

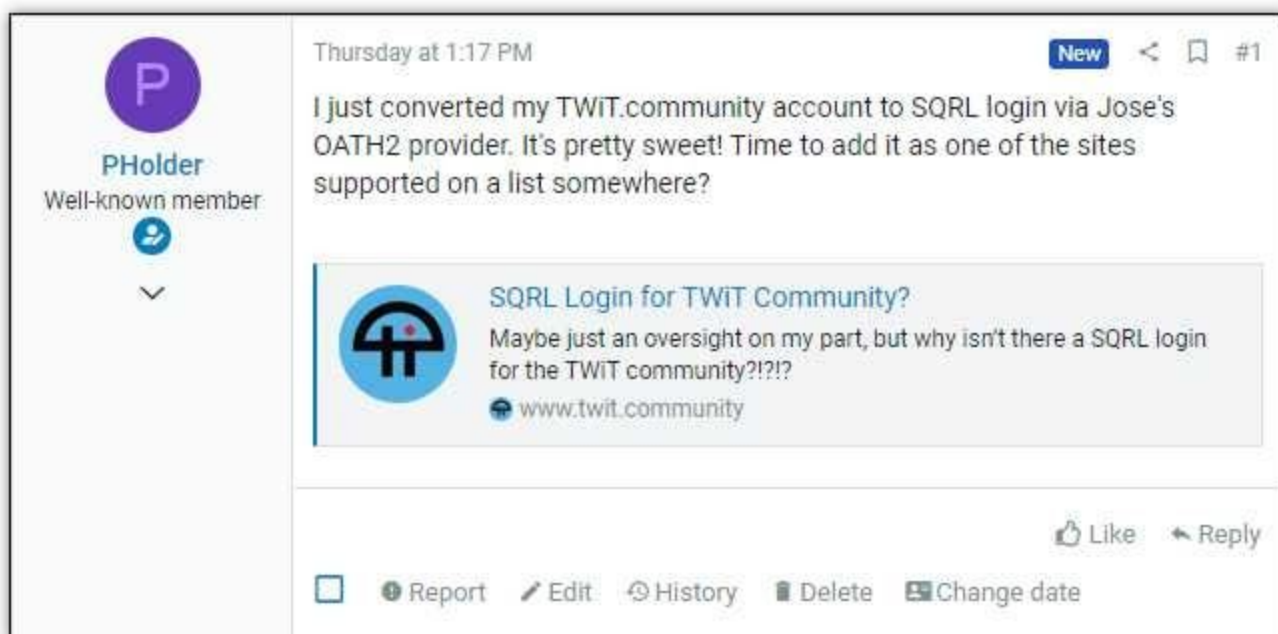
Security Now! #746 - 12-23-19

A Decade of Hacks

This week on Security Now!

This week we stumble into Microsoft's own confusion about whether or not Microsoft's Security Essentials will continue receiving updates after January 14th. We look briefly at the year when Ransomware happened, we revisit the Avast and AVG Mozilla extensions to see how they're doing, we look at the just-announced big news for Apple's and Google's bug bounty programs for 2020, and also at Mozilla's addition of another very appealing DoH provider (which Leo apparently likes). We provide a nudge to Drupal site masters to update their Drupal Cores RIGHT NOW... And then we conclude by revisiting this past decade -- spanning 2010 to 2019 -- and the many hacks we've explored during these previous ten years.

SQLR is Running on the TWiT.Community Forums!



The screenshot shows a forum post on the TWiT.Community forums. The post is from a user named 'PHolder', who is identified as a 'Well-known member'. The post is dated 'Thursday at 1:17 PM' and is marked as 'New'. The text of the post reads: 'I just converted my TWiT.community account to SQLR login via Jose's OATH2 provider. It's pretty sweet! Time to add it as one of the sites supported on a list somewhere?'. Below the text is a link to a forum topic titled 'SQLR Login for TWiT Community?' with the text 'Maybe just an oversight on my part, but why isn't there a SQLR login for the TWiT community?!?!?' and the URL 'www.twit.community'. At the bottom of the post, there are icons for 'Like' and 'Reply', and a row of icons for 'Report', 'Edit', 'History', 'Delete', and 'Change date'.

<https://www.twit.community/t/sqlr-login-for-twit-community/1175>

Security News

In a reversal: MSE signatures WILL continue to receive updates after Jan. 14

We know this thanks to ComputerWorld's Woody Leonard who posed the question to Microsoft. According to an official post, the company will continue to ship updates to Microsoft Security Essentials after Win7's demise on Jan. 14th. At least, that's what we've been promised. The FAQ hasn't been fixed yet.

Here's what Woody explained:

"Late last week, I talked about a discrepancy in Microsoft's promised handling of Microsoft Security Essentials as Windows 7 reaches end of support. An internally inconsistent official announcement seemed to say that MSE signature file updates would stop — even for those who have paid for Extended Security Updates. Which is absurd. Why would Microsoft stop updating its antivirus program even for people who are paying to continue receiving Monthly Rollup patches?"

So then last Tuesday, Microsoft held an "Ask Me Anything" session, as Woody termed it, for the Win7 forlorn, on the Microsoft Tech Community Forum.

Woody asked: *"Can you confirm that Microsoft will really, for sure, cut off Microsoft Security Essentials malware signature updates after January 14? Even if you're paying for Extended Support?"*

Microsoft engineer Mike Cure provided an official response: *"MSE will continue to receive signature updates after Jan. 14."* Mike cited the Windows 7 support FAQ which says:

"Microsoft Security Essentials (MSE) will continue to receive signature updates after January 14, 2020. However, the MSE platform will no longer be updated."

Then, during the AMA, @Brian responded by referring to the Extended Security Update FAQ, which asks:

Q: Will Microsoft Security Essentials continue to protect my PC after end of support?

A: No, your Windows 7 PC will not be protected by Microsoft Security Essentials (MSE) after January 14, 2020. This product is unique to Windows 7 and follows the same lifecycle dates for support.

Woody wrote: *"That's an obfuscating piece of bafflegab, subject to whimsical interpretation, as I described in the Computerworld article last week."*

Mike Cure then clarified the situation by promising: *"I'll get [the ESU FAQ] corrected as soon as possible."*

Woody concluded by noting that as of early last Wednesday morning (when he posted), nothing's been corrected. And that *"Those of us who actually like and rely on MSE are still hanging on a limb."*

Armor reports: Since October 20th, 11 more school districts hit by Ransomware

<https://www.armor.com/reports/11-new-us-school-districts-compromised-by-ransomware-a-total-of-72-educational-institutions-in-2019-reports-armor/>

72 school districts and/or individual educational institutions publicly reported being a victim of ransomware, impacting 1,039 individual schools.



Since today's podcast is a retrospective, in many ways we could consider 2019 to have been the year that Ransomware really took off -- and in the process badly hurt many victims... and their insurers. The bad guys created a diabolical multi-level-marketing style distribution system where their agents did not need to engineer ransomware, negotiate with victims, or arrange payment. They merely needed to infect victims with a malicious payload they had received and, in return, they would receive the lion's share of the ransomed spoils.

We have witnessed the resulting explosion in the number of successful ransomware incidents.

An analysis of the incident details revealed another previously underappreciated security weakness in the way the "cloud business" model had quietly evolved: We learned that many services were now being outsourced to so-called "Managed Service Providers" (MSPs) whose access into their client's networks was apparently extensive, since if an MSP could be compromised, their entire client base could follow... with widespread devastating effect.

And, unfortunately, as we head into 2020, the only thing that has clearly changed is a much heightened awareness of the problem. These attacks generated headlines everywhere, so at least next year everyone will have been forewarned... even if they are still not forearmed.

Avast & AVG clean up their act and return to Mozilla

Recall that at the beginning of the month, Wladimir Palant, the creator of Adblock-Plus took the time to reverse-engineer the backhaul communications of the Avast and AVG plug-ins to discover and report that WAY WAY WAY too much information was being sent back, FAR above and beyond what would be needed to perform the task of checking for malicious URLs. Mozilla promptly responded by yanking the offending browser extensions from its repository.

Well, now the extensions are back and they are reportedly behavior themselves FAR better than they had been. We haven't yet heard from Wladimir, but others have looked.

Avast has since said: "Privacy is our top priority and the discussion about what is best practice in dealing with data is an ongoing one in the tech industry. We have never compromised on the security or privacy of personal data. We are listening to our users and acknowledge that we need to be more transparent with our users about what data is necessary for our security products to work, and to give them a choice in whether they wish to share their data further and for what purpose. We made changes to our extensions including limiting the use of data and these changes are explained clearly in our Privacy Policy. Our browser extensions Avast Online Security and AVG Online Security are back on the Chrome Store, and on the Mozilla Store (since 12/17). It's important to us that users understand that we're listening to concerns about transparency and data use, and striving to do better and lead by example in this area."

So the extensions are back and they now display a user-confirmation page to proactively obtain their user's permission:



Courtesy, BleepComputer: <https://www.bleepingcomputer.com/news/security/avast-and-avq-firefox-extensions-added-back-to-mozilla-addons-site/>

Google and Apple are revamping their bug bounty awards programs

On the Google side...

Last Wednesday, Google announced its plans to revamp its 6-year-old Patch Rewards program which was started in 2013. At the time, Google announced that it would provide financial aid to open-source projects if and when (and after) they implemented security features. Project maintainers had to apply, provide a plan for the feature they wanted to implement, and Google would commit to a financial reward that would be paid once the feature was implemented.

But, starting January 1, 2020, Google will be changing how this program works, to provide financial support upfront, even before projects implement the security features to which they commit. The rationale behind the change is the recognition that many open-source project maintainers prioritize features based upon the sponsorships they receive. Such sponsorship is prevalent in the Free Open Source Software community. SO, for example, if a company needs a particular feature in an open-source project, the company usually donates to the project with the condition that the maintainers implement the feature they need with a higher priority before other features.

Therefore, by providing its funds upfront, Google provides project maintainers a way to fund their work while prioritizing security features at the same time, rather than relying upon the largess of wealthy corporate entities whose needs for project features may be more self-serving.

According to Google, open-source project maintainers can request upfront funds via the Patch Rewards program for two types of security-related features and improvements:

- Smaller (\$5,000): Meant to motivate and reward a project for fixing a small number of security issues. Examples: improvements to privilege separation or sandboxing, cleanup of integer math, or more generally fixing vulnerabilities identified in open source software by other bug bounty programs.
- Larger (\$30,000): Meant to incentivize a larger project to invest heavily in security, e.g. providing support to find additional developers, or implement a significant new security feature (e.g. new compiler mitigations).

Any open-source project can apply, Google said. All they have to do is fill out a form located at: <http://goo.gle/patchz-nomination>

A panel reviews all submissions received during the previous month and select the projects they wish to fund.

Jan Keller, the technical program manager for security at Google said that *"When selecting projects, the panel will put an emphasis on projects that either are vital to the health of the Internet or are end-user projects with a large user base."*

To provide some idea of the types of apps and libraries Google usually selects, the Patch Rewards program homepage lists the following open-source projects as being "in scope":

- Open-source foundations of Chrome and Android: Chromium, Blink, Omaha, AOSP(aka Android)
- Security-critical, commonly used components of the Linux kernel (including KVM)
- High-profile web and mail servers: Apache httpd, lighttpd, nginx, Sendmail, Postfix, Exim, Dovecot
- Other high-impact network services: OpenSSH, OpenVPN, BIND, ISC DHCP, University of Delaware NTPD
- Core infrastructure data parsers: libjpeg, libjpeg-turbo, libpng, giflib, zlib, libxml2
- Other essential libraries: OpenSSL, Mozilla NSS
- The reference implementation of Certificate Transparency and its open-source dependencies
- Toolchain security improvements for GCC, binutils, and llvm
- Security-relevant bits of common package managers: yum, apt, pip, npm
- Popular web frameworks and libraries: Angular, Closure, Dart, Django, Dojo Foundation, Ember, GWT, Go, Jinja (Werkzeug, Flask), jQuery, Knockout, Polymer, Struts, Web2py, Wicket
- Widespread decompression libraries: zlib, bzip2, tar, gzip, info-zip, cpio, xz, 7z, p7zip, ncompress, lzo
- Critical software used for cloud computing: Envoy proxy
- Projects integrated into OSS-Fuzz

And, on the Apple side...

Apple has opened its previously closed public bug bounty program to all security researchers and has published its official rules.

On Friday, Apple formally opened its bug bounty program today to all security researchers, after announcing the move earlier this year in August at the Black Hat security conference in Las Vegas.

A new big splashy page on Apple's developer site is headlined: "Apple Security Bounty"
<https://developer.apple.com/security-bounty/>

Before now, Apple's bug bounty program was strictly "by invitation only" and only accepted iOS security bugs. But now Apple will accept vulnerability reports for a wide array of products that also includes their iPadOS, macOS, tvOS, watchOS, and iCloud.

In addition, the company has also increased its maximum bug bounty reward from \$200,000 to \$1,500,000, depending on the exploit chain's complexity and severity. However, Apple is not handing out such high rewards casually. The rules are strict and they have set a high bar for earning the top rewards. To be eligible for the top prizes and various bonuses, researchers must submit clear reports which include:

- A detailed description of the issues being reported.
- Any prerequisites and steps to get the system to an impacted state.
- A reasonably reliable exploit for the issue being reported.
- Enough information for Apple to be able to reasonably reproduce the issue.

Those bugs which are novel, affect multiple platforms, work on the latest hardware and software, and impact sensitive components are more likely to net the top \$1.5 million reward. And vulnerabilities discovered and reported in beta releases will also be highly-prized with Apple willing to add a 50% bonus on top of the regular payout for any bug reported in a beta release.

We've discussed this before and noted that this is entirely rational since it incentivizes researchers to look earlier at Apple's forthcoming releases rather than waiting for them to be in the wild... which, in turn, helps Apple by finding and fixing any major security flaws before they reach production versions of its software, where they could impact billions of devices.

And Apple will also pay a 50% bonus for regression bugs where older and previously-fixed problems return for an encore.

Since takeover bugs requiring "no user involvement" are the most sought after by the likes of Zerodium, the discovery and reporting of those will also bring researchers top money... so long as the researcher is able to provide a fully working exploit chain for these types of submissions. So, for example, if one of these attacks uses three bugs chained together, the researcher will have to submit a full exploit chain that incorporates all the three bugs if they wish to earn the maximum reward.

Requiring a working exploit or exploit chain places a much higher burden upon the researcher, but would greatly reduce the number of "false positive" claims of "Hey, I found this bug over there and I want some cash for it." sorts of reports, which have often plagued other bounty programs.

Under "Eligibility" Apple's page says researchers must:

- Be the first party to report the issue to Apple Product Security.
- Provide a clear report, which includes a working exploit (detailed below).
- Not disclose the issue publicly before Apple releases the security advisory for the report. (Generally, the advisory is released along with the associated update to resolve the issue). See terms and conditions.

Issues that are unknown to Apple and are unique to designated developer betas and public betas, including regressions, can result in a 50% bonus payment. Qualifying issues include:

- Security issues introduced in certain designated developer beta or public beta releases, as noted on this page when available. Not all developer or public betas are eligible for this additional bonus.
- Regressions of previously resolved issues, including those with published advisories, that have been reintroduced in a developer beta or public beta release, as noted on this page when available.

Bounty Categories

Bounty payments are determined by the level of access or execution achieved by the reported issue, modified by the quality of the report. A maximum amount is set for each category. The exact payment amounts are determined after review by Apple. All security issues with significant

impact to users will be considered for Apple Security Bounty payment, even if they do not fit the published bounty categories. Apple Security Bounty payments are at Apple's discretion.

iCloud

Unauthorized access to iCloud account data on Apple Servers	\$100,000
---	-----------

Device attack via physical access

Lock screen bypass	\$100,000
--------------------	-----------

User data extraction	\$250,000
----------------------	-----------

Device attack via user-installed app

Unauthorized access to sensitive data	\$100,000
---------------------------------------	-----------

Kernel code execution	\$150,000
-----------------------	-----------

CPU side channel attack	\$250,000
-------------------------	-----------

Network attack with user interaction

One-click unauthorized access to sensitive data	\$150,000
---	-----------

One-click kernel code execution	\$250,000
---------------------------------	-----------

Network attack without user interaction

Zero-click radio to kernel with physical proximity	\$250,000
--	-----------

Zero-click unauthorized access to sensitive data	\$500,000
--	-----------

Zero-click kernel code execution with persistence and kernel PAC bypass	\$1,000,000
---	-------------

Report and Payout Guidelines

The goal of the Apple Security Bounty is to protect customers through understanding both vulnerabilities and their exploitation techniques. Reports that include a basic proof of concept instead of a working exploit are eligible to receive no more than 50% of the maximum payout amount. Reports lacking necessary information to enable Apple to efficiently reproduce the issue will result in a significantly reduced bounty payment, if accepted at all.

A complete report includes:

- A detailed description of the issues being reported.
- Any prerequisites and steps to get the system to an impacted state.
- A reasonably reliable exploit for the issue being reported.
- Enough information for Apple to be able to reasonably reproduce the issue.

Maximizing Your Payout

To maximize your payout, keep in mind that Apple is particularly interested in issues that:

- Affect multiple platforms.
- Impact the latest publicly available hardware and software.
- Are unique to newly added features or code in designated developer betas or public betas, including regressions, as noted on this page when available.
- Impact sensitive components.
- Are novel.

Additional Requirements

In addition to a complete report, issues that require the execution of multiple exploits, as well as one-click and zero-click issues, require a full chain for maximum payout. The chain and report must include:

- Both compiled and source versions.
- Everything needed to execute the chain.
- A sample non-destructive payload, if needed.

Sending Your Report

Send your report by email to product-security@apple.com. Whenever possible, encrypt all communications with the Apple Product Security PGP Key. Include all relevant videos, crash logs, and system diagnosis reports in your email. If necessary, use Mail Drop to send large files. Learn how to report a security or privacy vulnerability.

Mozilla expands its DoH provider offering

Last Tuesday, Mozilla announced the addition of a second DoH server provider to its previous list of one. So now users can choose between Cloudflare and NextDNS. Mozilla's announcement was:

<https://blog.mozilla.org/blog/2019/12/17/firefox-announces-new-partner-in-delivering-private-and-secure-dns-services-to-users/>

'Firefox Announces New Partner in Delivering Private and Secure DNS Services to Users. NextDNS Joins Firefox's Trusted Recursive Resolver Program Committing to Data Retention and Transparency Requirements that Respect User Privacy'

By adding a second provider -- NextDNS -- a relative newcomer startup founded just this past May 2019, Mozilla has not only added an alternative but has lifted its promised Trusted Recursive Resolver program (TRR) off the ground.

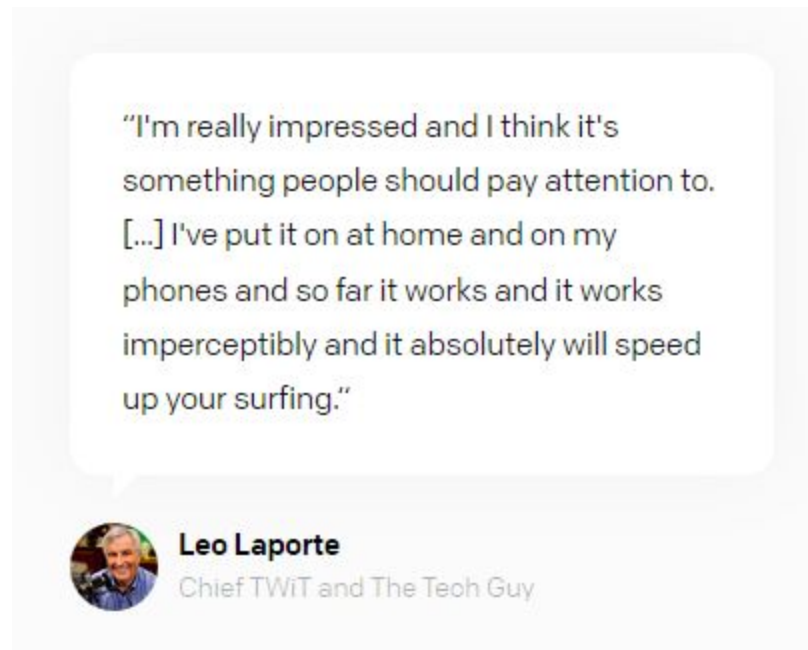
Mozilla says that its Trusted Recursive Resolver program matters because: *"DoH's ability to encrypt DNS data addresses is only half the problem we are trying to solve. The second half is requiring that companies with the ability to see and store your browsing history change their data handling practices."*

In other words, just encrypting DNS queries to make it more difficult for ISPs and governments to snoop on website visits won't mean much if the company offering the DoH service hasn't itself signed up to a robust privacy policy.

Mozilla's TRR program requires that DoH resolvers, among other things:

- Only collect data (e.g. IP addresses) for the purposes of running the service and don't keep it for longer than 24 hours.
- Publish a privacy policy explaining this.
- Do not block, modify or censor websites unless required to by law.

NextDNS may particularly appeal to more capable tinkerers, like Security Now listeners. And it appears to appeal to our fearless leader, himself:



What's the appeal? Control and visibility -- User who sign up for an account are given an inordinate amount of control over what gets blocked and what doesn't, including being able to create domain allow/blocklists, and sign up for a range of public advertising/tracking and filtering lists. Techie users can even block specific applications as well as view traffic logs -- all providing a level of control and visibility into DNS that very unusual for a DNS resolver of any type.

The reason why so many ISPs are chafing at the pending loss of access to their customer's DNS is the reason why putting the power of DNS management into the hands of those who want it makes sense.

NextDNS's service has been compared to a cloud implementation of "PiHole", a well-known Raspberry Pi-based network adblocker and DNS server.

The fact that NextDNS has built its service in such a way suggests that the company sees the possibility that DNS and DoH resolution could eventually grow into a more general privacy system, competing with related services such as adblocking.

In some testing by the technical press, NextDNS's apps for Windows, macOS, Linux, Android, and iOS were not yet widely known and therefore caused some over-protective security software that hadn't encountered them before to throw up warnings about installing them. (Yeah... I know that feeling!)

Drupal admins need to update now!

Last Wednesday the Drupal Core team released updates which foreclose on one CRITICAL and three Moderately CRITICAL vulnerabilities.

<https://www.drupal.org/security>

If you haven't recently updated your Drupal-based blog or business website to the latest available versions, it's the time.

Considering that Drupal-powered websites are among the all-time favorite targets for hackers, the website administrators are highly recommended to install the latest release Drupal v7.69, v8.7.11, or v8.8.1 to prevent remote hackers from compromising web servers.

The advisory with the critical severity includes patches for multiple vulnerabilities in the third-party "Archive_Tar" library that Drupal Core uses for creating, listing, extracting, and adding files to tar archives.

The vulnerability resides in the way the affected library untar archives with symlinks, which, if exploited, could allow an attacker to overwrite sensitive files on a targeted server by uploading a maliciously crafted tar file.

So, one mitigating factor is that the flaw only affects Drupal websites that are configured to process .tar, .tar.gz, .bz2, or .tlz files uploaded by untrusted users. But the Drupal developers note that a working proof-of-concept exploit for this vulnerability DOES exist and considering the popularity of Drupal exploits among hackers, we might expect to see hackers actively exploiting this flaw in the wild to target Drupal websites. So... You don't want yours to be among them.⁷

Moderately Critical Drupal Vulnerabilities

In addition to this critical vulnerability, the Drupal devs have also patched three moderately critical vulnerabilities in the Core software. There's a...

- Denial of Service (DoS): The install.php file used by Drupal 8 Core contains a flaw that can be exploited by a remote, unauthenticated attacker to impair the availability of a targeted website by corrupting its cached data.
- Security Restriction Bypass: The file upload function in Drupal 8 does not strip leading and trailing dot ('.') from filenames, which can be used by an attacker with file upload ability to overwrite arbitrary system files, such as .htaccess to bypass security protections.
- Unauthorized Access: This vulnerability exists in Drupal's default Media Library module when it doesn't correctly restrict access to media items in certain configurations. Thus, it could allow a low-privileged user to gain unauthorized access to sensitive information that is otherwise out of his reach.

According to the developers, affected website administrators can mitigate the access media bypass vulnerability by unchecking the "Enable advanced UI" checkbox on /admin/config/media/media-library, though this mitigation is not available in 8.7.x.

All three of the “moderately critical” vulnerabilities have been patched with the release of Drupal versions v8.7.11 and v8.8.1, and at the time of writing, no proof-of-concept for these flaws have been made available.

However, since a proof-of-concept DOES currently exist for the critical Drupal vulnerability, users running vulnerable versions of Drupal are strongly encouraged to update their Drupal systems to the latest core release as soon as possible.

A Decade of Hacks

On this Eve of 2020, we look back over the hacks of the past decade.

The big news of 2010 was Stuxnet -- Boy did THAT make an impression.

Today we're pretty certain that the Stuxnet worm was co-developed by the US and Israeli intelligence services as a means to sabotage Iran's nuclear weapons program, which was ramping up in the late 2000s. Stuxnet was cleverly designed to ride on thumb drives as a means of jumping the "air gap" to non-networked computers. It was specifically designed to destroy SCADA (supervisory control and data acquisition) equipment -- primarily centrifuges -- used by the Iranian government for its nuclear fuel enrichment process. The Stuxnet worm successfully destroyed equipment in several locations.

Though there were other cyber-attacks carried out by nation-states against one another before 2010, Stuxnet was the first incident that grabbed headlines across the world and marked the entry into a new phase of cyber-war -- from simple data theft and information gathering to actual physical destruction.

Operation Aurora - the hack that changed Google

Though these attacks by the Chinese government's military were actually conducted in the 2000's, their efforts to compromise US properties including Adobe, Rackspace, Juniper, Yahoo, Symantec, Northrop Grumman, Morgan Stanley... and Google, came to light in early 2010. Operation Aurora, as it was called, marked a turning point for Google. After Google discovered and publicly disclosed the attacks against its infrastructure, Google decided to stop working with the Chinese government in censoring the search results for Google.cn, and Google eventually shut down operations in China. In explaining their decision, Google specifically mentioned the Operation Aurora cyber-attack as one of the factors behind its decision.

The Sony Playstation Hack

In the spring of 2011, Sony announced that a hacker had stolen details for 77 million PlayStation Network users, including personally identifiable information and financial details. It's interesting that by today's measure such a breach would be a bit of a yawn -- "Oh, okay, another massive breach of personal information?" But at the time, and for many years afterward, Sony's

Playstation Network breach was one of the largest in the world.

And thus, for Sony, the breach was catastrophic. They were forced to shut down their cash cow -- the Sony PlayStation Network -- for 23 days while their IT people addressed the security breach. And it remains the longest outage in PSN's history.

Sony not only lost profit directly due to the outage, but then moreso over class-action lawsuits filed by users after some started noticing credit card fraud. It also lost more when it was forced to give users a bunch of free PlayStation 3 games to get them back online.

What the industry learned in a big way was the degree of damage that a successful network attack could cause when a company fails to invest in proper security. This event also stands out because corporate lawyers woke up and started a trend of companies adding CYA clauses to their Terms of Service requiring that users relinquish rights to file lawsuits following security breaches. Although Sony wasn't the first to add such a clause, they put such clauses on the map and many other companies added similar clauses soon after.

And then we have... Diginotar

It was in the later half of 2011 that we first learned of the Iranian government's successful hack of the then-popular Dutch certificate authority, Diginotar. In a nice retrospective summary written a year later, Threatpost wrote:

The attacker who penetrated the Dutch CA DigiNotar last year had complete control of all eight of the company's certificate-issuing servers during the operation and he may also have issued some rogue certificates that have not yet been identified. The final report from a security company commissioned to investigate the DigiNotar attack shows that the compromise of the now-bankrupt certificate authority was much deeper than previously thought.

In August 2011 indications began to emerge of a major compromise at a certificate authority in the Netherlands, and the details quickly revealed that the attack would have serious ramifications. The first public acknowledgement of the attack was the discovery of a large-scale man-in-the-middle attack against Gmail users in Iran. Researchers investigating that attack discovered that the operation was using a valid wildcard certificate, issued by DigiNotar, for *.google.com, giving the attacker the ability to impersonate Google to any browser that trusted the certificate.

It quickly emerged that the attackers had also obtained valid certificates for a number of other high-value domains, including Yahoo, Mozilla and others. Browser manufacturers scrambled to

revoke trust in the compromised certificates and reassure users that the Internet was not broken. Now, the final report from Fox-IT, the Dutch company brought in at the time of the attack in 2011 to find the root cause and determine the extent of the damage, says in its final report that the attack was a wide-ranging one that likely started more than a month before the CA discovered it.

Edward Snowden

How many times since 2013 have I referred to Snowden, and the fundamental way the Snowden revelations changed the world's security landscape? I think it would not be an overstatement to conclude that the Snowden leaks were the most important cyber-security event of the decade. They exposed a global surveillance network that the US and its Five Eyes partners had set up after the 9/11 attacks and they forever changed cybersecurity.

Unfortunately, Edward's revelations also drove repressive countries like China, Russia, and Iran to ramp up their own surveillance operations and increase their foreign intelligence-gathering efforts, which has led to an increase in cyber-espionage as a whole.

Wikipedia has more on the downstream impact of Snowden's leaks.

The Target hack

At the end of 2013, Target admitted that malware planted on its stores' systems had enabled hackers to collect payment card details for 40 million of its previous shoppers... and much of the world was introduced to the concept of Point Of Sale malware -- meaning that we purchase something at an infected retailer and now we're at risk due to our purchase. There had been previous incidents of POS malware, but this was the first time a major retailer suffered a breach of such proportion. As we know many other retailers have fallen since, but Target was the first biggie.

The Adobe hack

Also in November 2013, Adobe admitted that hackers had stolen the data of more than 153 million users. The data was dumped online, and their users' passwords were almost immediately cracked and reversed back to their plaintext versions. For many years after the Adobe breach was used as a cautionary warning about the use of weak and easily guessed passwords.

Silk Road takedown

2013 was the year that Silk Road, the Tor-hosted dark web marketplace for selling illegal products, was taken down. Silk Road's discovery and takedown showed the world for the first time that the dark web and Tor were not providing perfect anonymity and security.

Have I Been Pwned?

Following the Adobe breach, Australian security researcher Troy Hunt launched his "Have I Been Pwned" website as a simple way for users to learn whether their password was among those exposed in the massive Adobe breach. As we know, this has been a huge success and today the site includes the breach databases from over 410 hacked sites and information on more than 9 billion accounts. The site now has an API allowing for automated querying and it's been integrated into Firefox, password managers, company backends, and even some government systems.

The hack of Sony Pictures

We learned in 2014 that North Korea had some competent hackers of their own. Initially calling themselves the Guardians of Peace then later the Lazarus Squad, they were eventually linked to North Korea's intelligence apparatus. As we'll recall, the motivation behind the hack was to force the studio to abandon its planned release of "The Interview" which was a comedy about an assassination plot against North Korea's leader Kim Jong-un. When Sony refused to be intimidated the hackers damaged Sony's network and leaked studio data and private emails online.

And our listeners will recall that this gave birth to the term: APT -- Advanced Persistent Threat -- since we learned that the Sony's breachers had been lurking inside their network for quite some time.

The hack of Mt. Gox

Mt. Gox was not the first cryptocurrency exchange to get hacked, but it remains the biggest cyber-heist of the cryptocurrency ecosystem to this day. The hack, which is still shrouded in mystery today, occurred in early 2014, when hackers made off with 850,000 bitcoins, worth more than \$6.3 billion today. At the time, Mt. Gox was the biggest cryptocurrency exchange in the world.

Unfortunately, just as the infamous bank robber, Willie Sutton, explained that he robs banks because that's where the money is, hackers also realized that stealing virtual currency was a lot easier than making it the hard way. So now cryptocurrency exchanges are a frequent target of attack.

Heartbleed

No review of 2014 would be complete without reminding everyone of "Heartbleed." A not-just-theoretical remote data extraction vulnerability that rocked the Internet. It really did enable the discovery of a server's private keys with a low but non-zero probability.

The promise of compromise was so juicy that it also began the now common practice of jumping on newly announced vulnerabilities before they can be patched. Heartbleed was exploited almost

immediately after being publicly disclosed and led to a long string of hacks during 2014 and beyond, as some server operators failed to patch their OpenSSL instances, despite repeated warnings. At the time it was publicly disclosed, it was believed that about half a million Internet servers were vulnerable, a number that took years to decline.

RowHammer

Their June 24th, 2014 paper carried the innocent and academic title: "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors" ... and the result was RowHammer, another authentic and not-just-theoretical attack. And, as we known today, it would prove to be just the first of the many that we would be seeing in subsequent years against the computing hardware that we had naively believed to be bullet proof.

Ashley Madison data breach

2015 was the year of the Ashley Madison dating website data breach. In July of 2015 a hacking group calling themselves the Impact Team released the internal database of Ashley Madison, a website which was aimed at those wishing to have an affair. Whereas most breaches today may expose our username and hashed password for websites we don't even recall visiting, the Ashley Madison breach exposed people's real world lives. And sadly, a few committed suicide after being publicly outed as having an account on the site.

SIM swapping

The practice known as "SIM swapping", where hackers contact a mobile provider and trick their personnel into transferring a victim's phone number to a SIM card controlled by the attacker, first surfaced in 2015. The initial SIM swapping attacks were linked to incidents where hackers reset passwords on social media accounts or hijacked sought-after usernames. But, as with Willie Sutton, once hackers realized that they could also use the technique to gain access to cryptocurrency or bank accounts, from where they could steal large sums of money, the practice became much more than a nuisance.

The Ukraine power grid hacks

The cyber-attack on Ukraine's power grid in December 2015 caused power outages across western Ukraine and was the first successful attack on a power grid's control network ever recorded. While Stuxnet and Shamoon were the first cyber-attacks against an industrial target, the Ukraine incident was the first one impacting the general public. It opened everyone's eyes to the dangers cyber-attacks can pose to a country's critical infrastructure. The threat continues to loom today.

DNC hack

We should also note that in the spring of 2016, the Democratic National Committee admitted that it had suffered a security breach after a hacker going by the name of Guccifer 2.0 started publishing emails and documents from the organization's servers. It was later determined that the DNC had been hacked not by one, but two Russian Bears -- cyber-espionage groups -- Fancy Bear (APT28) and Cozy Bear (APT29). The data that was stolen during the hack was used in a carefully staged intelligence operation with the intent of influencing the upcoming US presidential election.

Yahoo hacks go public

It was also in 2016 that Yahoo admitted that it had suffered two data breaches in the span of four months, including one that would turn out to be the largest breach in the history of the internet. Whoopsie.

The Shadow Brokers

Although to this day we still have no idea who they are, it was between August 2016 and April 2017 that the group calling themselves "The Shadow Brokers" teased, auctioned, and leaked hacking tools developed by the Equation Group, a codename for the US National Security Agency (NSA). These tools, as we know, were top quality hacking tools which made an immediate impact. A month after the final Shadow Brokers leak, one of the tools -- EternalBlue -- gave the WannaCry worm the teeth it used to wreak havoc across the global Internet.

The birth of IoT botnets

A blog post in early September 2016 introduced the world to Mirai, a strain of Linux malware designed to work on routers and smart Internet of Things devices. During the 90 days that followed, after being used to launch some of the biggest DDoS attacks ever seen, Mirai would become one of the most well-known malware strains in the world. And after its source code was released online in an attempt by its author to disavow its authorship, it has become one of today's most widespread malware families with its code being the foundation of most IoT/DDoS botnets.

This podcast has used two pithy slogans as a result: "The 'S' in IoT stands for security" and "IoT" is short for "Installation of Trojan."

WannaCry

It was in May of 2017 that WannaCry first swept across the Internet fueled, as we know, by the Shadow Brokers' leak of the NSA's internal EternalBlue exploit against Windows file sharing SMB protocol. We now know that WannaCry was also developed by North Korean hackers looking to infect companies and extort ransom payments as part of an operation to raise funds for the sanctioned Pyongyang regime.

Vault7 leaks

Vault7 was WikiLeaks' last good leak. It was a trove of documentation files describing the CIA's cyber-weapons. No source code was ever included; however, the leak provided a look into the CIA's technical capabilities, some of which included tools to hack iPhones, all the major desktop operating systems, the major browsers, and even smart TVs. At the time, WikiLeaks said it received the Vault7 data trove from a whistleblower, who was later identified as Joshua Adam Schulte.

MongoDB exposed

Although incautious sysadmins had been leaving databases exposed online without any password for years, 2017 was the year when hackers finally turned their attention to this previously untapped Internet resource. It began at the tail end of 2016 and picked up steam by January of 2017 with hackers accessing databases, deleting their content, and leaving ransom notes behind, asking for cryptocurrency to return the non-existent and previously deleted data. Although the first wave of attacks targeted the low-hanging fruit of MongoDB servers, hackers later expanded their reach to compromise other database technologies such as MySQL, Cassandra, Hadoop, Elasticsearch, and others.

Though widespread attacks died out by the end of 2017, they served to highlight the significant dangers of publicly exposed misconfigured databases. And by the end of the year a new category of security researchers known as "breach hunters" had been born. These were individuals who looked for open databases and then contact companies to let them know they're exposing sensitive information online. During 2018 and 2019 most security breaches and data exposures were being discovered by breach hunters, rather than hackers dumping a company's data online after an intrusion.

Equifax

2017 was also the year of the Equifax hack during which the personal details of more than 145.5 million Americans, British, and Canadian citizens were stolen from the company's systems. We know that the breach was the fault of Equifax failing to patch the Apache Struts vulnerability, but we still don't know who was behind the intrusion, or what their motives may have been.

Coinhive & Cryptojacking

It was also in the latter half of 2017 that Coinhive appeared and the term "Cryptojacking" was coined. The Coinhive service enabled hackers to make money by mining the Monero cryptocurrency on other people's computers after somehow arranging to load a snippet of JavaScript into a victim's browser. This continued until the collapse of cryptocurrency valuations which rendered the hacking less profitable.

Meltdown, Spectre, and the CPU side-channel attacks

Coming up with the big security event of 2018 is a no-brainer when you have Meltdown, Spectre and the myriad other attacks which were subsequently discovered to be theoretically effective against our modern processor's speculative executing microarchitectures. Even though not a single one of these was ever found to be exploited in the wild, by this time we had learned that, given time and sufficient motivation, bad guys WILL arrange to leverage ANY perceived weakness into a working exploit. So every single one of these fundamental architectural mistakes needed to be, and have so far been, cleaned up. Future CPU design has been hugely impacted as a result at the cost of some hopefully short-term performance.

Marriott gets hacked

While not as big as Yahoo's three-billion figure, but the Starwood/Marriott data breach deserves a mention due to its sheer size. The breach which was disclosed in November of 2018 impacted around 383 million of the chain's guests. When forensics investigators dug into the Starwood reservation system they discovered a RAT -- a Remote Access Trojan -- and the MimiKatz tool used to sniff username and passwords. There's never been any public disclosure of the route into Starwood's systems and it's entirely possible that only the attackers know.

2019 - The Year of the Ransomware

This brings us current with this year. Aside from the additional ongoing discoveries of yet another way to leverage security holes in mostly-Intel's processor architecture design, this has been, as I've noted earlier, by any measure the year when Ransomware really took off and created huge amounts of damage.

Given these past ten years I have no doubt that 2020 is going to be a year to watch. And we'll be right here bringing the news to all of our terrific listeners!

