Security Now! #696 - 01-08-19

Here Comes 2019!

This week on Security Now!

This week we look at the NSA's announced forthcoming release of an internal powerful reverse-engineering tool for examining and understanding other people's code, emergency out-of-cycle patches from both Adobe and Microsoft, and, yes, we do need to mention PewDiePie again. We also need to mention our prolific 0-day dropper SandboxEscaper, a new effort by the US government to educate industry about the risks of Cyber attacks, some welcome news on the ransomware front, some VERY welcome news of a new Windows 10 feature and a note about a just-published side-channel attack on OS page caches. Then we'll wrap with an update on my work on SQRL and my discovery of a VERY impressive and free large file transmission and sharing facility.

Security News

The NSA to release GHIDRA

On Podcast Tuesday, March 5th, 2019 Robert Joyce, a senior advisor with the US National Security Agency will be offering this talk, titled: "Come Get Your Free NSA Reverse Engineering Tool!"

Robert's talk abstract reads: "NSA has developed a software reverse engineering framework known as GHIDRA, which will be demonstrated for the first time at RSAC 2019. An interactive GUI capability enables reverse engineers to leverage an integrated set of features that run on a variety of platforms including Windows, Mac OS and LINUX and supports a variety of processor instruction sets. The GHIDRA platform includes all the features expected in high-end commercial tools, with new and expanded functionality NSA uniquely developed, and will be released for free public use at RSA."

The public was first made aware of GHIDRA from a Vault7 WikiLeaks leak:
https://wikileaks.org/ciav7p1/cms/page_51183656.html

Ghidra (Final Fantasy V): "Ghidra is an enemy fought at Ronka Ruins alone and can also be fought in the battle with an Alchymia. It is a dangerous foe as it has Auto-Reflect and battles using Poison Breath and Lightning. It is the earliest that the Blue Magic spell, Level 4 Graviga, can be obtained, and it has the Killer Bow to steal (Ronka Ruins only). If caught by a Beastmaster's Catch ability, it will cast Earth Shaker when released (Earthquake if caught from the Alchymia battle)."

The WikiLeaks-quoted version of Ghidra was v7.0.2.
We know that Ghidra requires Java. The current version requires Java 1.7

According to the Vault 7 documents, GHIDRA was initially developed by the NSA in the early 2000s, and a Reddit user named hash_define, who claimed to have had access to GHIDRA, said that the tool had been shared with several other US government agencies (mentioning the IA) in the past few years.

While there is no explicit announcement yet that the NSA plans to open source GHIDRA, some believe the agency will also publish GHIDRA source code on the NSA's Github code repository where it has already released 32 projects, so that the open source community can help maintain it for free.

The buzz within the reverse engineering community is that the promise of a good solid user-interface, apparently with a strong "typing" feature set, would fill an important gap that's lacking in current reverse engineering tools. And since a single-seat license for IDA-Pro (Interactive DisAssembler), the current favored tool, costs $1,866.99, we might imagine that everyone except "Hex-Rays" -- the company that's been offering IDA-Pro, is quite delighted by the idea of a serious free alternative.

And IDE is a Integrated Development Environment. An IDA -- an Interactive DisAssembler -- is sort of the reverse. The IDA's challenge is that so much of the programmer's originally supplied information is inherently lost in the process of assembling or compiling. Unless "debugging" information is deliberately left in the shipping product -- which should never happen -- ALL of the textual labeling of the program's objects: subroutine, procedure and variable names are lost... since those were only ever for the convenience of the coder and the computer uses the memory addresses of those objects.

The automated portion of the disassembler can analyze the program's flow. It can essentially step through the code, emulating its operation and following all of the code's various possible execution paths. This identifies what's code and what's non-code data. The disassembler can note the addresses that are being read and written, when the size of the reads and write to strengthen its heuristic sense for what's what. And it can then graphically break things apart into visual blocks of execution. It can observe chunks of code that have an entry point and a return to their caller, and decide they must be subroutines. And when the code calls into the operating system -- as it invariably must --to execute known operating system functions -- which, being known, can provide significant clues to that those regions of the program may be doing. And since the types of parameters used by those OS functions is also known, those parameters can be automatically labeled and identified. So, without attempting to "understand" what the program does, it can be sort of "unfolded" and opened up.

It's at that point where the user gets involved interactively. By examining and actually understanding what those displayed program instructions are doing, meaning can be added onto this framework. Actual names can be ascribed to variables and to those previously anonymous subroutines, and, over time, working back and forth, a full understanding of the program's operation can be divined.

I imagine that the week after the March 5th presentation, during our March 12th podcast, we may have a lot more to say about this interesting development.

Adobe patches two CRITICAL bugs

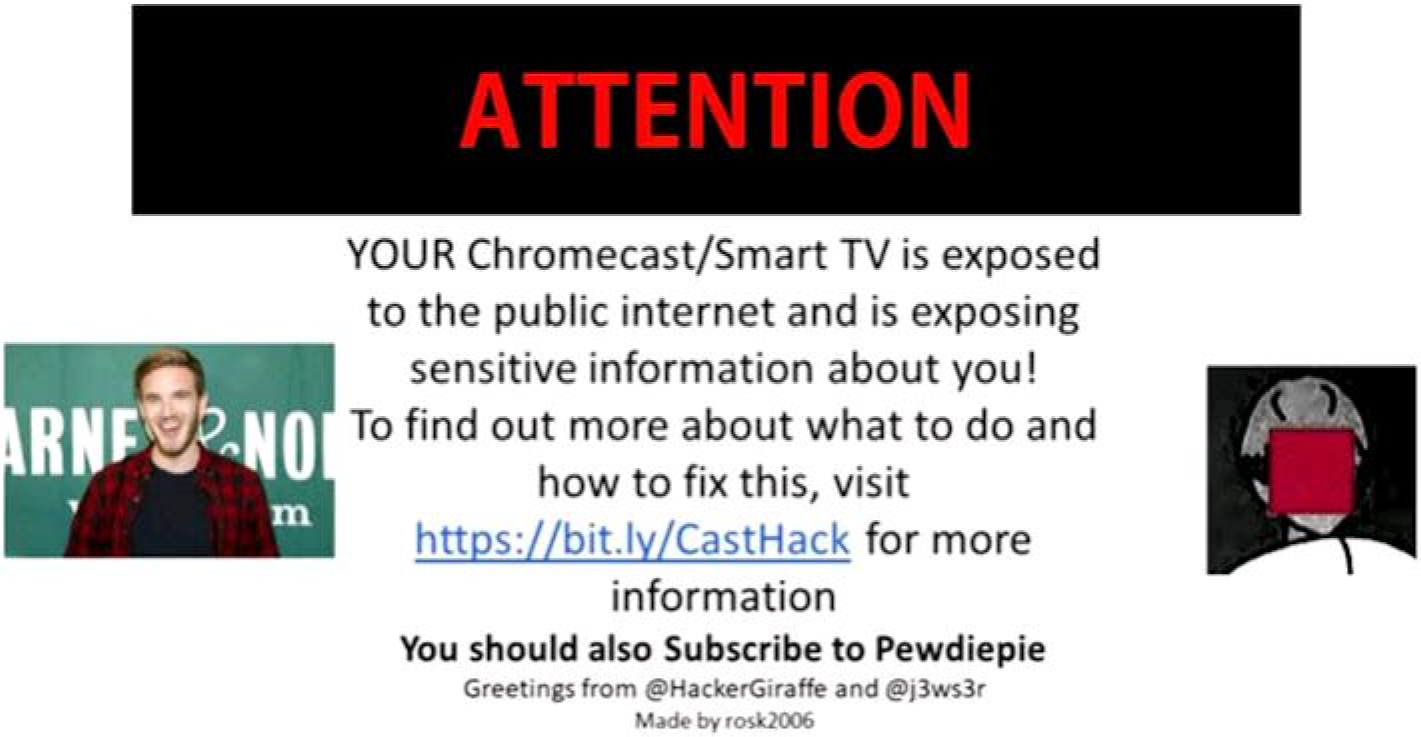
Last Thursday the 3rd, Adobe released a pair of emergency out-of-cycle patches for their Acrobat and Reader PDF system. The good news is that while the bugs are rated critical and do allow for remote code execution and privilege elevation, Trend Micro, who found and reported the problems to Adobe, was unaware of any ongoing exploitation in the wild. However, an attack leveraging these flaws only requires the victim to open a specially crafted PDF... and BLAMO!. This makes them high-value for targeted phishing attacks and so they would be unlikely to be used widely -- and spotted easily -- if they were in use. So, when you can, check your instances of Acrobat and Reader for any available updates.

And believe it or not, on this 1st podcast of the New Year…

…. we're going to talk about…

.... wait for it…

…. Yes……………………………………………. **PewDiePie!**



ATTENTION

YOUR Chromecast/Smart TV is exposed to the public internet and is exposing sensitive information about you!
To find out more about what to do and how to fix this, visit https://bit.ly/CastHack for more information

You should also Subscribe to Pewdiepie

Greetings from @HackerGiraffe and @j3ws3r

Made by rosk2006

https://casthack.thehackergiraffe.com/#faq

FAQ - Frequently Asked Questions

- What is going on?
  If you came here because you're a victim of #CastHack, then know that your Chromecast/SmartTV/GoogleHome is exposed to the public internet, and is leaking sensitive information related to your device and home.

- What information is being leaked?
  What WIFI your Chromecast/Google Home is connected to, bluetooth devices it has paired to, how long it's been on, what WiFi networks your device remembers, what alarms you have set, and much more.

- What can hackers do with this?
  Remotely play media on your device, rename your device, factory reset or reboot the device, force it to forget all wifi networks, force it to pair to a new bluetooth speaker/wifi point, and so on.

- What CAN'T hackers do with this?
  Assuming the Chromecast/Google Home is the only problem you have, hackers CANNOT access other devices on the network or sniff information besides WIFI points and Bluetooth devices. They also don't have access to your personal Google account, nor the Google Home's microphone. They do have access to the noise level in the room though :)

- Who are you?
  Your friendly neighbourhood @HackerGiraffe and @j3ws3r. We just want to have a bit of fun while educating and protecting people from open devices on the internet. We were also behind the #PrinterHack and #PrinterHack2.

- Why are you doing this?
  We want to help you, and also our favorite YouTubers (mostly PewDiePie). We're only trying to protect you and inform you of this before someone takes real advantage of it. Imagine the consequences of having access to the information above.

- What do you want?
  Well, fix your device first. Also subscribe to PewDiePie on YouTube! Also Pyrocynical, Dolan Dark and grandayy. Don't forget good ol' Keemstar!

- How do I fix my device?
  Disable UPnP on your router, and if you're port forwarding ports 8008/8443/8009 then STOP forwarding them.

- Thank you, any way to show support?
  Yes! I (HackerGiraffe j3ws3r has other things to do) use my free time teaching people cybersecurity and ethical hacking. If you want to support personally or or enjoyed this hack, consider becoming a Patron on my Patreon page here!

Total exposed devices: 72,341
Of those, 8,254 were renamed and 65,283 devices have been forced to play video
1,542 of the 72,341 total were Google Homes devices and the remaining 67,049 were SmartTVs/Chromecast devices.

On Reddit: "TV randomly switching to some PewDiePie video"

> Every 20 minutes or so my TV switches to some crappy YouTube video about PewDiePie with shitty rap music and a “#ChromeCastHack” hashtag. Anyone know how to stop this, it’s driving me bonkers.

Google’s Response: GraceFromGoogle / Google Community Manager - 4 days ago

> Hi everybody,
>
> We know how frightening this is. The good news is your Chromecast hasn't actually been “hacked” - rather, someone was able to cast to your Chromecast due to an opening in your home network. This is the result of your router making some smart devices, including Chromecast, publicly reachable, due to a router feature called Universal Plug and Play (UPnP).
>
> To make your network more secure, you can disable UPnP to avoid any unwanted content being played on your devices. The instructions are different from router to router, so we suggest checking with the manufacturer of your particular device. However, this may affect other apps and devices that use UPnP to function.

So, having tired of Printers, our illustrious @HackerGiraffe went looking for Chromecast devices being publicly exposed to the Internet thanks to UPnP... and, as the Google representative said, 'cast PewDiePie to them.

What Google misrepresented was to blame this on the router. As we know, UPnP (bad is it is) merely enables devices inside the network to request a static port mapping to themselves from the outside. So, yes, UPnP is and has always been a very unsafe technology, which is a drum we've been beating for quite a while. But it was also Chromecast that ASKED UPnP to please open those incoming ports for it. So this is just as much on Google as on the router and its unwitting owner.

What's more annoying is that YouTube (aside from having videos of PewDiePie), has multiple demonstrations of this and Google has reportedly been aware of this since 2013 or 2014. The Hacker News wrote: "Interestingly, Google was made aware of the Chromecast bug multiple times since 2014 shortly after the streaming device was launched and also acknowledged the hack, but the company has decided to ignore the issue."

Some of the press coverage of what to do about this was a bi flawed. Many outlets repeated the instructions of disabling UPnP and stop forwarding ports 8008, 8443 and 8009. That's fine, except that UPnP port mappings are invisible. So existing mappings cannot be seen, and disabling UPnP only prevents NEW mappings. So the solution is to disable UPnP, fully reboot the router (and while your at it, check the manufacturer's site for any firmware update (remember that in at least one reported case the router itself was unable that an update was available) and update the firmware if available.) Then after powering back up... verify that UPnP is still disabled.

And, as we know, GRC's ShieldsUP! has a very fast and dedicated UPnP exposure test that can be run anytime.

Microsoft issued an energency out-of-cycle patch for IE...
The day after our last podcast Microsoft issued an emergency out-of-cycle patch to close a 0-day vulnerability in Internet Explorer that was under active use for attacking Windows users.

The ongoing in-the-wild attack was discovered by a researcher with Google's Threat Analysis Group. The flaw is a remote code execution flaw in the IE browser's javascript engine. According to the advisory, a memory corruption vulnerability resides in the scripting engine's JScript component of IE. When exploited, the vulnerability allows attackers to execute arbitrary code in the context of the current user. And, if the current user is logged on with administrative user rights, an attacker who exploited the vulnerability could take control of an affected system, allowing them to install programs; view, change, or delete data; or create new accounts with full user rights.

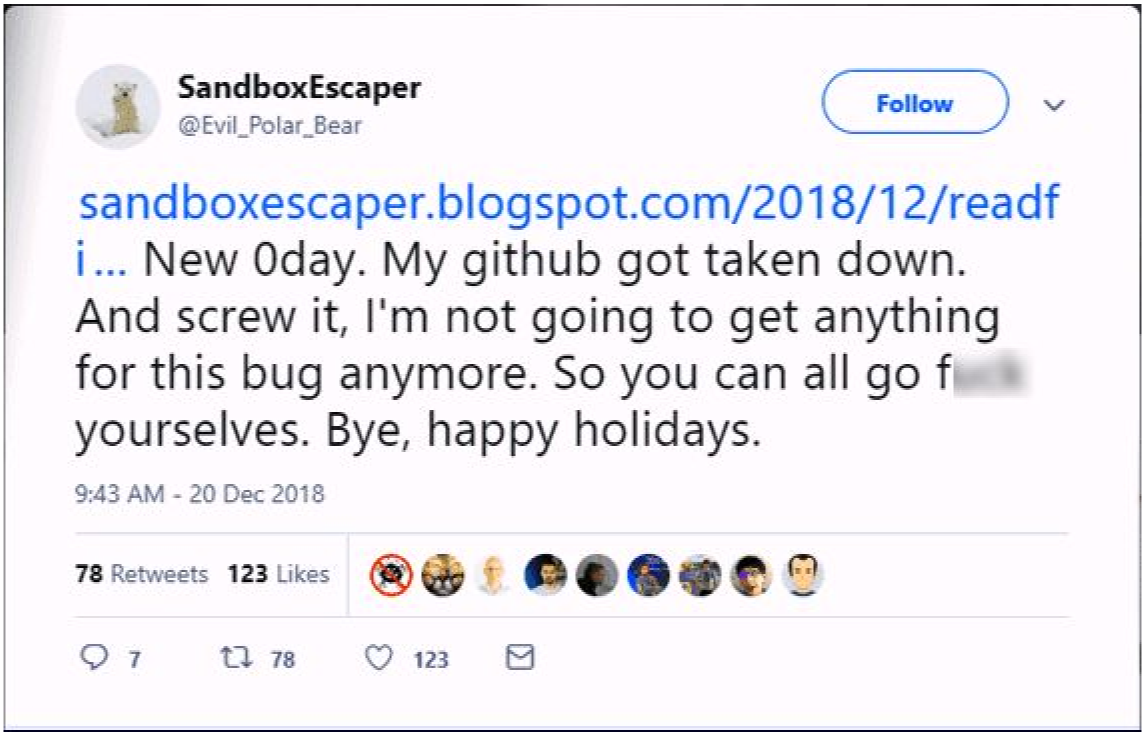
What makes this more worrisome is that, as we know, our browsers now run javascript code offered by virtually every website we visit. So just by viewing a specially-designed web page, an HTML eMail or mail attachment, an MS Office document, a PDF file, or anything else that supports embedded IE scripting engine content... the user's machine can be taken over.

The flaw exists in ALL supported versions of IE, so:
IE 9 on Windows Server 2008, IE 10 on Windows Server 2012, IE 11 from Windows 7 to Windows 10, and IE 11 on Windows Server 2019, Windows Server 2016, Windows Server 2008 R2, Windows Server 2012 R2.

Neither Google nor Microsoft has publicly disclosed details about the vulnerability, proof-of-concept exploit code, or details about the ongoing cyber attack campaign utilizing this RCE bug. But since the vulnerability is actively being exploited in the wild -- which makes it a critical zero-day flaw -- users are encouraged to install the latest updates provided by Microsoft as soon as possible.

The then... the day after this news broke...

SandboxEscaper Strikes Again...
... and she's still apparently not any happier than we've seen her in the past:



SandboxEscaper
@Evil_Polar_Bear

sandboxescaper.blogspot.com/2018/12/readfi... New 0day. My github got taken down. And screw it, I'm not going to get anything for this bug anymore. So you can all go f[redacted] yourselves. Bye, happy holidays.

9:43 AM - 20 Dec 2018

https://sandboxescaper.blogspot.com/2018/12/readfile-0day.html

A quick recap:

First, back in late August, SandboxEscaper exposed details and provided a PoC exploit for a local privilege escalation flaw in Windows Task Scheduler which was present due to errors in the handling of the Advanced Local Procedure Call (ALPC) service.

A few days after the release of that PoC, the then-0-day vulnerability was found actively being exploited in the wild. Microsoft addressed it the following month in the September 2018 Security Patch. But people were being actively hurt in the interim.

Then, last October, she released a PoC exploit for a privilege escalation vulnerability in Microsoft Data Sharing that allowed a low privileged user to delete critical system files from a targeted Windows system.

> *Leo: She appears to be a serious hiker. Check out these photos...*
> *https://sandboxescaper.blogspot.com/p/travel-photos.html*
> *And she has a really cool little single-person tent.*

So, anyway...

Two days after our previous podcast she dropped yet another 0-day. I guess that's just the way she rolls despite the pain it can cause. But this time her Twitter and Github accounts have both been suspended, so it seems that people are finally becoming a bit annoyed with this behavior. I noted that she preemptively cleaned up her 2018 blogging pages, perhaps to avoid the same thing happening to them.

So this time, also dropped onto the world via her now-suspended Twitter account, we have a unpatched (unless it's being fixed this very day) Windows 0-day arbitrary file read vulnerability that allows a low-privileged user or a malicious program to read the content of any file on a targeted Windows computer that would otherwise require admin privilege..

The 0-day resides in the "MsiAdvertiseProduct" function of Windows that’s responsible for generating <quote> "An advertise script or advertises a product to the computer and enables the installer to write to a script the registry and shortcut information used to assign or publish a product."

According to SandboxEscaper at the time of her disclosure, due to improper validation, the affected function can be abused to force the Windows installer service into making a copy of any file with SYSTEM privileges and read its content, resulting in arbitrary file read vulnerability.

She write: "Even without an enumeration vector, this is still bad news, because a lot of document software, like office, will actually keep files in static locations that contain the full path and file names of recently opened documents. Thus by reading files like this, you can get filenames of documents created by other users. The filesystem is a web of references to user-created files which can be found everywhere, so the lack of an enumeration bug is not that big of a deal."

I would agree that in this day and age, needing to know the name and location of a specific privileged file is not a huge encumbrance. There's little doubt that bad guys could put this to good use. And since it's not a big deal to fix, I expect this bug will bite the dust quickly.

Meanwhile, at the U.S. National Counterintelligence and Security Center (NCSC)...
The U.S. National Counterintelligence and Security Center (NCSC) has been distributing materials ranging from brochures to videos, to privately held companies around the United States, promoting and encouraging heightened awareness of rising cybersecurity threats from nation-state actors.

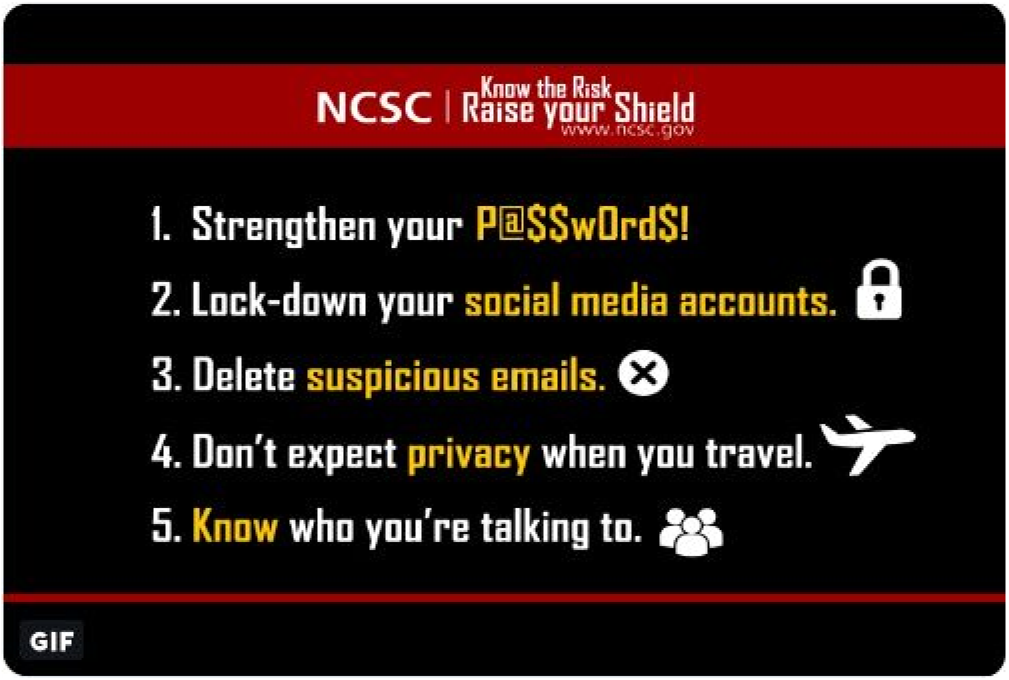
NCSC Director William Evanina wrote: "Make no mistake, American companies are squarely in the cross-hairs of well-financed nation-state actors, who are routinely breaching private sector networks, stealing proprietary data, and compromising supply chains. The attacks are persistent, aggressive, and cost our nation jobs, economic advantage, and hundreds of billions of dollars."

The campaign provides detailed info on the growing threat from foreign state hackers

NCSC is an Office of the DNI (Director of National Intelligence), designed to provide counterintelligence and security expertise in several areas, ranging from insider threat and supply chain risk management to personnel security. To push back against this growing threat, the NCSC decided to provide the U.S. private sector with information it needs to understand and defend against cyber intrusions initiated by foreign governments.

Yesterday, the NCSC Tweeted: "The National Counterintelligence and Security Center (NCSC) is today disseminating a series of videos, tips, and other materials to help U.S. industry guard against growing counterintelligence and security threats from foreign nation states and other actors. pic.twitter.com/3esqUtgqRX
— NCSC (@NCSCgov) January 7, 2019"

https://twitter.com/NCSCgov/status/1082311944030298113/photo/1



NCSC | Know the Risk Raise your Shield
www.ncsc.gov

1. Strengthen your P@$SwOrd$!
2. Lock-down your social media accounts.
3. Delete suspicious emails.
4. Don't expect privacy when you travel.
5. Know who you're talking to.

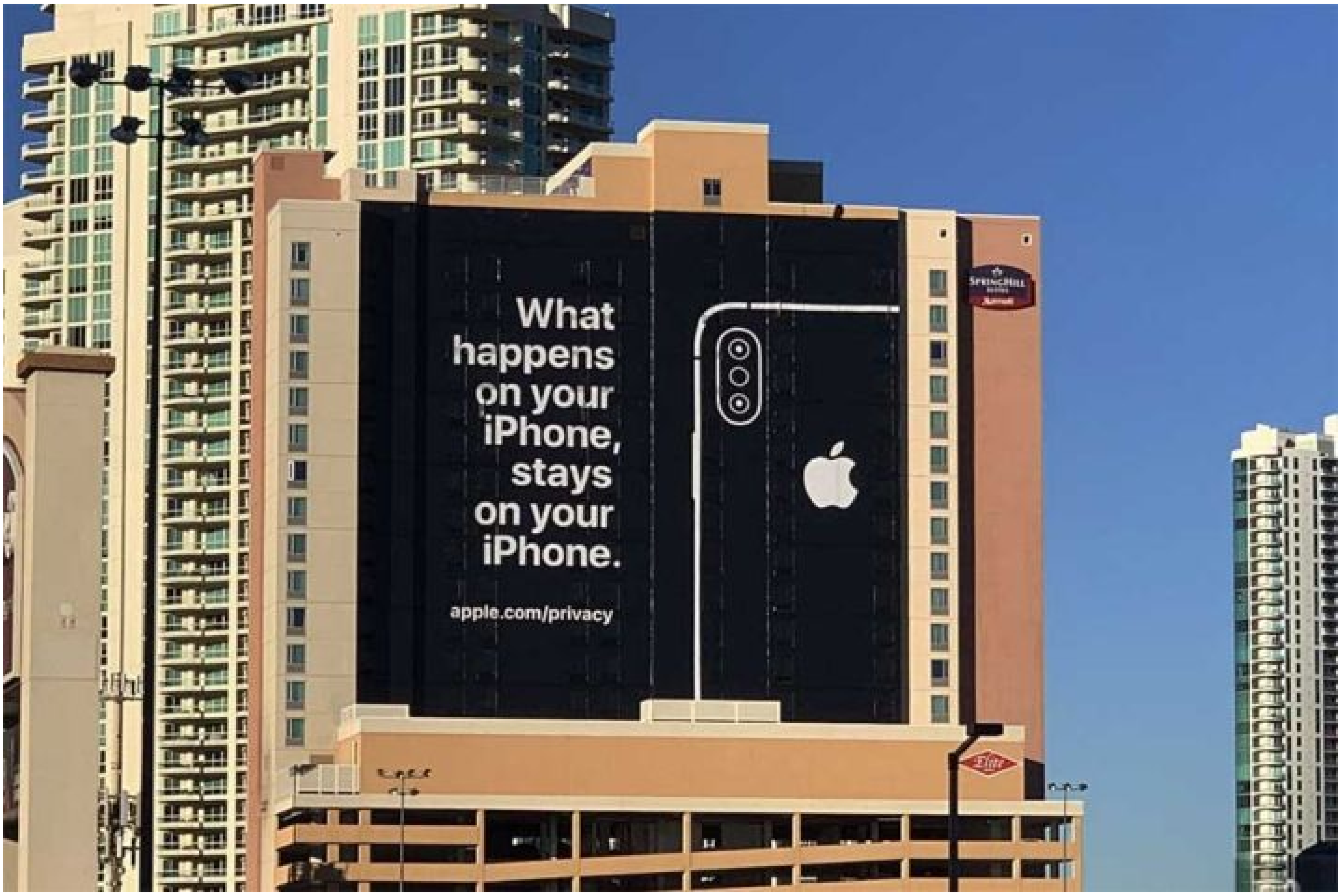
And this comes on the heels of a statement made before the US Senate Judiciary Committee last month by Bill Priestap, the Assistant Director of the FBI's Counterintelligence Division. He stated:

> *Many American businesses are just now starting to understand the new environment in which they are operating. The continued proliferation of cyber hacking tools and human intelligence capabilities means that this environment will only become more hostile and more treacherous for our companies. Our businesses face competitors in the form of aforeign enterprises assisted or directed by extremely capable intelligence and security services.*

The materials distributed by the NCSC to raise awareness among private sector companies are part of a campaign dubbed "Know the Risk, Raise Your Shield." The materials being disseminated by the NCSC cover a range of subjects, from supply chain risks, spear-phishing, and social engineering, to economic espionage, social media deception, foreign travel risks, and mobile device safety.

For those who are not already on their toes, this would be a useful wake up call... if the attention that's due this warning gets paid.

As we know, Apple no longer attends the industry's annual Consumer Electronics Show (CES), normally held in Las Vegas, because they are large enough to create their own shows....



But this year, while still absent, Apple decided to have some fun with the famous “What happens in Vegas stays in Vegas” slogan… at the expense of their less-privacy-enforcing consumer competitors, Amazon and Google, who both, in the past year, suffered from some embarrassing privacy slips.

So… a huge black & white, building-size graphic, facing the Las Vegas convention center, shows the distinctive black and white outline of the iPhone with the slogan “What happens on your iPhone stays on your iPhone.” … with apple.com/privacy at the bottom.

There’s a tiny and somewhat ironic aspect to this which those in the tech press have noted: The huge building-size graphic appears on the side of a Marriott Hotel, which, as we know, also suffered from its own embarrassing years-old data breach which we learned of late last year.

When your of your system’s files have been encrypted…
... all may not be lost.

We recently -- it may have been the last podcast of 2018 -- ran through some of the many variations of randsomware that had been derived from a single poorly written starter on Github, and the fact that someone named Michael Gillespie was creating various decryptors for its ransomware descendents.

Since then, Bleeping Computer, which closely follows and reports on this ransomware universe has been following Michael's subsequent developments.

On January 2nd, Lawrence Abrams posted "How to Decrypt the FilesLocker Ransomware with FilesLockerDecrypter. Although Michael Gillespie did produce a decryptor for this ransomware, in this instance he was aided by the fact that on December 29th, an unknown user released the master RSA decryption key for FilesLocker v1 and v2.

Two days later, on January 4th, Lawrence Abrams posted "How to Decrypt the Aurora Ransomware with AuroraDecrypter" and provided a complete walkthrough of the use of Michael's decryptor for the Aurora ransomware.

And then, doing a bit more digging and catching up on everything that had happened since our last podcast three weeks ago, I discovered an article that Lawrence had posted on Thursday the 20th:

"BleepingComputer.com Is Now a Partner With No More Ransom!"

BleepingComputer is humbled and honored to announce that we have joined the "No More Ransom" project as an associate partner! We have been providing ransomware information, support, and the amazing decryptors from Michael Gillespie since the beginning and this partnership will enable more victims to receive the help they need.

No More Ransom project is a joint project created by Europol, Politie, and McAfeee to provide information and assistance to those affected by Ransomware. Since its creation, numerous other law enforcement agencies, security companies, and supporters have joined the project, which now supports 35 different languages with over 59 free decryption tools for 91 ransomware families.

https://www.nomoreransom.org/
https://www.nomoreransom.org/en/decryption-tools.html

This is very very cool. But remember that decryption tools ONLY WORK on poorly implemented ransomware crypto. If the crypto is done right, and eventually it will be, there will be no way to decrypt a system's files without access to information that only the the evildoer has.

Windows Sandbox -- now for Win10 Pro, too!

Last August we covered the mixed-blessing news that Microsoft would was introducing something they were calling at the time "InPrivate Desktop." Their description read:

InPrivate Desktop (Preview) provides admins a way to launch a throwaway sandbox for secure, one-time execution of untrusted software. This is basically an in-box, speedy VM that is recycled when you close the app!

Prerequisites:

- Windows 10 Enterprise
- Builds 17718+
- Branch: Any
- Hypervisor capabilities enabled in BIOS
- At least 4GB of RAM
- At least 5GB free disk space
- At least 2 CPU cores

This was very cool. The idea of having an easy-to-use, readily accessible, throwaway VM for safely doing stuff. But, of course, it was also disappointing because... who among us has Win10 Enterprise? But... we're discussing this again because shortly before Christmas, Santa Microsoft left news of a welcome present under our Windows 10 tree...

https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/Windows-Sandbox/ba-p/301849

Microsoft's Hari Pulapaka posted:

Windows Sandbox is a new lightweight desktop environment tailored for safely running applications in isolation.

How many times have you downloaded an executable file, but were afraid to run it? Have you ever been in a situation which required a clean installation of Windows, but didn't want to set up a virtual machine?

At Microsoft we regularly encounter these situations, so we developed Windows Sandbox: an isolated, temporary, desktop environment where you can run untrusted software without the fear of lasting impact to your PC. Any software installed in Windows Sandbox stays only in the sandbox and cannot affect your host. Once Windows Sandbox is closed, all the software with all its files and state are permanently deleted.

Windows Sandbox has the following properties:

- Part of Windows – everything required for this feature ships with Windows 10 Pro and Enterprise. No need to download a VHD!
- Pristine – every time Windows Sandbox runs, it’s as clean as a brand-new installation of Windows
- Disposable – nothing persists on the device; everything is discarded after you close the application
- Secure – uses hardware-based virtualization for kernel isolation, which relies on the Microsoft’s hypervisor to run a separate kernel which isolates Windows Sandbox from the host
- Efficient – uses integrated kernel scheduler, smart memory management, and virtual GPU

Prerequisites for using the feature

- Windows 10 Pro or Enterprise Insider build 18305 or later
- AMD64 architecture
- Virtualization capabilities enabled in BIOS
- At least 4GB of RAM (8GB recommended)
- At least 1 GB of free disk space (SSD recommended)
- At least 2 CPU cores (4 cores with hyperthreading recommended)

So the EXTREMELY good news is that Windows 10 Pro will soon have this feature. It is currently shipping in the Fast Ring of 18305 which is AKA 19H1. To add Windows Sandbox to your machine, go to Settings > Apps > Apps & Features > Programs and Features > Turn Windows Features on or off, and then select Enable Windows Sandbox.

A new Page Cache Side-Channel Attack

Just as the podcast was being assembled came the news of another side-channel attack. I scanned it quickly and it didn't look like the end of the world, but I'm sure I'll more to say about it next week. So... stay tuned!

SpinRite

GRC / Spinrite testimonial

Steve,

We'd swapped e-mails a few years ago but today I write with my profound thanks for your Spinrite creation.

Recently I'd been transferring all my Patent work, and other high-value documents & settings to an older Acer laptop with Ubuntu OS which I use as a dedicated, secure work station.

During this massive, multi-platform undertaking, an OS update came thru and after re-starting, the Linux system was completely locked up: few files would even open, and no system operation would execute. It wouldn't even shut down!

I envisioned hours of reconstructing files from other backups (if even possible)...a massive headache with profound monetary implications if unsuccessful.

I decided to run my years old copy of Spinrite (5.0) on it, just to reassure that the bits would be readable with my adapter transfer hardware during the laborious HDD swap-and-read attempts.

Finished after 12 hours of plodding along, I decided to reboot the Acer just to see if anything would even function, then lo and behold, it was "all systems go!" files recovered and system operations normal.

The English language is inadequate to express my relief, and further: in today's techno-centered, disposable world, it is nearly impossible to find any product that actually does what it says it will, and at a fraction of the cost compared to the alternative, but Spinrite is one that delivers.

My eternal Thanks, Steve.
Dunbar Pappy

SQRL Update

The SSPAPI work is finished https://www.grc.com/sqrl/sspapi.htm
My code is Windows x86 MASM, so I built a Win10 VM
A talented Danish XenForo developer is
LETHAL Meets January 27th

Miscellany

Filemail
https://www.filemail.com / Oslo Norway. Free for files up to 50 GB.
$15/month offers many additional features.
SCREAMING fast. Saturated my cable modem's upstream bandwidth.