Security News Digest
January 09, 2018

It is a New Year and there is a New Quiz made for the occasion!
'Security New Year' Quiz

Make some 2018 New Year's Resolutions to protect your personal and financial information, to use security and privacy best practices, and to inform and educate other people in your life. Be Security Aware in all of your online activities (that includes the new fridge, coffee maker and internet-connected TV).

New Rules Let U.S. Border Agents Access Data on Phones, Laptops - But Not on the Cloud

https://globalnews.ca/news/3948960/u-s-border-agents-device-search-rules/

[Planning to travel to, or through, the United States? If yes, you should know your rights in advance.]
U.S. border agents can inspect data located on physical devices such as phones and laptops, but cannot access information stored remotely or on the cloud, under a new directive from U.S. Customs and Border Protection (CBP). **Under the updated rules, travellers can be asked to provide their devices' passwords to agents, but the passwords must be deleted or destroyed immediately following the search**. Searches of electronic devices should be carried out in the presence of the individual whose devices is being scrutinized unless there are concerns regarding national security or officer safety, the directive states. But allowing an individual to be present during a search "does not necessarily mean that the individual shall observe the search itself."
In order to prevent agents from accessing data stored remotely, travellers will be asked to disable network connectivity or put their devices in airplane mode before submitting them for inspection.
But while the directive offers privacy safeguards, it also includes exceptions under which officers can conduct more advanced searches. **In cases of "reasonable suspicion" concerning national security, law breaking or officer safety, agents can ask supervisors for permission to connect external devices, physically or wirelessly, to travellers' devices in order to review and copy their contents.**
Where sensitive data is accessed, such as medical records or journalists' work materials, agents will handle the data in accordance with "applicable federal law and CBP policy."
While CBP insisted that its rules strike a balance between national security and civil liberties, privacy advocates weren't convinced. In a statement, the American Civil Liberties Union (ACLU) said that the use of "reasonable suspicion" to justify searching devices falls short of the Constitutional requirement for search warrants based on probable cause. The ACLU also criticized the directive for not making it clear that while travellers can be asked to provide their passwords, they are not under any obligation to do so. "Congress should continue to press CBP to improve its policy," the group said.
In addition to the new rules, the agency also released data showing the government inspected a record number of devices last year. Agents inspected 30,200 electronic devices in the fiscal year 2017, which ended in September - a nearly 60 per cent increase from 2016. However, the agency stressed that only around 0.007 per cent of incoming international travellers had their devices checked.
The spike in searches comes as the Trump administration has moved to ramp up border security.

WPA3 WiFi Standard Announced After Researchers KRACKed WPA2 Three Months Ago

https://www.bleepingcomputer.com/news/hardware/wpa3-wifi-standard-announced-after-researchers-kracked-wpa2-three-months-ago/

People say "every kick in the ass is a step forward." Well, Belgian security researcher Mathy Vanhoef gave the WiFi Protected Access (WPA) standard a huge kick in the ass last fall when it disclosed details about **KRACK, a vulnerability in the WPA2 WiFi protocol used by billions of devices**. The step forward came today when the WiFi Alliance, the organization that decides WiFi standards, published the first details about the upcoming WPA3 WiFi protocol. **A first official draft of the WPA3 WiFi**

authentication protocol will be available later this year, but the WiFi Alliance teased four major features today that users and hardware vendors should look forward in the new standard.
The **first feature is protection against brute-force attacks** by blocking the WiFi authentication process after several failed login attempts. This is a basic feature found in many web or software authentication systems and makes perfect sense to be deployed with WiFi networks, which are most often subject to dictionary brute-force attacks. The **second is the ability to use nearby WiFi-enabled devices as the configuration panel for other devices**. For example, a user will be able to use his phone or tablet to configure the WiFi WPA3 options of another device that doesn't have a screen, such as tiny IoT equipment like smart locks, smart light bulbs, and others.
The **third and fourth features are related to encryption capabilities included in WiFi WPA3**. The third is "individualized data encryption," which is a feature that encrypts connections between each device and the router or access point, and the fourth is an improved cryptographic standard that the WiFi Alliance described as "a 192-bit security suite, aligned with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems, [which] will further protect Wi-Fi networks with higher security requirements such as government, defense, and industrial." **More details besides these generic descriptions are expected later in 2018**.
WPA3 will reach real-world devices in months. Despite the WiFi Alliance's quick move to get a new version of the WPA WiFi authentication standard out, it will take some time before users will be able to buy devices with WPA3 support included. Nonetheless, the rollout process is expected to go on without snags as vendors got on board with the new WPA protocol in a hurry, and most knew WPA2's time was up when they received word of the KRACK vulnerability under embargo, earlier in 2017.
"The standards behind WPA3 already existed for a while," said Mathy Vanhoef, the author of the KRACK attack on WPA2. "But now devices are required to support them, otherwise they're won't receive the 'WPA3-certified' label." "Linux's open source Wi-Fi client and access point already support the improved handshake," he added. "It just isn't used in practice.. But hopefully, that will change now."

Critical Unpatched Flaws Disclosed in Western Digital 'My Cloud' Storage Devices

https://thehackernews.com/2018/01/western-digital-mycloud.html

Security researchers have discovered several severe vulnerabilities and a secret hard-coded backdoor in Western Digital's My Cloud NAS devices that could allow remote attackers to gain unrestricted root access to the device. Western Digital's My Cloud (WDMyCloud) is one of the most popular network-attached storage devices which is being used by individuals and businesses to host their files, and automatically backup and sync them with various cloud and web-based services. **The device lets users not only share files in a home network, but the private cloud feature also allows them to access their data from anywhere at any time.** Since these devices have been designed to be connected over the Internet, the hardcoded backdoor would leave user data open to hackers.
GulfTech research and development team has recently published an advisory detailing a hardcoded backdoor and several vulnerabilities it found in WD My Cloud storage devices that **could allow remote attackers to inject their own commands and upload and download sensitive files without permission**. Noteworthy, James Bercegay of GulfTech contacted the vendor and reported the issues in June last year. The vendor confirmed the vulnerabilities and requested a period of 90 days until full disclosure. **On 3rd January (that's almost after 180 days), GulfTech publicly disclosed the details of the vulnerabilities, which are still unpatched**. [see article to read the technical details]

Everything You Need to Know - And What You Should Do - About the Computer Chip Security Flaws

http://business.financialpost.com/technology/personal-tech/what-you-need-to-do-because-of-flaws-in-computer-chips

The two security flaws affect nearly all microprocessors, the digital brains of the world's computers. Here's a guide to Meltdown and Spectre.
On Wednesday, a group of security experts revealed two security flaws that affect nearly all microprocessors, the digital brains of the world's computers. **These flaws, called Meltdown and Spectre, could allow hackers to lift passwords, photos, documents and other data from smartphones, PCs and the cloud computing services that many businesses rely on.** Some of the world's largest tech companies have been working on fixes for these problems. But the researchers who discovered the flaws said one of them, Spectre, is not completely fixable. "It is a fundamental flaw in the

way processors have been built over the last decades," said Paul Kocher, one of the researchers who discovered these flaws.

Here is a guide to what you need to know and what you should do.

Where exactly are these flaws? - Both are issues with the way computer chips are designed. Meltdown affects most processors made by Intel, the company that supplies the chips for a majority of PCs and more than 90 per cent of computer servers. Spectre is far more difficult for hackers to exploit. But it is even more pervasive, affecting Intel chips, microprocessors from the long-time Intel rival AMD and the many chips that use designs from the British company ARM. Your smartphone most likely contains an ARM chip.

Why are they such a problem? - Both flaws provide hackers with a way of stealing data, including passwords and other sensitive information. **If hackers manage to get software running on one of these chips**, they can grab data from other software running on the same machine. This is a particular issue on cloud computing services.

Why are cloud computing services so important? - Operated by companies like Amazon, Microsoft and Google, **these are services where any business or individual can rent access to computing power over the internet**. On a cloud service, each server is typically shared by many different customers. By exploiting the Meltdown flaw, a hacker can just load some software onto a cloud service and then grab data from anyone else who has loaded software onto the same server.

What about phones and PCs? - Phones and PCs are more difficult targets. Before they can exploit the chip flaws, hackers must find a way of getting their software onto your device. They could fool you into downloading an app from a smartphone app store. Or they could trick you into visiting a website that moves code onto your machine.

But companies are fixing these flaws? - They are trying. Meltdown can be fixed by installing a software "patch" on the machine. Microsoft has released a patch for PCs that use its Windows operating system. Apple said it had released software patches for iOS, Macs and the Apple TV that help mitigate the issue. Intel is also working on updates to help fix the problem. **The onus is now on consumers and businesses to install the fix on their machines.**

What should I do as a consumer? - Keep your software up to date. That includes your operating system and apps like your web browser and anti-virus software. Microsoft, Mozilla and Google have already released patches for Internet Explorer, Firefox and Chrome to help address the problem. Installing an ad blocker on your web browser is also a safeguard, according to security experts. Even the largest websites do not have tight control over the ads that appear on their sites - sometimes malicious code can appear inside their ad networks. A popular ad blocker among security researchers is uBlock Origin. "The real problem is **ads are dangerous**," said Jeremiah Grossman, the head of security strategy for SentinelOne, a computer security company. **"They're fully functioning programs, and they carry malware."**

How do I update my software? - Your operating system and apps typically have a button you can click to check for software updates. For example, in Google's Chrome browser on a computer, you can click on the three dots in the upper-right corner and click Update Google Chrome. To update Windows, click the Start button and click through these buttons: Settings, Update & security, Windows Update and Check for updates. To update the Mac system, open the App Store app and check the Updates tab for the latest software. **Don't procrastinate.** Last year, a piece of malware called WannaCry infected hundreds of thousands of Windows machines worldwide. Microsoft had released an update before the attack, but many machines were behind on downloading the latest security updates.

What about the cloud services? - Amazon, Google and Microsoft said that they had already patched most of the of servers that underpin their cloud computing services, and that largely addresses the problem. But Amazon and Google also said customers might need to make additional changes. To share computing power with customers, cloud services offer "virtual machines." These are computers that exist only in digital form. Customers use these virtual machines to run their own software. After Amazon, Google and Microsoft update their machines, customers may have to update the operating systems running on their own virtual machines to guard against some exploits.

If everybody updates his or her software, all is good? - No. The researchers who discovered Meltdown said that patching systems would slow them down by as much as 30 per cent in certain situations. That could be a problem for big cloud systems. Independent software developers also ran tests on a patched version of Linux, the open-source operating system that now drives more than 30 per cent of the world's servers, and saw similar slowdowns. "There are many cases where the performance

impact is zero," said Andres Frome, a software developer who has tested the new code. "But if you are running something like a payment system, where a lot of small changes are made to data, it looks like there will be a significant performance impact." Consumers are less likely to be affected, and Kocher said slowdowns could dissipate over time as companies refined their patches.
What about the Spectre flaw? - According to the researchers who discovered these flaws, including security experts at Google, the memory chip maker Rambus and various academic institutions, Spectre can't be completely fixed. But patches can solve the problems in some situations. Intel and Microsoft and others said the same.
Spectre can't be fixed? - No, according to the researchers. **But Spectre is much more difficult than Meltdown for hackers to exploit**. Similar to Meltdown, Spectre can steal information from one application and share it with another. For example, an app you download from the web could steal information like passwords from other software on a computer.
On Wednesday, the Department of Homeland Security issued an alert that said the only solution to the threats posed by Meltdown and Spectre would be a full replacement of the chips. But that does not seem feasible, given how many machines are involved. "Spectre is going to be with us a lot longer," Kocher said. **An Intel vice president, Donald Parker, is adamant that the company's chips will not need to be replaced. He said that with software patches and "firmware updates" - a way of updating code on the chip itself - Intel and other companies could "mitigate the issues."**

Microsoft Halts Chip Patches After Some PCs Can't Reboot

https://www.cnet.com/news/microsoft-amd-spectre-meltdown-halt-chip-patches-pcs-unbootable-brick/
[Jan9] Microsoft is putting critical Windows updates on hold after learning that some computers can't start up again after installing the patches. **The updates to Windows included fixes for the Spectre and Meltdown flaws that made a device's central processing unit vulnerable to hacking attacks. The PCs that couldn't reboot had processors made by AMD**, one of the three chipmakers whose products were affected by Spectre.
Microsoft said on its support website that **the halt to the Windows updates is temporary**. "Microsoft is working with AMD to resolve this issue and resume Windows OS security updates to the affected AMD devices via Windows Update and WSUS as soon as possible," the company said. The halted update adds to the chaos surrounding the revelation of the chip flaws, which could let hackers access secret information from processors on computers, phones and servers. The news of the flaws broke on Wednesday, before AMD, Intel and ARM had finished coordinating their response to the research that found the flaws. Hundreds of millions of devices contain affected chips, and the chipmakers worked with companies like Windows and Apple to update operating systems, as well as with cloud service providers like Google and Amazon to patch potentially affected servers.

Android Malware Steals Uber Logins, Then Covers It Up

https://www.infosecurity-magazine.com/news/android-malware-steals-uber-logins/
Symantec has discovered Android malware that steals Uber credentials and covers it up with the use of deep links. As explained in a blog post on the firm's website, the **Android.Fakeapp variant uses a spoofed Uber app interface that pops up on the users screen at regular intervals to trick them into entering their Uber ID and password. Once they do and click Next the credentials are sent to a remote server.** To make the heist seem legitimate and avoid alarming the victim, the malware then uses the deep link URI of the real app to display a screen which shows the user's location, something that would be expected when using Uber and is unlikely to raise suspicion.
In terms of mitigation, **Symantec advised users to follow these best practices**: Keep your software up to date, Refrain from downloading apps from unfamiliar sites and only install apps from trusted sources, Pay close attention to the permissions requested by apps, Install a suitable mobile security app, such as Norton, to protect your device and data, and Make frequent backups of important data
Nick Shaw, EMEA vice-president and general manager at Norton by Symantec, added that **users should think before they click: "Unsolicited communications may not be what they seem so use caution with any link delivered to you and always read the message first. Go directly to the website instead of clicking a link supplied."**

North Korea Appears to be Mining Cryptocurrency, Like Bitcoin, to Fund Regime: Report

https://globalnews.ca/news/3953855/north-korea-mining-cryptocurrency-to-fund-regime/

SEOUL – A cybersecurity company said it has found software that appears to install code for mining cryptocurrency and sends any mined coins to a server at a North Korean university, the latest sign that North Korea may be searching for new ways to infuse its economy with cash. The application, which was created on Dec. 24, uses host computers to mine a cryptocurrency called Monero. It then sends any coins to Kim Il Sung University in Pyongyang, said cybersecurity firm AlienVault, which examined the program. "Crypto-currencies may provide a financial lifeline to a country hit hard by sanctions, and as a result universities in Pyongyang have shown a clear interest in cryptocurrencies," the California-based security firm said in a release, adding that the software "may be the most recent product of their endeavours."

The company added a caveat that a North Korean server used in the code does not appear to be connected to the wider internet, which could mean its inclusion is meant to trick observers into making a North Korean connection. Kim Il Sung University, however, plays host to foreign students and lecturers, not just North Koreans. Kim Il Sung University did not immediately respond to requests for comment. Government officials representing North Korea at the United Nations were not immediately available for comment. Others have flagged increasing signs of North Korean interest in cryptocurrencies and underlying blockchain technology. "With economic sanctions in place, cryptocurrencies are currently the best way to earn foreign currency in North Korea's situation. It is hard to trace and can be laundered several times," said Mun Chong-hyun, chief analyst at South Korean cybersecurity firm ESTsecurity.

Cryptocurrency watchers say technical details of Monero, the 13th-largest crypto asset in the world.. with a total value of more than $7 billion, make it more appealing than bitcoin to those who value secrecy. Monero funds go to an un-linkable, one-time address generated with random numbers every time a payment is issued. That makes it less traceable than bitcoin, where transactions can be linked to specific, albeit anonymous, private addresses, cybersecurity experts said.

South Korea-based Bithumb, the world's busiest cryptocurrency exchange, is also the largest Monero trading exchange in the world, with about 24 percent of trading volume. The next largest were Europe-based exchange HitBTC and Hong Kong-based Bitfinex, as of Monday. Marshal Swatt, an expert in blockchain technology and financial exchange, said cryptocurrencies' independence from government regulation – and sanctions – made them logical choices for covert transactions. "They don't by themselves discriminate between good and bad actors," he said. "This makes it extremely compelling for countries like North Korea, Venezuela, Iran, Russia and others to exploit these non-governmental blockchain currencies for their own self-interest."

Breach of India's Biometric Database Puts 1 Billion Users at Risk

https://www.darkreading.com/vulnerabilities---threats/breach-of-indias-biometric-database-puts-1-billion-users-at-risk-/d/d-id/1330758

A breach of the Unique Identification Authority of India's Aadhaar biometric system is putting personally identifiable information (PII) of more than 1 billion Indian residents at risk, reports the Tribune, an Indian publication. Attackers created a gateway to the biometric database, in which any Aadhaar user's ID number can be entered into a portal, the Tribune reports. Once the number is entered, it will pull up the resident's name, address, postal code, photo, phone number, and email address, according to the Tribune. Cyberthieves are selling access to the portal for 500 rupees and are charging an additional 300 rupees for software that allows a victim's Aadhaar card to be printed, according to the report. The Unique Identification Authority of India denies its Aadhaar database has been breached, the Tribune reports, but notes that Tribune reporters were able to make Aadhaar data purchases as part of its investigation. [Update: India has since changed the way in which information on the system is accessed.]

And Now, This:

Apple Needs to Address iPhone Addiction Among Young People: Investors

https://globalnews.ca/news/3951107/apple-should-address-iphone-addiction-investors/

Apple Inc shareholders Jana Partners and the California State Teachers' Retirement System are urging the smartphone maker to take steps to address what they say is a growing problem of young people getting addicted to Apple's iPhones, Jana partner Charles Penner said. Jana, a leading activist shareholder, and CalSTRS, one of the nation's largest public pension plans, delivered a letter to Apple on Saturday asking the company to consider developing software that would allow parents to limit children's phone use, the Wall Street Journal reported earlier on Sunday. Jana and CalSTRS also asked Apple to

study the impact of excessive phone use on mental health, according to the publication. CalSTRS and Apple did not immediately respond to requests for comment.
Jana and CalSTRS together control about $2 billion worth of Apple shares, the Journal reports. The social rights issue is a new turn for Jana, which is known for pushing companies it invests in to make financial changes. However, the issue of phone addiction among young people has become a growing concern in the United States as parents report their children cannot give up their phones. CalSTRS and Jana worry that Apple's reputation and stock could be hurt if it does not address those concerns, according to the Journal.
Half of teenagers in the United States feel like they are addicted to their mobile phones and report feeling pressure to immediately respond to phone messages, according to a 2016 survey of children and their parents by Common Sense Media. The phone addiction issue got a high-profile boost from the former Disney child star Selena Gomez, 24, who said she canceled a 2016 world tour to go to therapy for depression and low self-esteem, feelings she linked to her addiction to social media and the mobile photo-sharing app Instagram.

Feel free to forward the Digest to others that might be interested.
Click Unsubscribe to stop receiving the Digest.

****

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****