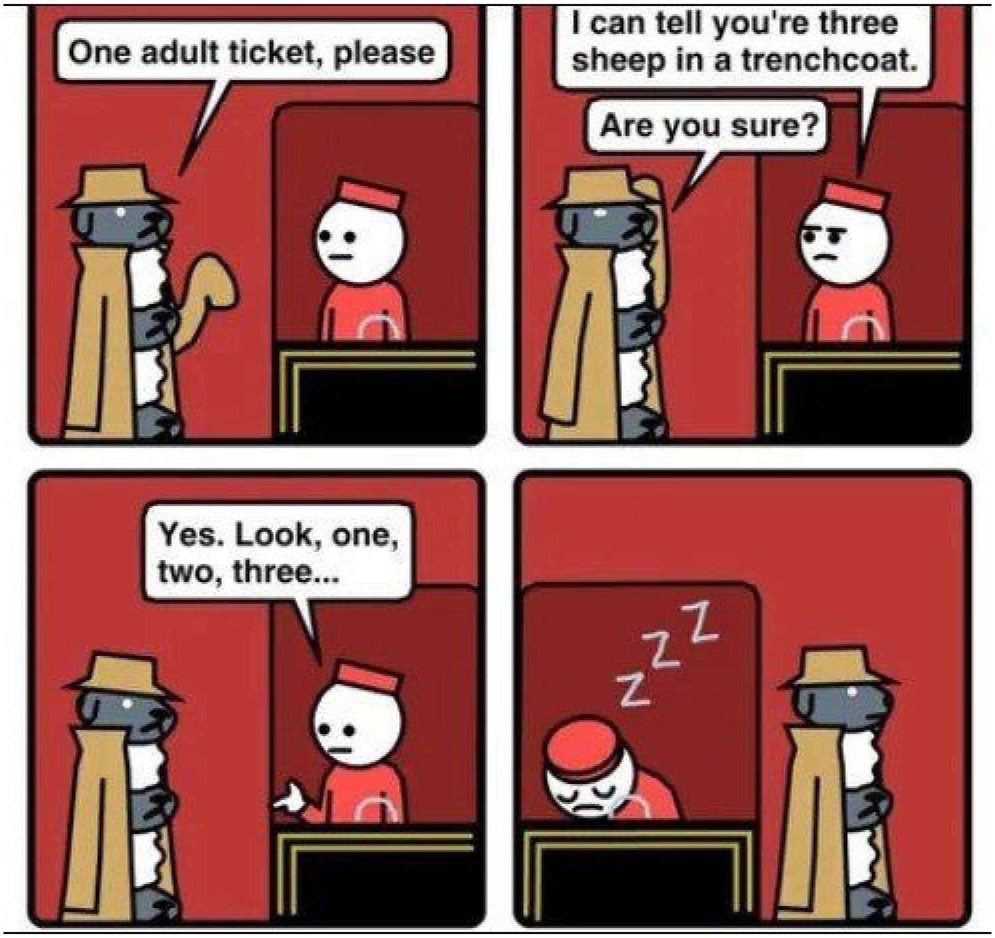
Security Now! #797 - 12-15-20
SolarWinds

This week on Security Now!

This week is crammed with news leading up to our holiday break. Chrome is throttling ads, there's new cross-browser as insertion malware, we have a new term in the ransomware world, we have last week's patch Tuesday, a jaw dropping policy leak from Microsoft, trouble for Cisco's Jabber, an embarrassing vulnerability in many D-Link VPN servers, the brief Google outage, more horrific news of IoT network stack vulnerabilities, another WordPress mess, the 2020 Pwnie Awards, the welcome end-of-life of Flash, JavaScript's 25th birthday and free instruction classes, a bit of closing the loop and SpinRite news, then we take a full reconnaissance dive into what happened with the monumental and in so many ways horrific SolarWinds supply chain security breach.

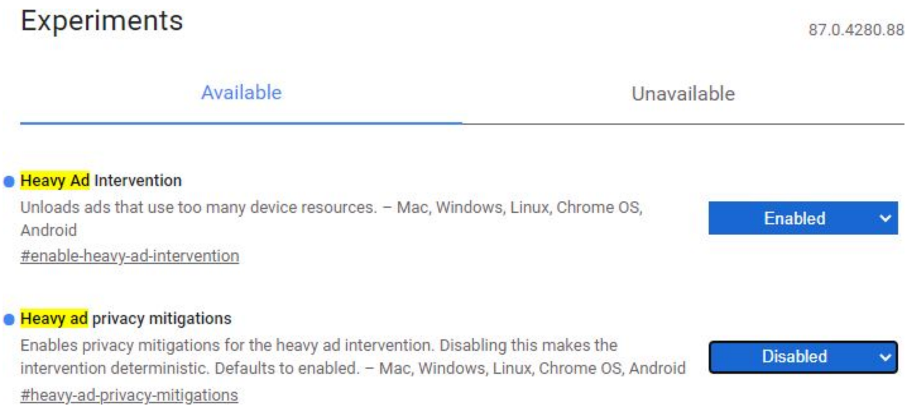

One adult ticket, please
I can tell you're three sheep in a trenchcoat.
Are you sure?
Yes. Look, one, two, three...
z z z

Browser News

Chrome's Heavy Ad Intervention

Chrome has begun rolling out its so-called “Heavy And Intervention” in Chrome 87. It's being spotted in the wild by some lucky users, and it affects both 3rd party ads and Google's own AdSense equally.

It's being rolled out gradually, and it wasn't yet enabled in my Chrome, but I definitely wanted it, so I turned it on. Anyone may do so by going to chrome://flags and search for “heavy ad” which will return two settings. They were both set to default, so I enabled the first and disabled the second:



● Heavy Ad Intervention
Unloads ads that use too many device resources. – Mac, Windows, Linux, Chrome OS, Android
#enable-heavy-ad-intervention
Enabled

● Heavy ad privacy mitigations
Enables privacy mitigations for the heavy ad intervention. Disabling this makes the intervention deterministic. Defaults to enabled. – Mac, Windows, Linux, Chrome OS, Android
#heavy-ad-privacy-mitigations
Disabled

The second option appears to make Chrome’s intervention less certain so that the presence of heavy ad blocking cannot be used as a tracking beacon.

Adrozek

Last Thursday, Microsoft's 365 Defender Research Team posted a blog titled: “Widespread malware campaign seeks to silently inject ads into search results, affects multiple browsers.” Microsoft named this malware “Adrozek” and one of the things that makes this malware noteworthy is that it is cross-family multi-browser, affecting Edge, Chrome, Yandex and Firefox.

And although its most prominent feature is unwanted ad injection, it not only injects ads, but the malware also exfiltrates any of the browser's stored credentials, which can cause significantly more harm than some unwanted ads injected into search results.

Microsoft wrote:

> We call this family of browser modifiers Adrozek. If not detected and blocked, Adrozek adds browser extensions, modifies a specific DLL per target browser, and changes browser settings to insert unauthorized ads into web pages, often on top of legitimate ads from search engines. The intended effect is for users, searching for certain keywords, to inadvertently click on these malware-inserted ads, which lead to affiliated pages. The attackers earn through affiliate advertising programs, which pay by amount of traffic referred to sponsored affiliated pages.
>
> Cybercriminals abusing affiliate programs is not new—browser modifiers are some of the oldest types of threats. However, the fact that this campaign utilizes a piece of malware that affects multiple browsers is an indication of how this threat type continues to be increasingly

> sophisticated. In addition, the malware maintains persistence and exfiltrates website credentials, exposing affected devices to additional risks.

The malware is surprisingly sophisticated. It disables browser updates to prevent its configuration modifications from being reversed, and it even establishes a Windows service to gain persistence over the long term.

The bad news is, before effective safeguards were put in place, Adrozek's sophistication allowed it to compromise more than 30,000 PCs per day. The good news is, as Microsoft's security people become aware of these threats, so does the Windows Defender protection suite. So it might be a good idea, just for some peace of mind, to ask Defender to perform a full scan of your various Windows systems.

(By the way, full scans take time. There's no way around that. As the author of SpinRite, I'm all too aware! Defender says to go ahead and use your PC while it scans in the background. But it aggressively throttles its scanning so as not to interfere with your use of the computer in the foreground. So it's best to choose a time when you're about to be away from your machine. In that case Defender will zoom along at best speed.)

I took my own advice and "Full Scanned" my Win10 machine last night while I was assembling these notes. It took 90 minutes and scanned 5,797,899 files…

Leo... after the scan was finished, I just stared at that number. I remember (fondly) when our hard drives had seven files. Now the number of files has seven digits. I do miss those days.

Ransomware News

"Double Extortion"

On the ransomware front, I just wanted to note the emergence of a new term coined by the security industry: "Double Extortion." It originated with CheckPoint last April to refer to the double threat of encryption plus public exposure of proprietary data if the victim should choose not to pay up. As we know, some companies will be extremely sensitive to the reputation damage — not to mention the potential liability — if the news of their breach should become widely known. So, henceforth, that embarrassment strategy will be termed "double extortion."

Security News

Patch Tuesday Retrospective

Your first thought upon hearing that last week Microsoft patched 58 known vulnerabilities across their various products you might think, "Wow! Only 58 this month! That's way fewer than the more than 100 we've been beaten into accepting as normal this year!" But then, when you stop to look closer, you realize that fully more than one third of those — 22 in total — are remote code execution (RCE) vulnerabilities!! And because several are in Exchange Server and SharePoint, I hope everyone has by now made time to get these updated. Although none are 0-days, meaning that none are known to be under exploitation at the time of their discovery, a total of 9 are rated critical, and some are not difficult to exploit once they become known. We know that bad guys rejoice every month now, and quickly work to reverse engineering Microsoft's updates in hope of working out an effective exploit before hapless Windows users update their vulnerable machines — especially when they are enterprises running servers that they would like to avoid rebooting and having offline during a patch cycle.

Among these 58 that Microsoft fixed this month was a bug in Microsoft's Hyper-V virtualization technology. It was exploitable via a malicious SMB packet and would allow remote attackers to compromise virtualized sandboxed environments, which Hyper-V was designed to protect.

So, yes, as always... Don't wait long to update.

And speaking of Microsoft updates, here’s a little bit of tid that caught my eye…
The news was about a 0-click wormable vulnerability in Microsoft Teams. Before this was fixed it would have allowed an adversarial attacker to remotely compromise a target's machine simply by sending them a specially-crafted hat message. The reception of this message would have enabled zero-click remote code execution on that system. This discovery was reported to Microsoft at the end of August, on the 31st, by Oskars Vegeris, a security engineer with Evolution Gaming. Microsoft addressed the issue at the end of October.

In Oskars' write up, he said: “No user interaction is required, exploit executes upon seeing the chat message. The result is a complete loss of confidentiality and integrity for end users — access to private chats, files, internal network, private keys and personal data outside MS Teams.”

And... the RCE is cross-platform — affecting Microsoft Teams for Windows (v1.3.00.21759), Linux (v1.3.00.16851), macOS (v1.3.00.23764), and the web (teams.microsoft.com) — and can be, as I said, made wormable. So it could be propagated by automatically reposting the malicious payload to other channels. This means the exploit can be passed on from one account to a whole group of users, thereby compromising an entire channel. So it's bad, right?

Now here's the tasty bit: This quite serious, 0-click, wormable, remote code execution vulnerability was assigned no CVE designation by Microsoft. Why? Microsoft said — and I quote — "It is currently Microsoft's policy to not issue CVEs [for flaws in] products that automatically update without user's interaction."

Wait. What?!?!

Leo... I haven't tracked down this apparent policy change. But it would be VERY interesting for you to ask Paul and MaryJo about this tomorrow. Could Microsoft's “solution” to the embarrassment of hundreds of CVE's being patched every month be to redefine problems by whether or not they are automatically repaired? If so... this is a whole new ballgame. This would suggest that anything that auto-updates — like Windows — would no longer have any actual vulnerabilities. After all, Windows is now a continually moving target that's always in flux. So, those are not actually vulnerabilities at all... They're just some miscellaneous things — like remotely taking over a Microsoft Teams user by sending them a Chat message — that haven't been finalized yet. But don't worry, we're working on it. It's not worth bothering yourself about.

Cisco is Jabbering...
Cisco has also been having recurring trouble keeping Chat secure. They have again attempted to patch their Jabber conferencing and messaging application against a critical vulnerability that made it possible for attackers to execute malicious code that would spread from computer to computer with no user interaction required.

https://www.watchcom.no/nyheter/nyhetsarkiv/cisco-jabber-vulnerabilities-resurface/

The discoverers of the trouble. Watchcom Security, explained what's been going on:

> The TL;DR is: Three months ago, Watchcom disclosed four high severity vulnerabilities in Cisco Jabber. One of the vulnerabilities allowed Remote Code Execution (RCE) by sending specially crafted chat messages — a problem that everyone seems to be having. The vulnerabilities were reported to Cisco and a patch was issued. Shortly after, one of Watchcom's clients requested a verification audit of the patch to ensure that the vulnerabilities had been sufficiently mitigated. Whoops!
>
> Three of the four vulnerabilities Watchcom disclosed in September have NOT been sufficiently mitigated! "Hello Cisco... Are you listening? Is anyone home?" Watchcom reported that Cisco released a patch that fixed the injection points they had reported, but the underlying problem was not fixed. And consequently, Watchcome was able to find new injection points that could be used to exploit the same vulnerabilities. All currently supported versions of the Cisco Jabber client (12.1 - 12.9) are affected.

For the sake of clarity, the three new(ish) vulnerabilities have been assigned new CVE numbers to distinguish them from the original similar vulnerabilities disclosed last September.

Watchcom explained that the new(ish) vulnerabilities have the same impact as the original and range in severity from medium to critical. As such, two of the vulnerabilities can be used to gain remote code execution.

The most severe vulnerability is a Cross Site Scripting (XSS) vulnerability that can be used to achieve RCE by escaping the Chromium Embedded Framework (CEF) sandbox. This vulnerability does not require user interaction and is wormable, since the payload is delivered via an instant message. This means that it can be used to automatically spread malware without any user interaction.

The second vulnerability can be exploited to collect NTLM (NT LanMan) password hashes from unsuspecting users. In a very clever hack... by sending a message that contains a malicious <img> tag, an attacker can induce the victim's Cisco Jabber client to interact with a file share under the attacker's control. If the file share requires authentication, the victim's NTLM password hash will be sent.

The 3rd vulnerability involves the custom protocol handlers used by Cisco Jabber. These protocol handlers are vulnerable to command injection because they fail to consider URLs that contain spaces. By including a space in the URL, an attacker can inject arbitrary command line flags that will be passed to the application. Since the application uses CEF (the Chromium Embedded

Framework) and accepts Chromium command line flags, several flags that can be used to execute arbitrary commands or load arbitrary DLLs exist. Whoopsie.

While Cisco's first patch filtered some of these, Watchcom was still able to identify a dangerous flag that could bypass the filter. The flag can be used to enable remote debugging, allowing an attacker on the same network to take control of the embedded browser in the victims Cisco Jabber client.

Watchcome wrote something in the conclusion of their disclosure that I thought was worthy of the whole story. They wrote:

> The continued existence of these vulnerabilities, even after the first patch, highlight the complexity of modern software and the challenges developers face when trying to secure it. When choosing to use frameworks such as CEF, it is important to consider their security implications. Security should also be considered in every step of the development process, both in the initial planning stages as well as during implementation and maintenance.
>
> This also serves as a reminder that software acquired from external vendors also pose a risk to organizations' IT-security. It is important to be aware of these risks and take steps to mitigate them. Watchcom recommends regular audits of third-party software for security vulnerabilities.

Amen to all of that.

An embarrassing vulnerability in D-Link VPN servers

The embarrassing vulnerabilities — yes, three of them — were discovered by the guys at Digital Defense and were subsequently responsibly disclosed to D-Link four months ago on August 11th. D-Link finally confirmed the issues in an advisory on December 1, adding that patches were under development for two of three flaws which have now been released to the public.

The flaws are high-risk (as I said, embarrassing!) critical security vulnerabilities affecting D-Link's widely sold VPN router models DSR-150, DSR-250, DSR-500, and DSR-1000AC and other VPN router models in the DSR Family, running the current firmware versions 3.14 and 3.17. Even if these devices are secured with strong passwords, the vulnerabilities have left millions of home and business networks open to attack... Because they provide a full authentication bypass, allowing remote attackers to execute arbitrary commands on those devices through specially-crafted requests.

Did I mention that these were particularly embarrassing? The flaws originate from the fact that the web management interface uses "Lua CGI" which is fully accessible without authentication and lacks any server-side filtering. This makes it possible for an unauthenticated attacker to inject malicious commands that will be executed with root privileges. And this works over the Internet-facing WAN interface.

The takeaway for our listeners is that if you or your enterprise are using any of these quite popular D-Link VPNs, be sure to obtain and update to the most recent firmware with some priority.

Google suffered an outage — nothing to see here. These are not the droids you're looking for. The conspiracy folks stepped right up with various attack nonsense. But Google quickly dispelled those theories. They first acknowledged the trouble at 4:20am Pacific Time, posting:

"We're aware of a problem with Gmail affecting a majority of users. The affected users are unable to access Gmail. We will provide an update by December 14, 2020 4:12:00 AM PST detailing when we expect to resolve the problem. Please note that this resolution time is an estimate and may change."

Then, about 3 hours later, at 7:30am Pacific Time, they updated:

“Today, at 3:47am PT Google experienced an authentication system outage for approximately 45 minutes due to an internal storage quota issue. This was resolved at 4:32AM PT, and all services are now restored.”

So, unusual as that was, it was no attack, nothing untoward... Just whatever that was.

Amnesia:33

Last Wednesday, during BlackHat Europe 2020, researchers from Forescout Technologies presented their paper titled: “How Embedded TCP/IP Stacks Breed Critical Vulnerabilities”

In their teaser synopsis they wrote:

> In the past few years, there's been a rise in critical vulnerabilities affecting embedded TCP/IP stacks which had remained undiscovered for over a decade. The direct, unauthenticated and sometimes cross-perimeter network exposure of these stacks, the often privileged portions of the system they run in and their position at the top of opaque supply chains complicating vulnerability management efforts make for a highly dangerous mix resulting in periodic waves of critical vulnerabilities affecting billions of devices across industry verticals. But contrary to what many assume, the fragility of these fundamental components isn't limited to specific vendors or older, closed-source stacks alone.
>
> In this talk, we will present over a dozen new vulnerabilities in multiple widely used embedded TCP/IP stacks deployed in everything from networking equipment and medical devices to industrial control systems. We will discuss the nuances in their exploitability & potential impact and demonstrate a proof-of-concept against a yet-to-be-disclosed high profile target. In addition, we will present the first quantitative & qualitative study into vulnerabilities affecting embedded TCP/IP stacks showing a clear pattern to the affected components & features as well as the root causes of the vulnerabilities that affect them. Finally, we will provide concrete advice on how to mitigate and manage vulnerabilities affecting billions of devices in the absence of centralized patching and notification efforts.

Needless to say, that's quite a meal.

https://i.blackhat.com/eu-20/Wednesday/eu-20-dosSantos-How-Embedded-TCPIP-Stacks-Breed-Critical-Vulnerabilities-wp.pdf

That's the introduction to their 47-page paper. Stepping back a bit, they coined the name “Amnesia:33” because they uncovered a set of 33 vulnerabilities collectively impacting four different open-source TCP/IP protocol stacks — uIP, FNET, picoTCP, and Nut/Net — are commonly used in Internet-of-Things (IoT) and embedded devices. As a consequence of improper memory management, successful exploitation of these flaws could cause memory corruption, allowing attackers to compromise devices, execute malicious code, perform denial-of-service (DoS) attacks, steal sensitive information, and even poison DNS cache memory. In real world scenarios, these attacks could play out in various ways: disrupting the functioning of a power station to result in a blackout or taking smoke alarm and temperature monitor systems offline by using any of the DoS vulnerabilities.

Many millions of devices from an estimated 158 vendors are vulnerable to the AMNESIA:33 discoveries, with the possibility of remote code execution allowing an adversary to take complete control of a device, and using it as an entry point on a network of IoT devices to then move laterally, establish persistence, and co-opt the compromised systems without any outward appearance of compromise.

If we imagine that nation-state actors are greedily mopping up all available exploits everrywhere they appear, then this research from Firescout was likely greeted with a great deal of mopping. Forescout said that “AMNESIA:33 affects multiple open source TCP/IP stacks that are not owned by a single company. This means that a single vulnerability will exist across multiple codebases, development teams, companies and products, which presents significant challenges to patch management.”

Because these vulnerabilities span a complex IoT supply chain, Forescout cautioned it's as challenging to determine which devices are affected as they are hard to eradicate. The AMNESIA:33 flaws stem from out-of-bounds writes, buffer overflows, and lack of input validation. They lead to memory corruption, enabling an attacker to put devices into infinite loops, poison DNS caches, and extract arbitrary data.

Critical remote code execution vulnerabilities exist in uIP, picoTCP, and Nut/Net. Each has a CVSS score of 9.8. Some of the vendors who utilize these stacks are being responsible. Vendors such as Microchip Technology and Siemens whoSe products are affected by these vulnerabilities have released security advisories.

As Forescout put it: “Embedded systems, such as IoT and [operational technology] devices, tend to have long vulnerability lifespans resulting from a combination of patching issues, long support lifecycles and vulnerabilities 'trickling down' highly complex and opaque supply chains. As a result, vulnerabilities in embedded TCP/IP stacks have the potential to affect millions – if not billions – of devices across vertical markets and tend to remain a problem for a very long time.”

The problems are severe enough for the CISA to get involved and to urge awareness. But that didn't appear to have much impact when they had urged companies to update against the Microsoft ZeroLogon vulnerability. Asking IoT vendors to path their unpatchable devices seems a clearly doomed exercise in futility.

My feeling is that we MUST treat IoT gadgets with the assumption that they are compromised and rigorously relegate them to their own isolated networks.

If you can access your various IoT devices from outside your home then it's clear that you and they do not need to share a common network. Your untrusted IoT LAN should coexist with your trusted LAN, but they should not have any contact with one another.

Another WordPress mess

I got a kick out of the subhead that ZDNet chose. Their headline was: “Zero-day in WordPress SMTP plugin abused to reset admin account passwords.” and their sub-head was: “A patch was released earlier this week but many WordPress sites remained unpatched —as usual.”

So, first off, as we know, the term “0-day” has unfortunately become synonymous with “bug”. The press is tending to call everything a 0-day because it sounds a lot more serious. It was meant to. But referring to everything as a 0-day will ultimately render the term worthless.

In this case, refreshingly, it really is a 0-day. Hackers have been using a design mistake coupled with a dumb configuration setting of a popular WordPress add-on to easily reset the admin passwords on WordPress sites. And the add-on is considered popular because it's installed on more than 500,000 sites. The hacking has been underway for some weeks and a patch for the design error was made available last Monday — thus, a true 0-day vulnerability.

The add-on in question is “Easy WP SMTP” — obviously a plugin that lets site owners configure the SMTP settings for their website's outgoing emails and add features.

One of the several features it boasts is the: “Option to enable debug logging to see if the emails are getting sent out successfully or not.” That feature causes the system to log all eMail headers and body that is sent. And that eMail log is located in the plug-in's well-known installation directory “/wp-content/plugins/easy-wp-smtp/”. Thus that's no mystery.

https://blog.nintechnet.com/wordpress-easy-wp-smtp-plugin-fixed-zero-day-vulnerability/

But, the team at Ninja Technologies Network (NinTechNet) discovered that although Easy WP SMTP v1.4.2 and older — which was current before last week's update — gives the log a fancy random name like “5fcdb91308506_debug_log.txt”, the plug-in's folder lacks any index.html file. So when the site is being hosted on servers with directory listing enabled, hackers can view the directory, see the fancy-named eMail log, and view its contents. Then, they cause the blogging site to send its administrator a password reset eMail, refresh the view of the sent eMail log, capture the password recovery link and take over the site.

I mentioned before that while I was hosting my own WordPress blog, I was horrified by the idea of the site's admin login form being public. The idea that anyone could enter the well-known URL of the admin logon and be looking at a prompt for a username and password to login as me was appalling. So, one of the first “belt and suspenders” things I did, was to completely block access to any admin-related pages — first and foremost the front door — from any remote IPs other than mine. As we know, the public IPs we're assigned by ISP are relatively static, so it's just as simple as using an .htaccess or in my case a web-config file for IIS to filter incoming page requests. If my IP did happen to change so that I was also locked-out, then I would need to log onto the hosting server itself — which I would do using a certificate-tied SSH client — not merely a username and password — to update the access control with my new remote IP.

My point is, I'll never know what attacks that bit of superstition might have thwarted. But the idea of exposing my WordPress login page to the world just made me shiver... as I hope it would for any of our listeners.

The 2020 Pwnie Awards

Speaking of Black Hat Europe 2020, the annual Pwnie awards were announced last week during the conference. For those who don't recall, the Pwnie's are to our cyber-security industry what the Oscars and the Razzie awards are to the movie industry.

Each year, cyber-security researchers are invited to nominate and vote for both the best and worst in their industry. This includes selecting the best and most ingenious vulnerabilities discovered during the past year, and also the worst vendor responses and epic fails that put their users at risk.

Traditionally, the Pwnie Awards ceremony has taken place every August during the Black Hat USA security conference in Las Vegas. But this year, with the COVID-19 pandemic virtualizing conferences, it was decided that the Pwnie Awards would be moved to Europe's Black Hat conference. Among the results are the many things we've talked about during the year:

- Best server-side bug: BraveStarr - a remote code exploit in the Telnet daemon on Fedora 31 servers.

- Best client-side bug: For a zero-click MMS attack on Samsung phones, bug discovered by the Google Project Zero team.

- Best privilege escalation bug: Checkm8 - an unpatchable hardware jailbreak for seven generations of Apple silicon.

- Best cryptography attack: Zerologon - a bug in Microsoft's Netlogon authentication protocol that can be performed by adding adding a bunch of zero characters in certain Netlogon authentication parameters.

- Most innovative research: TRRespass - bypassing TRR protections on modern RAM cards to carry out Rowhammer attacks.

- Most epic fail: Microsoft for CurveBall, a bug in how the company implemented elliptic curve signatures on Windows, allowing for easy spoofing of HTTPS sites and legitimate apps.

- Epic achievement: To Guang Gong, a known Chinese bug hunter, for discovering CVE-2019-5870, CVE-2019-5877, CVE-2019-10567, three bugs that allowed remote takeovers of Android Pixel devices [see PDF].

Not a Flash in the pan

Adobe's infamous flash player was anything but a flash in the pan. It was first released 24 years ago in January of 1996. Back then, web pages were predominantly static HTML. JavaScript was just beginning to happen, but it didn't have any of the new browser features to drive. So its application back then was very limited. But Flash added a complete self-contained content authoring, locally interactive and animating facility. You could write a working game in Flash — and many developers did. Because it was a world unto itself, it was inherently browser agnostic. If a browser had a Flash plug-in, the content would run. It really was quite something for the era, and it was immediately adopted by developers to create interactive content for the web.

Flash's Achilles' heel, as we all know too well, was that it was originally written, like most of the software of the time, with virtually no regard for security. And it was never able to recover from that lack of security legacy. It was much like the Internet back then... the fact that it ran at all was regarded as a miracle. Security wasn't even a thought, let alone an after thought.

But thanks to the incredible progress made in turning our browsers into fully programmable web application hosting containers, driven by JavaScript, more than 1,444,231 add-on JavaScript function libraries, and a very mature and formalized Document Object Model that allows a web page's presentation to be fully accessible and manipulatable by JavaScript... the only thing that has kept Flash alive has been the residual inertia still remaining from its once total dominance.

So, against that backdrop, last week Adobe released their **final update EVER** of their Flash player, and reminded the world that Flash is finally, once and for all, being extinguished forever. And it's not as if no one has received notice. It was way back in 2017 that Adobe, Microsoft, Google, Apple, and Mozilla made a joint announcement that they would be retiring support for Adobe Flash Player at the end of 2020.

In their final Flash Player release notes, Adobe said: “We want to take a moment to thank all of our customers and developers who have used and created amazing Flash Player content over the last two decades. We are proud that Flash had a crucial role in evolving web content across animation, interactivity, audio, and video.”

So, beginning next month, Chrome, Safari, Firefox, Edge, IE11, and other Chromium-based browsers will remove Flash from their bodies and it will become impossible to put it back. So long and farewell. Whew!

JavaScript

And while I'm on the topic of browser coding and automation, JavaScript is celebrating its 25th birthday and we're in the second week of free courses being offered every week at JavaScript.com:

https://www.javascript.com/

The site says: To celebrate one of the most popular languages in the world, we're making five of our expert-authored JavaScript courses free every week in December.

Closing The Loop

David P. Vallee @Yossarrian

Hi Steve, Listened to the Amazon Sidewalk podcast. Sounds like Amazon did everything imaginable to protect customers. The question that occurs to me is how often does the Internet connectivity of a single home go down? If the carrier drops, everyone's IOT devices will go out in a large radius. Way beyond the range of Sidewalk. Since IOT's use a small amount of bandwidth, for a home to need this, they would need a complete failure of either their router, or modem. When's the last time yours, or a friend of yours, had a router crash? Thanks again for a great podcast.

SKYNET @fairlane32

I'm excited about Amazon Sidewalk in that you could get pets that are microchipped onto the sidewalk network it may be possible, providing a lot of people participate, to locate them if they're ever lost. Imagine being able to find those dogs/ cats that get loose. And with all the established social media groups using the network, you could possibly be able to find lost pets within hours, not days or weeks. But are those microchips transmitting on the 900Mhz spectrum?

SpinRite

InitDisk release 4 published.

We've been at the Release Candidate stage of this project for a couple of weeks. But a diminishing number of minor things are still popping up here and there. My feeling is that it is much better to deal with them in our current relatively quiet setting with people who have become very familiar with this project than ignoring the edge cases and putting them off until after a much broader public release. So, as **very** anxious as I am to get this into the hands of a much wider audience, it makes more sense to first get it as right as possible.

For example, in the past week we found a system whose BIOS did not like the Master Boot Record (MBR) which I was using from Windows 2000, despite having deliberately chosen it for its maturity and assumed compatibility. But it did like the MBR from Windows 7... as has everyone else's systems. So that's changed.

Someone else had a USB thumb drive that just refused to work on his Win10 machine. But he was able to bring up a temporary Win7 PE system where it did work. Since my clear goal has been to create a single USB formatting utility that easily and always works everywhere, I needed to figure out what was going on. We struggled with that one for a few days until I realized that something about the history of that USB stick and his Windows system had to be the problem. So now InitDisk explicitly deletes any prior drive mounting history for the device it's formatting.

And a couple of people have dying drives where I was able to improve the error handling of the benchmark so that it would keep looking for a nearby block of storage where it might succeed.

The upshot is that our already public InitDisk utility is now at release 4 and it's better than ever. This is the technology that the ReadSpeed benchmark Windows prep utility will be using, as will the next SpinRite.

SolarWinds

FireEye:
The story begins with last Tuesday's news and admission from FireEye that they were hacked. FireEye is a three and a half billion dollar security company, one of the largest of its kind in the world. It was founded in 2004, has more than 8,500 customers spread across 103 countries and more than 3,200 employees worldwide.

https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

In his disclosure of the event, FireEye's CEO Kevin Mandia explained what they knew then:

> FireEye is on the front lines defending companies and critical infrastructure globally from cyber threats. We witness the growing threat firsthand, and we know that cyber threats are always evolving. Recently, we were attacked by a highly sophisticated threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Our number one priority is working to strengthen the security of our customers and the broader community. We hope that by sharing the details of our investigation, the entire community will be better equipped to fight and defeat cyber attacks.
>
> Based on my 25 years in cyber security and responding to incidents, I've concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past.
>
> We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.
>
> During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits. Consistent with our goal to protect the community, we are proactively releasing methods and means to detect the use of our stolen Red Team tools.
>
> We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools.

> Consistent with a nation-state cyber-espionage effort, the attacker primarily sought information related to certain government customers. While the attacker was able to access some of our internal systems, at this point in our investigation, we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements, or the metadata collected by our products in our dynamic threat intelligence systems. If we discover that customer information was taken, we will contact them directly.

So that was exactly one week ago today. Then, two days ago, on Sunday, the other BIG and startling shoe dropped. We'll stay with Kevin for the moment:

https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

His Sunday update posting was titled: "Global Intrusion Campaign Leverages Software Supply Chain Compromise." They discovered the bad guys' point of entry. Kevin wrote:

> In our announcement on Dec. 8, we stated we would provide updates as we discovered additional information, in order to ensure that the broader community is aware of the evolving threats we all face. As part of that commitment, we want to provide you with the following update on our investigation.
>
> We have identified a global campaign that introduces a compromise into the networks of public and private organizations through the software supply chain. This compromise is delivered through updates to a widely-used IT infrastructure management software—the Orion network monitoring product from SolarWinds. The campaign demonstrates top-tier operational tradecraft and resourcing consistent with state-sponsored threat actors.
>
> Based on our analysis, the attacks that we believe have been conducted as part of this campaign share certain common elements:
>
> - Use of malicious SolarWinds update: Inserting malicious code into legitimate software updates for the Orion software that allow an attacker remote access into the victim's environment
> - Light malware footprint: Using limited malware to accomplish the mission while avoiding detection
> - Prioritization of stealth: Going to significant lengths to observe and blend into normal network activity
> - High OPSEC: Patiently conducting reconnaissance, consistently covering their tracks, and using difficult-to-attribute tools
>
> Based on our analysis, we have now identified multiple organizations where we see indications of compromise dating back to the Spring of 2020, and we are in the process of notifying those

organizations. Our analysis indicates that these compromises are not self-propagating; each of the attacks require meticulous planning and manual interaction. Our ongoing investigation uncovered this campaign, and we are sharing this information consistent with our standard practice.

We have been in close coordination with SolarWinds, the Federal Bureau of Investigation, and other key partners. We believe it is critical to notify all our customers and the security community about this threat so organizations can take appropriate steps. As this activity is the subject of an ongoing FBI investigation, there are also limits to the information we are able to share at this time.

We have already updated our products to detect the known altered SolarWinds binaries. We are also scanning for any traces of activity by this actor and reaching out to both customers and non-customers if we see potential indicators.

FireEye's mission is to make our customers and the broader community safer. We are methodically uncovering and exposing this campaign piece by piece and working to prevent future attacks. It will require coordinated action by public and private organizations to fully expose and mitigate this threat, and we intend to continue our efforts.

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

FireEye's Technical Presentation:
Their technical presentation contains lots of interesting details. They begin by setting the stage, writing: "FireEye has uncovered a widespread campaign that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software. This campaign may have begun as early as Spring 2020 and is currently ongoing. Post compromise activity following this supply chain compromise has included lateral movement and data theft. The campaign is the work of a highly skilled actor and the operation was conducted with significant operational security."

Then they get into the details...

"SolarWinds.Orion.Core.BusinessLayer.dll" is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

[Note that this Trojan was digitally signed by SolarWinds on March 24th of this year. And once SolarWinds' customers updated their systems to incorporate this malicious — though signed — component, those customers were Trojanized.]

After an initial dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the

> Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. The backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as processes, services, and drivers.
>
> *[Okay. So note that this malware's deep knowledge of SolarWinds application software and network operation means that this was not a coincidental intrusion into SolarWinds, either. The bad guys would have had to first see whether they could somehow arrange to get their malware merged into SolarWinds' code base so that it would then be signed and sent along with the next update. They probably targeted SolarWinds because updates to this company's products would successfully spread any inserted compromise far and wide. This was clearly a huge effort.]*
>
> Multiple Trojanzied updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website, including:
>
> hxxps://downloads.solarwinds[.]com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20574/SolarWinds-Core-v2019.4.5220-Hotfix5.msp
>
> The trojanized update file is a standard Windows Installer Patch file that includes compressed resources associated with the update, including the trojanized “SolarWinds.Orion.Core.BusinessLayer.dll” component. Once the update is installed, the malicious DLL will be loaded by the legitimate “SolarWinds.BusinessLayerHost.exe” or “SolarWinds.BusinessLayerHostx64.exe” (depending on system configuration). After a dormant period of up to two weeks, the malware will attempt to resolve a subdomain of avsvmcloud[.]com. The DNS response will return a CNAME record that points to a Command and Control (C2) domain. The C2 traffic to the malicious domains is designed to mimic normal SolarWinds API communications. [This would allow the malicious traffic to slip through protocol-aware intrusion detection systems.' The list of known malicious infrastructure is available on FireEye’s GitHub page.
>
> FireEye has detected this activity at multiple entities worldwide. The victims have included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East. We anticipate there are additional victims in other countries and verticals. FireEye has notified all entities we are aware of being affected.
>
> We are currently tracking the software supply chain compromise and related post intrusion activity as UNC2452. After gaining initial access, this group uses a variety of techniques to disguise their operations while they move laterally. This actor prefers to maintain a light malware footprint, instead preferring legitimate credentials and remote access for access into a victim’s environment. This section will detail a few of the notable techniques and outline potential opportunities for detection.

These folks were really clever. The more details that emerge, the more you realize how much time and attention these people put into this. For example, the IP addresses used for the campaign were obfuscated by VPN servers located in the same country as the victim to evade suspicious IP detection.

What we know…
SolarWinds' networking and security products are used by more than 300,000 customers worldwide, including Fortune 500 companies, government agencies, and education institutions. SolarWinds used to have a page bragging about all their customers but — gee, I wonder what happened? — that page has disappeared from the Internet and from the Internet Archive.

SolarWinds also serves several major US telecommunications companies, all five branches of the US Military, and other prominent government organizations such as the Pentagon, State Department, NASA, National Security Agency (NSA), Postal Service, NOAA, Department of Justice, and the Office of the President of the United States. So, it's not difficult to imagine the frantic scurrying that has gone on over the past several days.

The US Department of Homeland Security, the US Treasury and the US NTIA are all confirmed victims. In an SEC filing, SolarWinds confirmed that the Trojanized updates were installed by more than 18,000 of their customers. SolarWinds is a major contractor for the US government, with regular customers including the CISA, US Cyber Command, the DOD, the FBI, the DHS, the VA and many many others.

Imagine being the US National Security Agency and learning that since March an extremely well designed and carefully used spying agent has without doubt been operating within your network? We don't know what protections the NSA might have. They may have fully separate networks so that only the administrative staff have SolarWinds Orion on their network. But, boy is this a huge event!

Brandon Wales, and acting director of CISA, US Cybersecurity and Infrastructure Security Agency released an emergency directive, urging federal civilian agencies to review their networks for suspicious activity and disconnect or power down SolarWinds Orion products immediately. He wrote: “The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks.” Yeah, thanks for the heads-up, Brandon. No kidding.

Citing industry sources, Reuters reported that despite a broad install base for the Orion platform, the attackers appear to have focused only on a small number of high-value targets, leaving most Orion customers unaffected. And, of course, this is exactly how you act when you have just landed the Golden Goose of all intrusions, arranging to have itself installed into many ultra-high value targets.

Other people familiar with the situation told the Wall Street Journal that the Russian foreign-intelligence service is believed to be behind the attacks and that quote “Hundreds of thousands of government and corporate networks” have been opened to potential risk, making it a notable attack that goes far beyond the garden-variety espionage attempt. That seems like a bit of an hysterical exaggeration, but it's true that any networks that were accessible by any compromised networks would have been put at risk.

At the Russian Embassy in Washington D.C., someone pressed a keyboard macro which automatically typed the response: ***“The reports are unfounded attempts of the U.S. Fake Media to blame Russia.”***

If SolarWinds knows how the bad guys gained the foothold within their enterprise network, they're still not saying publicly.

The ENDURING trouble, of course, is that networks are networks of computers. We all know that once a single computer has been infected with malware, the nature of malware means... that it's never possible to fully trust that machine again. And this would be especially true for this presumed ultra-highly sophisticated attacker. But what makes matters so much worse, is that it wasn't a single machine that was attacked, but a highly connected network management appliance... which itself, in turn, had access to any number of other machines on the network.

We know how good these guys are. So they may well have planned ahead for the day their hack was discovered by planting entirely different malware in targets they don't want to lose access to. I'd be shocked if they hadn't.

And to make matters still worse, it turns out that Orion had been (I’m using the past tense) a highly trusted component which, by design, was trusted to hold and deploy credentials, including the Domain Admin, Cisco/Router/SW root/enable credentials, ESXi/vCenter Credentials, AWS/Azure/Cloud root API keys. and so much more. If you had the malicious Orion component on your network, ALL of those credentials must be considered to have been compromised.

And let’s not forget that these cretins had been crawling around since the end of March of this year. The mistake they made — and they probably didn’t make it until they had already done a lot more damage elsewhere — was in attempting to crawl around within FireEye’s network. SOMETHING tipped-off FireEye to the presence of this extremely stealthful intrusion. If it weren’t for FireEye’s detection, SolarWinds would still be unwittingly distributing malicious components and this probably-Russian espionage campaign would still be going strong.