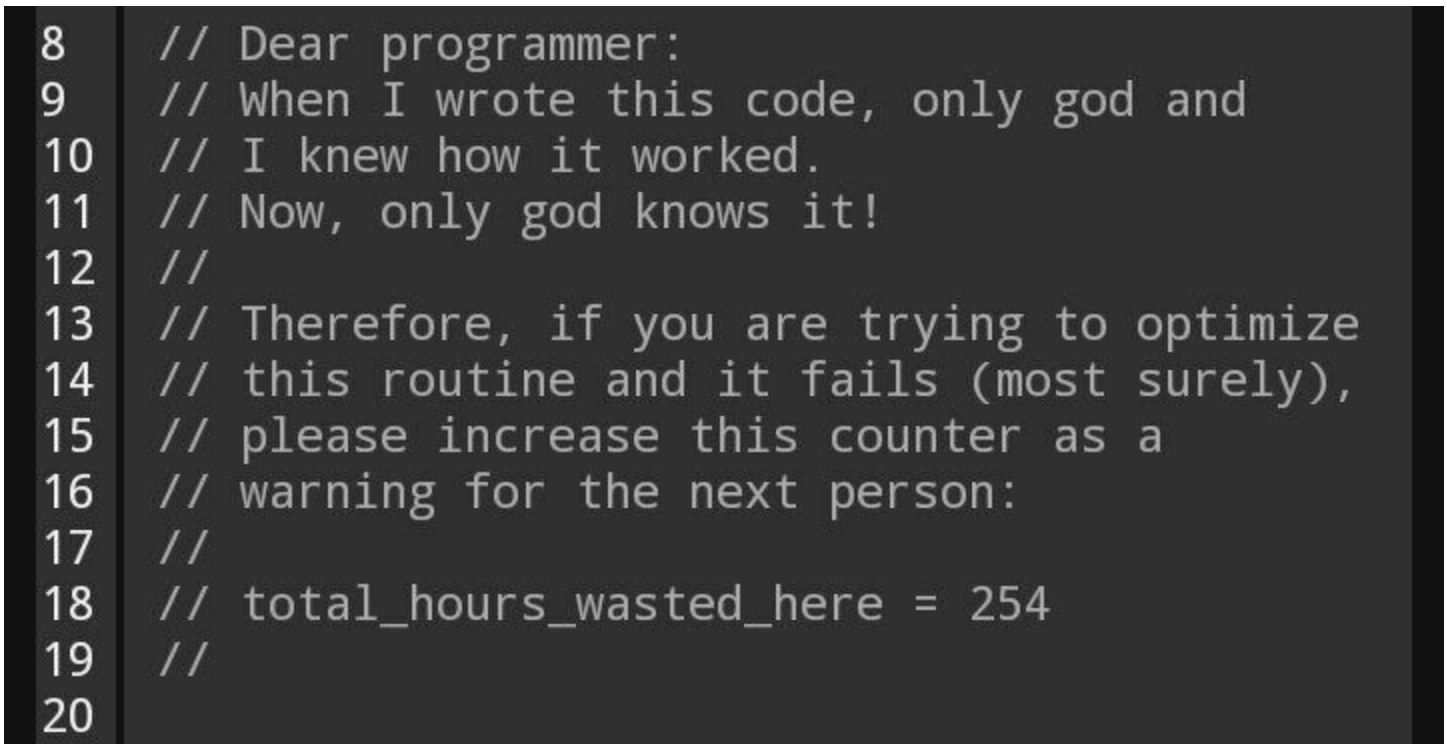
# Security Now! #743 - 12-03-19

# Android “StrandHogg”

## This week on Security Now!

This week we revisit free upgrades from Win7 or 8 to 10 (which can still be done, a alert for users of HP SSDs, the complications that arise with international privacy treaties when end-to-end encryption might be threatened, the US government's formal permission to hack, a quick look at a particularly devastating Ransomware attack, more anti-tracking privacy happiness coming soon, by default, to Firefox, the never-ending headaches caused by Windows DLLs, an update on my "Joy of Sync" determinations, and a look at the way some Android multitasking features can and are being actively abused -- with Google's knowledge.



# Security News

**Everyone can still upgrade to Windows 10**
https://www.microsoft.com/en-us/software-download/windows10 --or→

## https://grc.sc/win10

As we know, the official end of Microsoft's free Windows 10 upgrade occurred on July 29th, 2016. Later, there was a somewhat sketchy solution that was spotted, and which we told our listeners about, involving something mildly unsettling. I don't recall what it was exactly, but it was something like an extended Win10 upgrade period for disabled or special needs users... or something of that sort.

It was never clear to me why the upgrade was time-limited in the first place, since Windows 10 is now, god help us, "the OS as a service" model and we're having to pay a heavy toll by tolerating all of the crapware, monitoring and "monetization opportunities" Microsoft bragged to their shareholders about back in Win10's early days. And those opportunities have presumably come to pass (and are a large part of the reason why many people have elected to remain pre-Win10.)

Presumably, the deadline had the intent and goal of motivating recalcitrant users to bite the bullet, see the light -- or at least stop holding back -- and make the move. However, as it turns out, there is still an off the beaten path clean, simple and fully sanctioned "Download Windows 10" page offering to download an in-place upgrade tool:

https://www.microsoft.com/en-us/software-download/windows10 -or- https://grc.sc/win10

> Create Windows 10 installation media
>
> To get started, you will first need to have a license to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.

This "Media Creation Tool" can be run on an already-licensed copy of Win7/8/8.1 to either wipe and replace the existing Windows OS, or -- probably more useful -- to perform an in-place upgrade which will preserve all installed apps and user files.

After the upgrade you'll need an Internet connection to obtain a permanent activation license, but once that's done you'll be saddled with Windows 10 for the rest of time. I mean... You'll be able to experience for awe, wonder and joy that awaits all Win10 users.

What's a bit off-putting is that the Microsoft page clearly states that the upgrade must be purchased. But Bleeping Computer's coverage of this "Windows 10 Download" page is very clear that the upgrade is, in fact, free:
https://www.bleepingcomputer.com/news/microsoft/you-can-still-upgrade-to-windows-10-for-free-heres-how/

That Bleeping Computer page refers to a Reddit thread where others have successfully applied the upgrade without trouble.  So I read down into the thread to see whether I could learn more.

That eventually brought me to a page at "answers.microsoft.com" titled: "How you can still get Windows 10 for free ":  (115,800 views)
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install-winpc/how-you-can-still-get-windows-10-for-free/2159c2a7-a925-4fa3-9a03-08a5e1ecf891?auth=1

**Summary**
Windows 10 was released with a free upgrade offer that lasted for 1 year. Now, the free upgrade promotional period is officially over. However, you can still snag yourself a free license of Windows 10, perfectly legally, if you know how.

On that Microsoft page there was also a note about the "Assistive Technologies" upgrade offer, which, I'm sure, is what we recall from before… but this, it turns out, is not that. In the interim, Microsoft appears to have quietly loosened the restraints on upgrading to Win10.

And ZDNet carried the story and updated their coverage of it as of three months ago, saying:
https://www.zdnet.com/article/heres-how-you-can-still-get-a-free-windows-10-upgrade/

**Updated 20-Sep-2019:** Thank you to the many readers who have continued to provide firsthand reports that this procedure still works. The overwhelming majority of reader reports confirm that this upgrade is still available. A small number of readers have reported that the upgrade fails because of a Setup error or a compatibility block. For details on how to troubleshoot these errors, see "This free Windows 10 upgrade offer still works. Here's why - and how to get it."

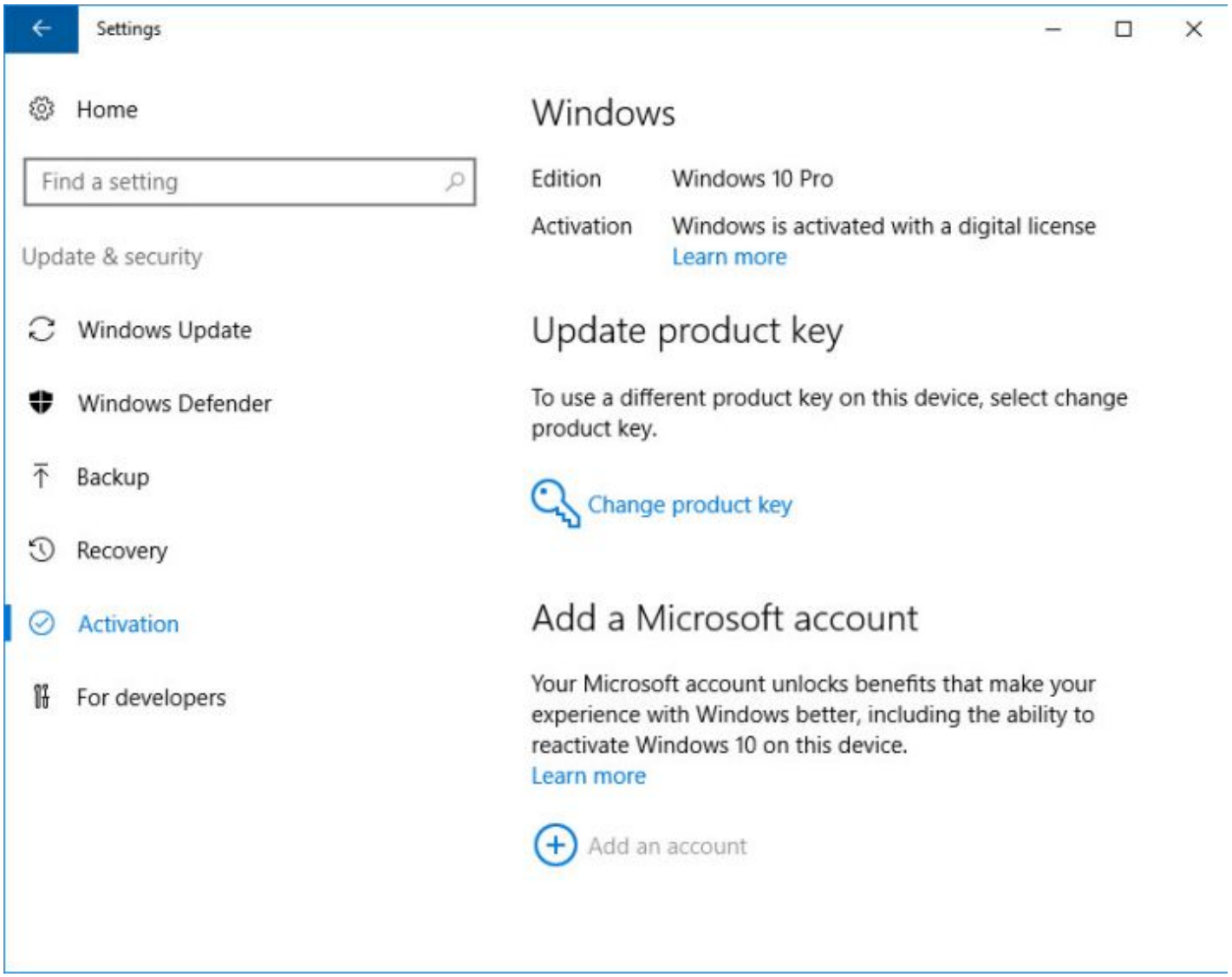
Ed Bott, who certainly knows his way around the subject wrote of this, this past April. He said:

In early 2017, I recycled an Intel small-form-factor PC that had previously been working full-time in the living room, running Windows Media Center on Windows 7 Ultimate. When I finally pulled the plug on Media Center after the release of Windows 10, I had put this little device on a shelf.

The GWX utility had never been installed on this PC and it had never been offered a Windows 10 upgrade via Windows Update.

As part of my digital clean-up, I decided to run the Windows 10 upgrade from Windows 7. I fully expected that after the upgrade was complete, the system would fail activation and I'd be asked for a product key.

Imagine my surprise when, instead, I was greeted with this screen:




I confirmed the same sequence on two different virtual machines, both created from scratch and running clean, fully activated installs of Windows 7 and Windows 8.1, respectively. I repeated those steps on test PCs at least monthly since the release of the Creators Update in April 2017 and the Fall Creators Update in October 2017, and as of mid-September 2019 I continue to receive confirmation from people who've seen the same results on their home or office PCs.

If you have a PC running a "genuine" copy of Windows 7/8/8.1 (Home or Pro edition, properly licensed and activated), you can follow the same steps I did to upgrade it to Windows 10.

To get started, go to the Download Windows 10 webpage and click the **Download tool now** button. After the download completes, run the Media Creation Tool.

If you've downloaded the Media Creation Tool on the machine you plan to upgrade, and you plan to upgrade one and only one PC, you can choose the **Upgrade this PC now** option and be done with it.

Then just follow the prompts to complete the upgrade. You will not be asked for a product key, and when the upgrade is complete and you've connected to the Internet, you'll have a digital license to Windows 10, which you can confirm by going to Settings > Update & Security >

Activation.

The digital license is associated with that specific device, which means you can reformat the disk and perform a clean installation of the same edition of Windows 10 anytime. You won't need a product key, and activation is automatic.

**Counting down to 32768 hours...**
Due to a mistake in the firmware running a large set of Hewlett-Packard SSDs, the instant the total powered-on running time crosses 32,768 hours (also known as 3 years, 270 days, and 8 hours) the drive will totally and unrecoverably fail, taking all of its stored data with it. Whoopsie.

https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00092491en_us

SUPPORT COMMUNICATION - CUSTOMER BULLETIN
Version: 2
Bulletin: HPE SAS Solid State Drives - Critical Firmware Upgrade Required for Certain HPE SAS Solid State Drive Models to Prevent Drive Failure at 32,768 Hours of Operation.

**IMPORTANT**: This HPD8 firmware is considered a critical fix and is required to address the issue detailed below. HPE strongly recommends immediate application of this critical fix. Neglecting to update to SSD Firmware Version HPD8 will result in drive failure and data loss at 32,768 hours of operation and require restoration of data from backup in non-fault tolerance, such as RAID 0 and in fault tolerance RAID mode if more drives fail than what is supported by the fault tolerance RAID mode logical drive. By disregarding this notification and not performing the recommended resolution, the customer accepts the risk of incurring future related errors.

HPE was notified by a Solid State Drive (SSD) manufacturer of a firmware defect affecting certain SAS SSD models (reference the table below) used in a number of HPE server and storage products (i.e., HPE ProLiant, Synergy, Apollo, D3000/D6000/D6020 disk enclosures, MSA Storage, StoreEasy 1000 Storage, StoreVirtual 4335 Hybrid Storage and StoreVirtual 3000 Storage are affected).

**NOTE**: The following platforms are **NOT AFFECTED** by this issue: HPE 3PAR StoreServ Storage, D8000 Disk Enclosure, Nimble Storage, Primera Storage, StoreOnce Systems, XP Storage and SimpliVity.

The issue affects SSDs with an HPE firmware version prior to HPD8 that results in SSD failure at 32,768 hours of operation (i.e., 3 years, 270 days 8 hours). After the SSD failure occurs, neither the SSD nor the data can be recovered. In addition, SSDs which were put into service at the same time will likely fail nearly simultaneously.

Their disclose contains a list of 20 SSD model numbers. So anyone who may be using any of these drives will definitely want to track this down and get their drive firmware updated!

**RESOLUTION**
Immediately upgrade the drive firmware to version HPD8, which HPE has released to prevent the issue described above. Links for Windows, Linux and VMWare ESXi are provided.

**The EU is not happy about a possible US encryption ban**
The ongoing battle over end-to-end encryption took another turn last week, when EU officials warned that they may not take kindly to a US encryption ban or insertion of crypto backdoor technology.

So... back in June of this year, senior US government officials quietly met to discuss whether they could legislate tech companies into not using unbreakable encryption. According to Politico, the National Security Council pondered whether to ask Congress to outlaw end-to-end encryption.

US officials did not reach a decision on the issue, but news of the conversation spooked some enough to ask the European Commission some formal questions which were picked up by Glyn Moody over at Techdirt. Körner asked whether the Commission would consider a similar ban on encryption in the EU. He also asked what a US ban would mean for existing data exchange agreements between the EU and the US:

Would a ban on encryption in the USA render data transfers to the US illegal in light of the requirement of the EU GDPR for built-in data protection?

At the moment the two regions enjoy an agreement known as the EU-US Privacy Shield, which they introduced after the European Court of Justice invalidated a previous agreement called the International Safe Harbor Privacy Principles.

Today's Privacy Shield is a voluntary certification scheme for US businesses. By certifying under the scheme, US companies prove their adequacy to transfer and process data on EU citizens. It shows that they have made some effort to follow Europe’s strict privacy principles in the absence of any cohesive federal privacy law in the US.

On 20 November, European Commission officials replied with their answers, confirming that they would not consider a ban on encryption in the region and pointing out that the General Data Protection Regulation (GDPR) explicitly refers to encryption as a privacy protection measure.

However, the answer to the next question was a bit more contentious:

If the U.S. were to enact new legislation in this area, the Commission will carefully assess its impact on the adequacy finding for the EU-U.S. Privacy Shield, a framework which the Commission has found to provide a level of data protection that is essentially equivalent to the level of the protection in the EU, thus allowing for the transfer of personal data from the EU to participating companies in the U.S. without any further restrictions.

So the jury is out on how the EU would react to cross-Atlantic data transfers if the US implemented crypto backdoors.

Attorney Ashley Winton, with McDermott Will & Emery, a UK-based specialist in data privacy law, explained that a split between the two territories on data exchange could have serious consequences. He said:

We know that under the GDPR personal data must be held securely, so legislating against strong encryption or introducing legal back doors is not going to be good for the safe passage of European Personal Data – howsoever it gets there.

Unlike the annual review of Privacy Shield, in theory, if the European Court were to determine that the transfer of Personal Data into the US was no longer safe, all affected transfers could be halted immediately. The fact that a world of data protection compliance pain would ensue suggests that saner heads will somehow manage to prevail.

However, the EU's somewhat reasonable position about the possibilities of a ban on encryption are in stark contrast to the UK's approach.

The Investigatory Powers Act of 2016 compels communication providers to let the government know in advance of any new encryption products and services, allowing it to request technical assistance in overcoming them. Last month, the UK and the US signed an agreement under the March 2018 CLOUD Act allowing each other to demand electronic data directly from tech companies based in the other country, without legal barriers.

The attorney, Ashley Winton, said that another soon-to-be decided case will once again bring the issue of data transfer from the EU to the US into the spotlight. This December 12th, (Thursday after next), the European Court of Justice (ECJ) will decide on a case known as Schrems 2. This is a legal challenge against Facebook in Ireland by Austrian Attorney and privacy advocate Max Schrems.

Schrems was responsible for bringing down the original Safe Harbour agreement. He has grown concerned by Facebook's cooperation with the US intelligence services as revealed by Edward Snowden. So he filed a complaint with the Irish Data Protection Commissioner complaining that the transfer of his personal data to Facebook in the US violated his rights. The European Court of Justice ruled in his favour.

Schrems 2 focuses on another mechanism used to transfer data from the EU to the US: standard contractual clauses (SCCs). SCCs are bilateral agreements between EU and US organizations based on standard templates which are frequently used by companies in countries that don't have any other formal agreement in place. SCCs are important because they are the mechanism used for extraterritorial data transfers among 88% of respondents.

I wanted to share all of this to highlight just how much remains up in the air, how much we are still unsure what's destined to happen, and how this is not just a local domestic issue, but that it directly affects our various neighbors with whom we covering data exchange agreements. While we're just happily clicking links, there are courts mulling over exactly what protections their extra-territorial neighbors should be required to commit to.

So the whole issue of end-to-end encryption -- or not -- is not only of local moment.

**Under the heading of "This should be interesting"**
The Cybersecurity and Infrastructure Agency (CISA), which is part of the Department of Homeland Security, has just published a Vulnerability Directive Policy (VDP) requiring executive branch federal agencies to be welcoming and responsive to cybersecurity bug reports from the general public.

Titled: Improving Vulnerability Disclosure Together
https://www.cisa.gov/blog/2019/11/27/improving-vulnerability-disclosure-together

A VDP directive and you

Today, we are issuing a draft binding operational directive, BOD 20-01, which will require federal civilian executive branch agencies to publish a vulnerability disclosure policy (VDP). A VDP allows people who have "seen something" to "say something" to those who can fix it. It makes clear that an agency welcomes and authorizes good faith security research on specific, internet-accessible systems.

In preparing this directive, we've worked with several agencies that have VDPs and made an effort to align the directive with federal guidance, international standards, and good practices. But this directive is slightly different from others we've issued, where agencies are directed to take an action and then CISA verifies the action has taken place. Here, while agencies must maintain VDPs and are the beneficiaries of vulnerability reports, it's the public that will provide those reports and will be the true beneficiaries of vulnerability remediation. That's why we're doing something we've never done before with our directives: seeking public feedback before issuance.

We want to hear from people with personal or institutional expertise in vulnerability disclosure. We also want to hear from organizations that have a VDP and manage coordinated vulnerability disclosures.

In seeking public comment, we're also nodding to the fact that, to our knowledge, a requirement for individual enterprises to maintain a vulnerability disclosure policy has never been done before, and certainly not on this scale.

What does the draft directive do?

- Lights a fire. Each agency must publish a VDP and maintain handling procedures, and the directive outlines a set of required elements for both.
- Draws a line in the sand. Systems "born" after publication of a VDP must be included in scope of an agency's VDP.
- Expands the circle. Until everything is included, at least one new system or service must be added every 90 days to the scope of an agency's VDP.
- Starts the clock. There's an upper bound – 2 years from issuance, in this draft – for when all internet-accessible systems must be in scope.
- All are welcome. Anyone that finds a problem must be able to report it to an agency.
- No "catch and keep". An agency may only request a reasonably time-limited restriction against outside disclosure to comply with their VDP.

- Defense, not offense. Submissions are for defensive purposes; they don't go to the Vulnerabilities Equities Process.

What doesn't it do?

- Does not establish a "federal bug bounty". A bug bounty is a program that pays researchers for valid and impactful findings. Nothing in the directive prevents individual agencies from establishing a bug bounty of their own, though.
- Does not create a "national VDP". The directive is an executive branch policy instruction that requires federal civilian executive branch agencies to have a VDP. The difference might appear slight but they're very different things.

Why isn't this a national VDP?

We think a single, universal vulnerability disclosure policy for the executive branch is a good goal. It makes sense particularly when each agency has all internet-accessible systems in scope, but we expect that goal to be an unrealistic starting place for most agencies. Instead, the directive supports a phased approach to widening scope, allowing each enterprise – comprised of the humans and their organizational tools, norms, and culture – to level up incrementally.

Doing good things together

We believe that if you make good things easier to do, more people will do them. With this directive, we want to take steps that diminish complexity and make expectations plain. In support of that, we're also sharing draft implementation guidance on the directive, as well as a draft VDP template.

We welcome your feedback and perspective on all these documents, as well as any comments on our approach. The public comment will take place on GitHub and last until December 27th, 11:59pm EST.

https://cyber.dhs.gov/assets/report/bod-20-01-vdp-template.docx
https://cyber.dhs.gov/bod/20-01/

**Ransomware impacts a healthcare Managed Service Provider with devastating effect.** About 110 nursing homes -- think about that, 110 -- and acute-care facilities have been crippled by a ransomware attack on their common shared IT provider, Virtual Care Provider Inc. (VCPI), based in Wisconsin. VCPI provides data management and records hosting, security and access management to nursing homes across the country.

When Brian Krebs first reported the attack last Monday the attack was still underway.

Krebs said that it involves our old friend Ryuk... And, as we know, the hackers who are driving Ryuk are known to calculate how much ransom victimized organizations can pay based on their size and perceived value.

But we've seen instances where the crooks get it wrong, as appears to again be the case here. VCPI's chief executive and owner Karen Christianson told Brian that her company simply cannot afford to pay the $14 million Bitcoin ransom that the attackers are demanding. As it is, VCPI's own employees have been asking when THEY'LL be getting paid, but the top priority is to wrestle back access to the lost electronic medical records.

The attack successfully affected all of the firm's core offerings: internet service, email, access to patient records, client billing and phone systems, and even the internal payroll operations that VCPI uses to pay its own workforce of nearly 150. Regaining access to electronic health records (EHR) is the top priority because without that access, the lives of the seniors and others who reside in critical-care facilities are at stake.

Christianson said: "We have some facilities where the nurses can't get the drugs updated and the order put in so the drugs can arrive on time. In another example we have an assisted living facility that is just a single unit that connects to billing. If they don't get their billing into Medicaid by December 5, they close their doors. It's over, and seniors who have no family to go to are then suddenly homeless." Karen added, "We have many clients right now who are demanding 'Just give me my data' ... but we can't."

Imagine how devastated she must be. A report from Vanderbilt University's Owen Graduate School of Management noted that the corrective actions being taken to harden and secure facilities and systems can, at least temporarily, worsen the problem. Hey wrote:

"Corrective actions are intended to remedy the deficiencies in privacy and security of protected health information. However, enhanced security measures may introduce usability – which we define as the ease of use – problems. New security procedures typically alter how clinicians access and use clinical information in health information systems and may disrupt the provision of care as providers require additional time to learn and use the new or modified systems."

In other words, yeah, no kidding. Layers of security can be annoying. But they can prevent this.

The Ryuk group behind Ryuk are serious. In a similar recent attack Ryuk took about another service provider affecting hundreds of veterinary hospitals.

In this attack, Brian Krebs reported that Ryuk was unleashed inside VCPI's networks around 1:30 a.m. CT on 17 November. It could have been lying in wait for some time as the intruders mapped out the internal networks, compromised resources and data backup systems in preparation for the ultimate attack.

Christianson said that VCPI will publicly document the attack – "When (and if)" it's brought under control. For now, it's focusing on rebuilding systems and informing clients, even in the face of the data kidnappers having seized control of the firm's phone systems at one point, when it tried to sidestep their damage. She pledged:

"We're going to make it part of our strategy to share everything we're going through. But we're still under attack, and as soon as we can open, we're going to document everything."

**Firefox is seriously pushing back on tracking signal leakage**
As we know, Cookies are only the most obvious, sanctioned and more easily controllable aspect of web browser based Internet tracking. Browser and user "fingerprinting" makes use of the many subtle signals a browser may send in an attempt to lock onto a user who is deliberately attempting to thwart cookie-based tracking.

I'm sitting in front of a very wide 3840x1600 screen right now and my browser IS, indeed, set to some smaller useful width on the screen. JavaScript running in an advertiser's ad is allowed to query the browser's location and its window size. So I'm sending back some information that, while it doesn't identify me directly, definitely narrows the possibilities.

When many such soft signals are merged and combined, who we are is narrowed down into a much smaller universe of possibilities. Things such as whether we have an external monitor plugged in; which fonts we have installed; how much battery power we have left; which specific OS and browser we're using; what timezone we're in; the exact pixel layout your browser chooses when rendering characters; and so on. Unfortunately, over the years gung-ho web app advocates have moved to give JavaScript access to everything imaginable.

And many of these features, no matter how useful they seemed at the time, have primarily been used for evil, not for good. The "navigator.getBattery()" function allows advertising script to track the precise battery state of our computers, a data value that tends to change predictably over time. We've talked about this before and imagined some way for web sites to use this information for their visitor's benefit. Sure, it's possible... But it's mostly used as another tracking indicator.

So, that's the terrain.  The welcome news is that Firefox has been vocal about the anti-fingerprinting code they've been building for a future release. It plans to deeply obscure many of these signals by doing things such as:

- Canvas image extraction is blocked.
- Absolute screen coordinates are obscured.
- Window dimensions are rounded to a multiple of 200×100.
- Only specific system fonts are allowed.
- Time precision is reduced to 100ms, with up to 100ms of jitter.
- The keyboard layout is spoofed.
- The locale is spoofed to 'en-US'.
- The date input field and date picker panel are spoofed to 'en-US'.
- Timezone is spoofed to 'UTC'.
- All device sensors are disabled.

The downside of all this, of course, is that any websites that make legitimate and positive use of these details – for example to improve the accessibility of the site or boost the performance and playability of online games – are out of luck. The upside is that every browser detail that gets "de-precisioned" is a setback for the Bad Guys, and thus a privacy win for the rest of us.

For those reasons, Firefox's latest fingerprinter blocking tools are easy to turn on, but they are not yet enabled by default in case obfuscating browser signals to prevent tracking might have a negative consequence that hasn't yet surfaced.

But the default will be changing soon. We're currently at Firefox v70 and Mozilla has stated that they are planning to enable their fingerprinter blocking two major versions from now, with release 72.

**Meanwhile... new problems with Windows DLLs**

Some ideas in computer science are fundamentally fraught with problems. An example would be the oh-so-convenient, though horrifically insecure, practice of allocating temporary communications buffers on a stack that is shared with code execution history and pointers. What could possibly go wrong?

Another historically bad idea has been Windows Dynamically Linked Libraries (DLLs). Windows designers had their hearts in the right place. Back in the 1980's, when Windows was attempting to run in a system with a 10 megabyte drive and 512 kbytes of RAM, there was not a single byte to waste. So there was tremendous pressure to share any common functional code among the system's components and applications. The idea of the DLL was clever in that not only could there be only one copy of the DLL stored on the hard drive, but only one copy would ever be physically loaded into physical memory. When another program wished to use some of the functions from one of the shareable DLLs, the image of an already loaded instance of that DLL would be "mapped" into the virtual memory space of the requesting app by the Windows loader. This allowed much more to be accomplished within a small disk and RAM footprint.

But this technology did not age well. Over time there was a divergence of DLL versions and capabilities. DLLs could use other DLLs, and that created a confusing network of inter-DLL dependencies. Such a mess arose that Microsoft was finally forced to step in and attempt to fix it. Quoting from the Wikipedia entry on what's known as Side-By-Side Assembly:

"Side-by-side assembly (SxS, or WinSxS on Microsoft Windows) technology is a standard for executable files in Windows 98 Second Edition, Windows 2000, and later versions of Windows that attempts to alleviate problems (collectively known as "DLL Hell") that arise from the use of dynamic-link libraries (DLLs) in Microsoft Windows. Such problems include version conflicts, missing DLLs, duplicate DLLs, and incorrect or missing registration. In side-by-side, Windows stores multiple versions of a DLL in the WinSxS subdirectory of the Windows directory, and loads them on demand. This reduces dependency problems for applications that include a side-by-side manifest.

Microsoft Visual C++ 2005 and 2008 employ SxS with all C runtime libraries. However, runtime libraries in Visual C++ 2010 no longer use this technology; instead, they include the version number of a DLL in its file name, which means that different versions of one DLL will technically be completely different DLLs now.

What an utter catastrophe. But as I said, Microsoft's designers were doing what they needed to at the time. If anything, with the unfair benefit of 20/20 hindsight, Microsoft might now be criticized for not completely killing-off DLLs a long time ago. But one thing that Microsoft has always provided, unlike, for example Apple that does choose to kill-off their mistakes and then weather the inevitable criticism, is very very strong backward compatibility as they have evolved Windows through the decades.

So this brings us to today, or rather yesterday, when researchers with SafeBreach Labs published a trio of security advisories which described DLL-related bugs occurring in Autodesk, Trend Micro, and Kaspersky software. All of the problems were responsibly reported to their respective software publishers before their public disclosure.

The first vulnerability, tracked as CVE-2019-15628, impacts all versions of Trend Micro Maximum Security below v16.0.1221. One of that system's components runs as a service with maximum NT AUTHORITY\SYSTEM permission. The researchers found that that service "coreServiceShell.exe" loads a DLL: paCoreProductAdaptor.dll. However, a missing DLL, lack of safe DLL loading and lack of DLL signature validation would allow attackers to exploit this as a security hole to cause their own unsigned and malicious replacement DLLs to be loaded -- with full system privilege -- as a result. This would be quite troublesome since the ability to load and execute arbitrary DLLs with signed software of high privileges could lead to application whitelisting bypass, the evasion of cybersecurity protections, and long-term persistence since the software runs at startup.

The researchers put a point on it by noting how easily this could be achieved: "The vulnerability gives attackers the ability to load and execute malicious payloads in a persistent way, each time the service is loaded. Once an attacker drops a malicious DLL in a vulnerable path, the service will load the malicious code each time it is restarted."

The second vulnerability affects Kaspersky Secure Connection which is a VPN client which is part of Kaspersky Internet Security solutions which creates a secure connection to the vendor's servers. Like Trend Micro, Kaspersky's VPN in versions below 4.0 does not check the signatures of the DLLs it loads, and it also runs with maximum system permissions. This exposes it to the same sort of DLL loading abuse. If an attacker can arrange to drop a malicious DLL in the Windows DLL search path, Kaspersky will load and execute it preferentially... thanks to Windows.

The third and final similar vulnerability was discovered in the Autodesk desktop app. The desktop app's service -- AdAppMgrSvc.exe -- has been present in Autodesk's software from 2017 to present and it also runs with full maximum NT AUTHORITY\SYSTEM permission. As with the previous two instances, a missing DLL call made by an accompanying library permitted the loading of arbitrary DLLs because there is no digital certificate validation... so unsigned DLLs can be executed.

The researchers wrote: "After an attacker gains access to a computer, they might have privileges limiting them to access only certain files and data. But the Autodesk service provides them with the ability to operate as NT AUTHORITY\SYSTEM which is the most powerful user in Windows, so they can access almost every file and process which belongs to the user on the computer."

The DLL design pattern and methodology is so deeply ingrained into Windows that there really is nothing that Microsoft can do about it today. That Windows Side-by-Side mess doesn't directly address DLL security, it's only there so that modern Windows has any chance to run at all. I was initially a bit surprised to learn that processes running with maximum permission were allowed to have unsigned DLLs loaded into their process space... but upon reflection, changing that at this point would likely break too many long-standing assumptions. So the best we can do is to

just keep patching and be glad that there are folks like SafeBreach Labs who take it upon themselves to find and responsibly disclose these problems when they are found.

## Miscellany

**"The Joy of Sync" Update**

- **Sync.com** **https://grc.sc/sync**
- **SyncThing**

---


https://promon.co/security-news/strandhogg/

The StrandHogg vulnerability

Promon security researchers have found proof of a dangerous Android vulnerability, dubbed 'StrandHogg', that allows real-life malware to pose as legitimate apps, with users unaware they are being targeted. The security firm Lookout, a Promon partner, confirmed that they have identified 36 malicious apps exploiting the vulnerability. Among them were variants of the

BankBot banking trojan which was first seen in 2017. During testing, Promon researchers found that all of the 500 most popular apps (as ranked by app intelligence company 42 Matters) are vulnerable to StrandHogg. All versions of Android are affected, including Android 10.

BankBot is one of the most widespread banking trojans around, with dozens of variants and new close relatives appearing continually. BankBot attacks have been detected around the world, in the U.S., Latin America, Europe and the Asia Pacific region. StrandHogg was first detected when banks reported that their customers were reporting missing funds from their accounts.

So what's the impact of this?

- All versions of Android affected, including. Android 10
- All top 500 most popular apps are at risk.
- Real-life malware is exploiting the vulnerability
- 36 malicious apps exploiting the vulnerability have been identified
- The vulnerability can be exploited without root access

When exploited by hackers

- They can listen to the user through the microphone
- Take photos through the camera
- Read and send SMS messages
- Make and/or record phone conversations
- Phish login credentials
- Get access to all private photos and files on the device
- Get location and GPS information
- Get access to the contacts list
- Access phone logs

How does any of this happen??? Through dangerous permission harvesting...


App icon of a legitimate app is clicked by the victim.

Instead of seeing the legitimate app, the malware is displayed and can now ask for any permission while pretending to be the legitimate app.

The victim is unknowingly giving permissions to the hacker. Victim is directed to the legitimate app.

The vulnerability makes it possible for a malicious app to ask for permissions while pretending to be the legitimate app. An attacker can ask for access to any permission, including SMS, photos, microphone, and GPS, allowing them to read messages, view photos, eavesdrop, and track the victim's movements.

The attack can be designed to request permissions which would be natural for different targeted apps to request to reduce suspicion from victims. Users are unaware that they are giving permission to the hacker and not the authentic app they believe they are using.

But wait! … there's more!!  Powerful credential stealing attacks are also enabled by the presentation of faked login pages:


By exploiting this vulnerability, a malicious app installed on the device can attack the device and trick it so that when the app icon of a legitimate app is clicked, a malicious version is instead displayed on the user's screen.

When the victim inputs their login credentials within this interface, sensitive details are immediately sent to the attacker, who can then login to, and control, security-sensitive apps.

So what's going on here?

What makes StrandHogg unique is that it enables sophisticated attacks without the need for a device to be rooted. It leverages weaknesses inherent in Android's multitasking system to enable powerful attacks that allows malicious apps to masquerade as any other app on the device. This exploit uses an Android feature called 'taskAffinity' which allows any app – including malicious ones – to freely assume any identity within the multitasking system they desire.

As I mentioned at the top, Promon's research found that every one of the top 500 most popular Android apps are vulnerable to this powerful attack… and across all versions of Android.

Promon calls this vulnerability 'StrandHogg' which is old Norse, referring to the Viking tactic of raiding coastal areas to plunder and hold people for ransom.

Promon's study significantly expands upon research carried out by Penn State University in

2015, where researchers theoretically described certain aspects of the vulnerability. At the time, Google dismissed the vulnerability's severity, but Promon now has clear evidence that hackers **are** exploiting StrandHogg to gain access to devices and apps.

The specific malware sample Promon analyzed did not reside on Google Play but was installed through several dropper apps/hostile downloaders distributed on Google Play. These apps **have** since been removed, but in spite of Google's Play Protect security suite, dropper apps continue to be published and frequently slip under the radar, with some being downloaded millions of times before being spotted and deleted.

Google is necessarily reactive: They will remove what they are aware of, but this means that some people are downloading and being hurt by malicious apps during the interim. An example of reactivity is the recently discovered "CamScanner" app which was a PDF creator which also contained a malicious module. It had been downloaded 100 million times.

Promon's Chief Technology Officer, Tom Lysemose Hansen comments: "We have tangible proof that attackers are exploiting StrandHogg in order to steal confidential information. The potential impact of this could be unprecedented in terms of scale and the amount of damage caused because most apps are vulnerable by default and all Android versions are affected."

So, what happened way back in 2015??

https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-ren-chuangang.pdf

The research conducted by Penn State University and FireEye was presented during the 24th USENIX Security Symposium which took place back in August of 2015. They titled their paper: "Towards Discovering and Understanding Task Hijacking in Android"

**Abstract:**
Android multitasking provides rich features to enhance user experience and offers great flexibility for app developers to promote app personalization. However, the security implication of Android multitasking remains under-investigated.

With a systematic study of the complex tasks dynamics, we find design flaws in Android multitasking which make all recent versions of Android vulnerable to task hijacking attacks.

We demonstrate proof-of-concept examples utilizing the task hijacking attack surface to implement UI spoofing, denial-of-service and user monitoring attacks. Attackers may steal login credentials, implement ransomware and spy on user's activities. We have collected and analyzed over 6.8 million apps from various Android markets. Our analysis shows that the task hijacking risk is prevalent.

Since many apps depend on the current multitasking design, defeating task hijacking is not easy. We have notified the Android team about these issues and we discuss possible mitigation techniques in this paper.

From the Android Developer Blog:

https://www.androidcookbook.info/android-1-6-sdk/the-allowtaskreparenting-attribute.html

## The allowTask Reparenting attribute

Last Updated on Wed, 29 May 2019 | Android 1 6 SDK

If an activity has its allowTaskReparenting attribute set to "true", it can move from the task it starts in to the task it has an affinity for when that task comes to the fore. For example, suppose that an activity that reports weather conditions in selected cities is defined as part of a travel application. It has the same affinity as other activities in the same application (the default affinity) and it allows reparenting. One of your activities starts the weather reporter, so it initially belongs to the same task as your activity. However, when the travel application next comes forward, the weather reporter will be reassigned to and displayed with that task.

So, where we are today, is that flexibility which Google deliberately designed into Android from the start (the Penn State / FireEye research was poking at Androids 3,4 and 5), which enables more powerful, handy and smooth smartphone application switching and sharing, not only **can** be abused -- as was clearly described and demonstrated more than four years ago, but **IS** now being actively abused in the wild to the detriment of Android users who are unlucky enough to mistakenly download a malicious Android app from the Google Play Store.  And… as we've seen, despite Google's best efforts to prevent it, malware gets in and gets downloaded… in some cases widely downloaded.