over this time period, and more than 20 machines have received the second-stage payload. It is important to understand that the target list can be and was changed over the period the server was active to target different organizations.

Talos has reached out to the affected companies to notify them of effective stage 2 infection.

Stepping back a bit...

We have a supply-chain attack on an extremely popular utility which is used to opportunistically and widely infect a large but uncontrollable -- untargeted -- audience. But then, when those millions of weakly infected machine reach out to their common command & control server, their source IP is looked up against a list of deliberately targeted domain names to determine whether the attackers may have "gotten lucky" with their initial blind scattershot attack. And, if so, a secondary Stage 2 payload is delivered and executed on those targeted machines.

The Cisco Talos report contains IOC -- Indicators of Compromise -- forensics to allow anyone to determine whether their machines may have received the second stage infection. Among other indications, the machine's registry will contain some specific entries.

ISPs caught adding FinFisher malware to popular communications app downloads
http://www.ibtimes.co.uk/are-you-being-watched-finfisher-government-spy-tool-found-hiding-whatsapp-skype-1640263

Malware used by intelligence agencies spotted in 7 countries, experts said.

WikiLeaks previously disclosed the existence of "FinFisher" -- advanced surveillance malware capable of snooping on webcam feeds, monitoring and recording keystrokes, microphone audio and web browsing.

These tools were developed and are sourced by "The Gamma Group" an international firm who has in the past sold its technology to repressive regimes including Bahrain, Egypt, an the UAE.

So... today's news is that the security firm ESET has found identifiable variants of FinFisher in seven countries, packed into popular downloads including WhatsApp, Skype, Avast, VLC Player and WinRAR.

And, most worrisome... the infected modified payloads appear to have been injected into customer data streams by their own ISPs!

When a surveillance target attempted to download any of the specified utilities they would, instead, be silently redirected to an infected version of the utility.

When does deliberately turning off WiFi & Bluetooth not actually turn them off?
After you have upgraded to Apple's latest iOS v11.
https://www.theguardian.com/technology/2017/sep/21/ios-11-apple-toggling-wifi-bluetooth-control-centre-doesnt-turn-them-off

I've been using iOS v11 continuously since last Tuesday's release. I'm becoming comfortable with its new features and operation, but I have never encountered a more massively buggy release of iOS. It has done, and does, different weird things on every one of my many iOS devices. So I expect that we will be seeing a number of bug fix and stability improvements in coming months as these oversights are found and eliminated.

But as everyone knows, mistakes happen and can always be forgiven if they are addressed responsibly. What's NEVER forgivable is deliberate and worrisome POLICY mistakes.

One of the really nifty new features of iOS 11 is the easily-accessible Control Center that gives quick and customizable access to many system widgets. Among them are the three radios -- Cellular, WiFi and Bluetooth. Unfortunately, it has come to light that <quote> "Turning Off" <unquote> the WiFi and Bluetooth radios from the Control Center, despite the appearance of doing exactly that doesn't actually do that at all. It simply drops the connections that the device has open... but the radios remain on, alive, and drawing power. <sigh>

https://support.apple.com/en-us/HT208086

- AirDrop
- AirPlay
- Apple Pencil
- Apple Watch
- Continuity features, like Handoff and Instant Hotspot
- Instant Hotspot
- Location Services

The trouble is that Apple has decided that they know better than their users how their device should be managed.

If you REALLY want to turn off the WiFi and Bluetooth radios, the Control Center won't do the job. You must use the original Control Panel applet to turn them off hard.

For both security and power consumption, turning off unnecessary and unneeded radios is always best practice. So our takeaway here is that, despite appearance, the new Control Center is only giving the appearance of that. Its drops overt foreground data connections, while leaving the various radios' background operations up and running.

Judge dismisses half of the FTC's complaint claims against D-Link for sloppy security
https://www.engadget.com/2017/09/21/ftc-lawsuit-d-link-lax-router-security-took-hit/?sr_source=Facebook
Plaintiffs do need to have standing.
If we had clear laws about the required levels of security that would be one thing. But we don't, yet.

Our Smartphone's GPS soon to jump from 5-meter to 30-centimeter accuracy
WHILE consuming half the power AND operating within Urban "concrete canyon" environments.
https://spectrum.ieee.org/tech-talk/semiconductors/design/superaccurate-gps-chips-coming-to-smartphones-in-2018

Broadcom is beginning to sample the first mass-market GPS chip, their BCM47755, which has been included in some smartphone slated for 2018 release -- though that's all Broadcom would say.

The original oldest generation of GPS satellites use a single designated as "L1". But a newer generation of GPS satellites also broadcast a secondary "L5" signal which is both more complex and available at a different frequency. Being at a much higher frequency, the L5 signal is much less prone to "multipath" interference which especially effects urban city environments. The L5 signal bursts are so brief that indirect reflected paths are much less prone to overlapping the receipt of the first direct signal, and are therefore much more easily ignored.

The L5-based system was not deployed earlier because the low number of L5-equipped satellites didn't justify its widespread use in consumer devices. But now, with about 30 L5 satellites in orbit, the justification is there.

The hidden danger of high-density bar codes
https://www.michalspacek.com/post-a-boarding-pass-on-facebook-get-your-account-stolen

Adobe inadvertently publicly posts their private PGP key. Whoops!
https://arstechnica.com/information-technology/2017/09/in-spectacular-fail-adobe-security-team-posts-private-pgp-key-on-blog/

Adobe was in the news again last week when their PSIRT -- Product Security Incident Response Team -- mistakenly posted BOTH their public and private PGP eMail keys on their site.

Whoops.

They have since generated a new key pair and been careful to only post the public key, keeping its matching private half secret... at least for the time being.

The mistake was subsequently tracked down to someone using the Mailvelope Chrome & Firefox extension and clicking on the "Export All" button rather than "Export Public" option.

SpinRite:

- **Vigen Galustian in West Hills, CA**
  I'm an avid user of Spinrite... it has save me several times. I hope in your future upgrade you can make it to support USB connection and independent of OS.

- **Greg (Location: Somewhere)**
  Subject: Will new Spinrite make it easy to run Spinrite off USB drive?

  It is more trouble to always have to get out CD Drive to use SpinRite. Sure would be handy if it was easy to put SpinRite onto a USB stick and run it from there. The current method for doing this is too complicated for me. Hopefully new version will make this easier?

Closing The Loop

Chad Wilkin (@cnwilkin)
@SGgrc have you thought how iOS's new QR code abilities will impact SQRL?
https://www.cultofmac.com/485380/how-to-scan-qr-codes-iphone/

(Jeff Arthur's iOS client for SQRL.)

Scar (@HarveyScar)
@SGgrc hey Steve, I've never heard you recommend a particular drive brand. I'd assume you've seen tons of hdd data. Any thoughts on top brand?

("Loss of process", fuzzy-manufacturing, Maxtor, Hitachi, IBM.)
(WD, Seagate)

slimbobwe (@slimbobwe)
Is @LastPass still your best choice for online password security. Price has doubled & I trust your opinion @SGgrc?

Thomas Smailus (@ThomasSmailus)
@padresj @SGgrc #sn629 disappointed to hear you advocating by paying the shakedown money to credit bureaus for the failures of the ban syst.

(I understand that... but what are we to do? There IS value provided by the credit reporting agencies for people who DO desperately need to be able to demonstrate their history of responsible handling of debt. That's not something can reasonably be asked of the party requesting credit. So locking the report is the bext solution. Do I wish it was free, yes, and it SHOULD BE. But it's not. Does that mean I'm going to refuse to lock because it's not free? No. Locking and paying is the least bad or the alternatives.)

Garrett (@slavexstate)
Big shouts to @SGgrc for the Certificate extension recommendation. Really useful!

ETC Maryland (@etc_md)
@SGgrc google for android uses the encrypted google play services as true 2FA account login authentication.

The Great DOM Fuzz-Off of 2017

https://googleprojectzero.blogspot.com/2017/09/the-great-dom-fuzz-off-of-2017.html

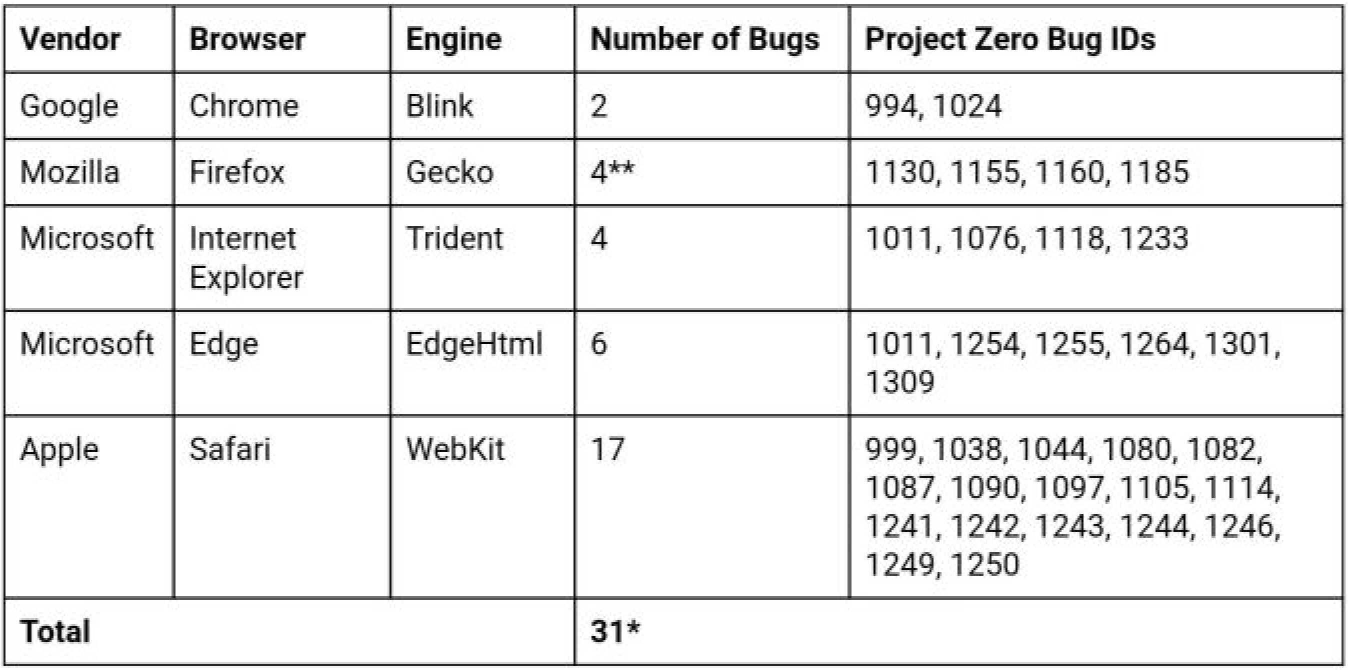
Ivan Fratric joined Google's Project Zero. In the past he had explored DOM fuzzing and had implemented a number of previous systems. So he decided that he wanted to start fresh, using all the experience he had acquired, to create a next-generation (and open source) DOM fuzzer.

What's a fuzzer and why are they useful? --> Interpreters!

Fuzzing Context:

We tested 5 browsers with the highest market share: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Apple Safari. We gave each browser approximately 100.000.000 iterations with the fuzzer and recorded the crashes. (If we fuzzed some browsers for longer than 100.000.000 iterations, only the bugs found within this number of iterations were counted in the results.) Running this number of iterations would take too long on a single machine and thus requires fuzzing at scale, but it is still well within the pay range of a determined attacker. For reference, it can be done for about $1k on Google Compute Engine given the smallest possible VM size, preemptable VMs (which I think work well for fuzzing jobs as they don’t need to be up all the time) and 10 seconds per run.

Results:



Vendor	**Browser**	**Engine**	**Number of Bugs**	**Project Zero Bug IDs**
Google	Chrome	Blink	2	994, 1024
Mozilla	Firefox	Gecko	4**	1130, 1155, 1160, 1185
Microsoft	Internet Explorer	Trident	4	1011, 1076, 1118, 1233
Microsoft	Edge	EdgeHtml	6	1011, 1254, 1255, 1264, 1301, 1309
Apple	Safari	WebKit	17	999, 1038, 1044, 1080, 1082, 1087, 1090, 1097, 1105, 1114, 1241, 1242, 1243, 1244, 1246, 1249, 1250
Total			**31***	