Security News Digest
September 19, 2017

Do you "live on your mobile device"? Then you should take the quiz:
September Living Mobile Quiz

Keep It Secret and Keep It Safe...September 17-23 is Tolkien Week

and September 22nd is Hobbit Day

September 22 is a grand day and holds much meaning for Tolkien fans around the world, [including this SND editor]. Bilbo and Frodo Baggins share their birthdays on the 22nd, and as such, it is the day of Bilbo's 111th Long Awaited Party found in *The Lord of the Rings*. In Tolkien's *The Hobbit,* it is the day poor, wet Bilbo arrives by barrel in Laketown. *Hobbit Day* was begun and first observed back in 1978, and is now widely celebrated throughout the Tolkien fandom. Parties are thrown, food is eaten, and most of all, the life and work of J. R. R. Tolkien is remembered and cherished.
(The font used above is Kereru, created by Daniel Reeve for The Lord of the Rings movie trilogy. I purchased the font at MyFonts.com and it resides on my work computer. Namarie)

Today, we also celebrate, along with the U.S., their ***National IT Professionals Day***!!
Observed annually every third Tuesday in September, National IT Professionals Day is set aside to honor the venerable geeks of the world we all rely on to keep us connected. The IT (information technology) professional is the unsung hero of modern business, but often under-appreciated by it. Whether it be desktops, laptops, mobile devices, applications, servers, networks, databases or cybersecurity, IT professionals keep business humming. However, there is often a lack of understanding by business leaders and end users of the important role they play and the difficulties and complexities associated with modern IT.

Friday, September 22, at 1:02 Pacific Time is the Autumnal Equinox – the first day of Autumn.

And, now your Security News Digest stories for this week…..

RCMP Warns Canadians of Fraudulent 'Traffic Infringement' Email Scam

http://globalnews.ca/news/3742636/rcmp-traffic-ticket-email-scam/
RCMP are warning Canadians about yet another email scam – this time involving traffic tickets. An example of the scam looks authentic, with the RCMP logo and an attachment of "photographic evidence" of an unspecified traffic infringement. **But RCMP say it does not issue any charges via email, and if you get an email like it, to immediately delete it**. The attached "evidence" could contain malware that could infect your computer with a virus. This type of phishing scam is not new; versions of the email were seen in Alberta last year.
The scam is similar to a phishing email that pretended to be the Canada Revenue Agency, either saying the recipient owed money, or asked for bank information so they could be given money. Canadians should be aware that **these phishing scams are a form of brand spoofing**, the Canadian Anti-Fraud Centre explained on its website. The emails copy a known, legitimate agency and are used to "trick users into submitting personal, financial, or password data."
The Centre offered some tips on spotting fraudulent emails: (1) Beware of unsolicited emails from individuals or organizations prompting you to click on an attachment or link. (2) Watch for spelling and formatting errors. (3) Check the embedded hyperlink in the suspicious email by hovering your mouse over the link to verify the address. (4) Go with your gut. If an email seems fishy, it probably is.

If you do receive what you believe to be a fraudulent email, you can [should] report it to the Canadian Anti-Fraud Centre here. More tips on how to spot phishing scams can be found on the RCMP's website here.

Just Clicking on 'Free' Facebook Offers Leaves You Open to Villains and Viruses

http://www.cbc.ca/news/canada/nova-scotia/free-spam-scam-facebook-1.4285985

If you're a frequent Facebook user you know all about those "free" ads that pop up on your timeline - postings that offer two free Air Canada tickets, a $100 Ikea gift certificate or free pizzas, to mention just a few. **The problem is, they're not real. The offers, shared countless times by unsuspecting Facebook users, illegally use well-known company names and logos**.

Calgary resident Arthene Riggs saw the so-called Air Canada offer after it was shared by her sister, who received it from one of her friends. "I thought, 'Oh, my sister sent it. I should be good. Let me just try it and from then it's been a nightmare,'" Riggs said. Her account was subsequently shut down by Facebook, which sent a message saying the offer was spam. She had to open a new account with a different name, losing all her contacts, before Facebook subsequently gave her instructions to restore her original account.

A look at Facebook feeds shows Riggs is not alone. Many have shared an offer for a $100 Ikea coupon, which was also a scam. It was shared widely in Nova Scotia, where Ikea is opening a much-anticipated store this month. "Please be aware this is not an Ikea website or a website affiliated to Ikea and the offer is not authorized by Ikea," a company spokesperson told CBC News.

But aside from losing your Facebook account, what is the danger of liking, sharing or answering questions on fake offers? Ed McHugh, a marketing expert at Nova Scotia Community College, said in some cases the fake offers are intended to infect your device with a virus or worm. In other cases, it's hackers out to see how many people they can fool. The problem, he said, is sharing or liking the offers "can lead us down a rabbit hole to anywhere on the planet." "You don't know what kind of villains or viruses you're opening yourself up to, which could destroy the technology you have, or maybe even be phish that could take down the technology and phones of friends," he said.

Air Canada and Pizza Hut. The Air Canada offer has been around for almost two years. On Sept. 23, 2015, Air Canada posted this message on its Facebook site: "There is currently a scam on Facebook that claims to offer two free Air Canada tickets. To protect your personal information, do not respond, share with your friends or 'like' the post." In response to the most recent fake coupon, Air Canada spokesperson Isabelle Arthur said the company has posted a warning on its website. She pointed out Air Canada isn't the only airline affected by this scam and said it has contacted Facebook and the hosting provider of the website to shut it down. Last year, Pizza Hut was targeted and posted a message on its Facebook page warning customers there was a "fraudulent coupon circulating on Facebook claiming to offer a free pizza from Pizza Hut." It characterized the post as "a scam."…

How do you know? Facebook said its members who click on spam may be unwittingly installing malicious software or giving people access to Facebook accounts, which are then used to send out more spam. Facebook's website said it has "dedicated teams across the company that focus on protecting people." The company also said it's built tools to prevent and remove spam. **It urges users to report spam to Facebook so it can protect others**.

So how do you know what's real and what isn't? (1) Think before you click. Is it reasonable that Air Canada would give two free tickets to everyone? (2) Check the source of the offer. Call Air Canada, Costco, or whichever company is making the offer. Ask if it's legitimate. (3) Does the company have a website? Some of the offers do not. That should raise a red flag. (4) Check out their Facebook page. Click on About. If there is no information, the page is likely not what it appears to be. [And, as always..] (5) Remember, if it's too good to be true, it [very] probably is not true!

Thousands in P.E.I. Get Spam Email After Government Hack

http://www.ctvnews.ca/canada/thousands-in-p-e-i-get-spam-email-after-government-hack-1.3594845

Charlottetown - More than 94,000 people in P.E.I. have received an unauthorized spam message from the P.E.I. government. The government issued a statement Monday warning residents not to open an emailed newsletter titled: "Tonight's Winner is Drawn in 10 Hours." The email includes a link, which should not be opened. The province says its e-mail newsletter system was accessed without authorization on Sunday. The e-mail system was taken offline when the hacking was discovered.

Avril Lavigne 'Most Dangerous Celebrity' on Internet: McAfee

http://www.ctvnews.ca/entertainment/avril-lavigne-most-dangerous-celebrity-on-internet-mcafee-1.3595727

One-time Canadian pop-punk princess Avril Lavigne has beaten superstar Beyonce at something, but she may not be totally happy with her victory - she's been named the most dangerous celebrity on the internet. Cybersecurity firm McAfee said Tuesday that Lavigne, whose last album came out in 2013, was **the most likely celebrity to land users on websites that carry viruses or malware**. Searches for Lavigne have a 14.5 per cent chance of landing on a web page with the potential for online threats, a number that increases to 22 per cent if users type her name and search for free MP3s.

Bruno Mars was second in his debut on the list, followed closely behind by Carly Rae Jepsen. Zayn Malik (No. 4), Celine Dion (No. 5), Calvin Harris (No. 6), Justin Bieber (No. 7), Sean "Diddy" Combs (No. 8), Katy Perry (No. 9) and Beyonce (No. 10) rounded out the top 10 list. It's a dubious step up for Lavigne, who was ranked No. 2 in 2013. Lavigne, whose hits include "Sk8er Boi," "Complicated" and "I'm With You," has been out of the spotlight for several years as she battles Lyme disease.

McAfee had a few suggestions for why Lavigne scored so high on the 11th annual list: Interest after the artist said she's working on a new album, a feature story on her by E! Online and an internet conspiracy that she has been replaced by an impostor. [She also performed with Nickelback recently.] Lavigne is the first female musician to take the No. 1 spot and replaced Amy Schumer, named the most dangerous celebrity on the internet in 2016. In 2015, it was Dutch trance DJ van Buuren.

The survey is meant to highlight the danger of clicking on suspicious links. McAfee urges internet users to consider risks associated with searching for downloadable content. The company used its own site ratings to compile the celebrity list and used searches on Google, Bing and Yahoo.

Canadians Should Worry About U.S. Border Searches of Cell Phones: Privacy Czar

http://www.ctvnews.ca/canada/canadians-should-worry-about-u-s-border-searches-of-cell-phones-privacy-czar-1.3595255

Canadians should be "very concerned" about their cell phones, computers and other electronic devices being searched by U.S. border agents, the federal privacy czar says. Privacy commissioner Daniel Therrien told a House of Commons committee Monday that **U.S. Customs and Border Protection officers can look at mobile devices and even demand passwords under American law**. Therrien cited statistics indicating U.S. border searches of mobile phones had increased between 2015 and 2016. "These devices contain a lot of sensitive information," Therrien said. "We should be very concerned." New Democrat MP Nathan Cullen asked if that means no Canadian should cross the border with a phone, laptop or tablet unless they have "great comfort" with a U.S. border official inspecting the contents. "Yes, as a matter of law," Therrien said, though he acknowledged officers would not have time to inspect everyone's devices, given the huge numbers of people that cross the border daily. Therrien agreed with Cullen's suggestion that nothing in law could prevent U.S. border officials from peeking at a senior Canadian official's "playbook" on a trade negotiation. **Cullen said one of his constituents was denied entry to the U.S. on health-related grounds because information on the person's phone indicated a prescription for heart medication**. "And I thought, well, this is a strange invasion of one's privacy." Therrien said **Canadians should assess the "risk tolerance" they have to their information being examined by U.S. officers**. "My point is, think about what you're exposing your information to, and limit the amount of information that you bring to the U.S., because it may be required by customs officers." **Canadian law also allows border officers to inspect cell phones, since they are treated as goods**, Therrien told the Commons committee on access to information, privacy and ethics. But he noted Canada's border agency has a policy of limiting searches to cases where an officer has grounds to do so - for instance, because a phone might contain information about contraband items. Therrien said his office had received a "small number of complaints" about Canadian border officers searching cell phones. Last spring, Therrien expressed concern about U.S. plans to demand cellphone and social media passwords from foreign visitors. In a letter to the House of Commons public safety committee, he warned that recent pronouncements from the Trump administration could mean intrusive searches - even at preclearance facilities in Canada. In February, John Kelly, then U.S. homeland security secretary, suggested at a hearing that American officials could ask people entering the U.S. about the Internet sites they visit as well as passwords to help assess their online activities. Kelly's proposal prompted an American coalition of human rights and civil liberties organizations and experts in security, technology and the law to express "deep concern."

Equifax Data Breach Catches Attention of Canada's Privacy Commissioner

http://globalnews.ca/news/3739498/equifax-data-breach-catches-attention-of-canadas-privacy-commissioner/

[Sept12] Canada's Privacy Commissioner office says it has prioritized an examination into the massive Equifax data hack to ensure that Canadians are protected against future risks. In a posting on its website, it says it plans to work with data protection authorities in Canada and elsewhere to find out what went wrong. It says it has asked the credit monitoring company to tell Canadians as soon as possible if their information was stolen and to adopt measures to help them.

Equifax said last Thursday a security breach occurred over the summer resulting in the private information of up to 143 million people in the United States being compromised, along with certain Canadian and U.K. residents. In a posting on the Canadian part of its website, Equifax says it is "working night and day to assess what happened." It says the data breach is "contained," and the Canadian breach may have involved names, addresses and social insurance numbers. Equifax says "only a limited number of Canadians may have been affected."

It says a dedicated website and call centre set up last week won't help Canadians because it uses U.S. social security numbers, without offering an alternative. The Privacy Commissioner suggested Canadians can call Equifax at 1-866-828-5961 (English service) or 1-877-323-2598 (French service).

One Week After Massive Equifax Hack, Beware of Phishing Scams

http://globalnews.ca/news/3745269/equifax-hack-phishing-scams/

[Sept16] In the wake of the Equifax data breach, which affected 143 million Americans and an unknown amount of Canadians, officials are warning people to be wary of calls purporting to be from the credit company. A warning from the American Federal Trade Commission says a telephone phishing scam is just one of the ways scammers could use the news of the hack to trick you. "Ring, ring. 'This is Equifax calling to verify your account information.' Stop. Don't tell them anything. They're not from Equifax. It's a scam. Equifax will not call you out of the blue," the warning from the FTC reads.

Equifax discovered the hack July 29 but waited until last Thursday to warn consumers that criminals exploited a U.S. website application to access files between mid-May and July of this year. **But Equifax has said it will notify those affected by the hack by mail, not by phone**. The data breach made major headlines, the Office of the Privacy Commissioner is examining and people in Canada and the U.S. are filing class action lawsuits. And that's the reason why scammers will use it to try to scare people into giving up their personal information. "The scammers will try to look for vulnerabilities," Jessica Johnson of the Canadian Anti-Fraud Centre told Global News. "So, anytime there's something that makes big news, we'll usually see [a new scam] within a week or two of a big story." Along with the Equifax hack, she said phishing scammers could be trying to capitalize on other news events, like the recent hurricanes, by pretending to be charities like the Red Cross.

…. The company is reportedly telling Canadians who call its help line that unless you have dealings in the U.S., it's not likely your information was compromised. **The Canadian Automobile Association (CAA) says it was partnered with Equifax on the auto organization's identity protection program**. It is informing about 10,000 of its members that they may have had sensitive data compromised by the massive Equifax cybersecurity breach. The organization says it has been trying since the first reports of the Equifax breach surfaced to determine if it affects any of the approximately 10,000 CAA members who signed up for the program. It says Equifax has not provided any answers so far. Equifax Canada did not respond to requests from The Canadian Press.

Equifax Cybersecurity Failings Revealed Following Breach

http://www.securityweek.com/equifax-cybersecurity-failings-revealed-following-breach

Shortcomings revealed by researchers and cybersecurity firms following the massive data breach suffered by Equifax show that a successful hacker attack on the credit reporting agency's systems was inevitable. Some members of the industry pointed out last week that the company's Chief Security Officer (CSO) Susan Mauldin was a music major with no educational background in cybersecurity or technology. Mauldin and Chief Information Officer David Webb retired from the company on Friday.

Others dug up old vulnerability reports that the firm had still not addressed and noted the lack of even basic protections on the company's website. Even the website set up by Equifax to provide information about the breach was riddled with security holes and some services flagged it as a phishing site. The organization does not have a vulnerability disclosure program that would allow and encourage security

experts to responsibly report the flaws they find. **The Apache Struts 2 vulnerability leveraged by cybercriminals to breach Equifax systems had been known and exploited for roughly two months before the attack on the company.** Equifax said its security team knew about the flaw and is now trying to determine why **an online dispute portal, which served as the initial point of entry, remained unpatched**.

Experts pointed out that the Apache Struts flaw is not easy to fix, especially if you have many systems that need patching. However, they believe the problem can be addressed with modern security solutions.

Comodo discovered that more than 388 records of Equifax users and employees are up for sale on the dark web. The information, which includes usernames, passwords and login URLs, was apparently stolen using Pony malware. The security firm pointed out that some Equifax credentials were also exposed in third-party incidents, including the massive LinkedIn and Dropbox breaches.

"From third-party (non-company system) sources, we uncovered that Equifax's chief privacy officer, CIO, VP of PR and VP of Sales, used all lowercase letters, no special symbols, and easily guessable words like spouses' names, city names, and even combinations of initials and birth year. This reveals that they didn't follow basic security best practices and were lacking a complex password requirement," Comodo said in a blog post.

Another security incident related to the company was brought to light by security blogger Brian Krebs, who was informed by researchers that an Equifax Argentina employee portal exposed 14,000 records, including credentials and consumer complaints. The breach, the manner in which the company investigated the incident, and some of these security failings have led to a significant drop in Equifax shares. Before the hack was disclosed, Equifax stock was worth roughly $140, but it has now dropped to $92, and financial experts believe it could plunge as low as $50. The incident has already cost the company nearly $10 billion in market value.

Android Apps Infected with ExpensiveWall Malware Downloaded 21M Times

https://www.hackread.com/expensivewall-malware-apps-21-million-times/

Time and again we have witnessed the reality to be reinforced that it is extremely difficult to maintain the optimal security of our devices. Google has infused great efforts in ensuring the security of software, Android apps, and devices, however, it turns out that it is next to impossible. Lately, we have seen Google Play Store becoming the victim of Trojan malware quite a few times, and as per latest reports, a new version of an old malware called ExpensiveWall has been found in many everyday use apps available on Play Store. What's more disturbing is the fact that the malicious apps have been downloaded 4.2 million times. The new variant and its older version both are believed to have been downloaded between 5.9 and 21.1 million times.

This particular malware campaign against Android devices is being touted as the biggest ever malware outbreak in recent times that makes fraudulent subscriptions on users' behalf without their knowledge or consent. The malware is dubbed ExpensiveWall because it was initially spotted in a number of wallpaper apps by Check Point cybersecurity firm and it was named after a free wallpaper app called LovelyWall.

According to Check Point's research team, **the malware sends fake premium SMS messages to charge users' account for services that they haven't subscribed to**. Check Point also shared the list of applications harboring the malware. The older version of ExpensiveWall was discovered in January 2017 by McAfee. ExpensiveWall was hidden in numerous apps, the majority of which were seemingly harmless photo or video editing, camera and free wallpaper applications available on Google Play Store. At least 50 applications contained this piece of malware before it was deleted from the Play Store. Check Point researchers claim that the malware is distributed through a software developer kit known as gtk that is embedded into their apps. The trojanized app compelled people to subscribe through SMS and the app was remotely installed, but its actual function was to steal and leak sensitive personal data such as phone number, IP address, GPS location and installed applications on the infected device. This particular app was downloaded millions of times, and hence data from such an astounding number of devices was leaked due to this app.

Security experts observed a stark similarity between these malware, which is that the number of infected devices is not in hundreds or thousands but millions in both instances. **ExpensiveWall was downloaded millions of times despite the fact that it had low star reviews on Play Store while some got to know about it through ads on Instagram**. According to security experts Andrey Polkovnichenko, Bohdan Melnykov and Elena Root, ExpensiveWall is different from other malware in this family because it is

'packed,' which refers to **an advanced "obfuscation technique" that malware developers use for encrypting malicious code so that the malware can evade the default anti-malware protections of Google Play Store**. These apps were downloaded millions of time without leaving any suspicion. In Packing technique, attackers hid the malicious code from Google by compressing and encrypting the executable file before its uploading on Play Store. The package also includes a key that reassembles the executable after the file has made it to the targeted device. Despite being a decade-old technique, it remains an effective method for hackers.
After Check Point security firm informed Google about the presence of malware in around 50 of Play Store apps, the tech giant removed them but it was too late as more than 5,000 devices were infected within days. It is yet unknown how much revenue was generated through the malware. Although the apps are now removed, many devices will remain infected until the malicious titles are uninstalled explicitly.

Vevo Hacked, 3.12 TB of Data Leaked

https://nakedsecurity.sophos.com/2017/09/17/vevo-hacked-3-12-tb-of-data-leaked/

There's a good chance that you've watched a popular music video from Vevo, either via YouTube, Vevo's website or its mobile app. **Most popular music artists release their videos through Vevo these days.** The company – a joint venture between Warner Music Group, Sony Music Entertainment, Universal Music Group, Alphabet Inc and Abu Dhabi Media – has taken the position that MTV and MuchMusic used to have in delivering music videos to the general public. Vevo has secured about $200 million USD in advertising revenue this year, on the strength of the tremendous popularity of videos from artists such as Taylor Swift, Beyonce, and Rihanna.
Well now, Vevo confirms that they've been hit by a huge cyber-attack. A Vevo spokesperson said to Gizmodo on Friday: (We) can confirm that Vevo experienced a data breach as a result of a phishing scam via LinkedIn. We have addressed the issue and are investigating the extent of exposure. OurMine has claimed responsibility for the attack. The group has previously taken over Mark Zuckerberg's Pinterest and Twitter accounts, taken over HBO's Twitter account, attacked BuzzFeed and TechCrunch, and poisoned WikiLeaks' DNS.
Through a LinkedIn phishing scam, OurMine was able to compromise a Vevo employee's account for Okta, an app used to sign into workplace networks. From there, they were apparently able to gain access to Vevo's media storage servers. About 3.12 TB of internal files have been leaked online, which include videos, internal office documents, promotional material, yet to be used social media content, and information about recording artists signed to the participating record companies.

LinkedIn Phishing Scam Steals Gmail Credentials Through Google Docs

https://www.hackread.com/linkedin-phishing-scam-stealing-gmail-data-via-google-doc/

LinkedIn, a business and employment-oriented social networking website contains personal information of more than 500 million users from around the world making it a jackpot for cybercriminals and those looking for identity theft. Also, since LinkedIn's data breach of 117 million users and then its sale on the dark web has helped malicious elements compromise websites and other social media accounts using leaked credentials. OurMine is a recent example of a hacking group using leaked passwords of LinkedIn users to hack their accounts on other sites.
Recently, **a new phishing scam has been detected in which Premium LinkedIn accounts are being used to trick users into giving away their login credentials and phone numbers in the hands of cybercriminals**. The scam was discovered by Malwarebytes' lead malware intelligence analyst Jérôme Segura who noticed that unsuspecting users have been receiving phishing links in private message and InMail hiding behind URL shortener ow.ly and gdk.mx a free hosting provider.
The message comes with following content: "I have just shared a document with you using GoogleDoc Drive, View shared document http:/.. Upon clicking the link, users are taken to a compromised website hosting a Gmail phishing page that asks them to log in with their Gmail id and passwords. It further asks for a phone number, and secondary email then displays a decoy Wells Fargo document hosted on Google Docs. But Yahoo and AOL users are also targeted in this scam since it asks for respective users to log in with their username and password, Segura added.
"The fraudulent message includes a reference to a shared document and a link that redirects to a phishing site for Gmail and other email providers which require potential victims to log in," Segura explained. "Those who proceed will have their username, password, and phone number stolen but won't

realize they were duped right away. Indeed, this phishing scam ends on a tricky note with a decoy document on wealth management from Wells Fargo." Furthermore, cybercriminals are also using LinkedIn InMail feature which allows Premium users to send direct messages to others even if they are not connected. Currently, it is unknown how many Premium accounts are being used to spread this scam.

"This kind of attack via social media is not new – we have seen hacked Skype, or Facebook accounts send spam – **but it reminds us of how much more difficult it is to block malicious activity when it comes from long-standing and trusted user accounts, not to mention work acquaintances or relatives**. This also makes such attacks more credible to potential victims and can lead to a snowball effect when victims become purveyors of phishing links themselves," Segura wrote. This is not the first time when cybercriminals have used LinkedIn for phishing attacks. In November 2016, a scam used Dropbox as bait to not only steal LinkedIn login credentials but also aimed at financial details, driving license and passport copy for identity theft. LinkedIn and other Internet users are advised not to open messages or emails from an unknown sender, never click or download attachments from an email whose sender is not known to them. Stay safe online.

Billions of Bluetooth Devices Vulnerable to Takeovers, MITM Attacks; No User Action Required

https://www.scmagazine.com/billions-of-bluetooth-devices-vulnerable-to-takeovers-mitm-attacks-no-user-action-required/article/688037/

Billions of Bluetooth devices, including those running on Android, iOS, Linux, and Windows, contain major vulnerabilities that can allow malicious actors to remotely execute code, take over devices, and perform man-in-the-middle (MITM) attacks, researchers have reported. What's more, attackers do not need to trick users into performing an action in order to compromise or infect them, nor does a target device's Bluetooth have to be paired with an attacking device or even be in Discovery Mode. **The device simply has to have its Bluetooth feature turned on, which for most products is the default setting**.

Even worse, compromised devices can then be **further leveraged to attack additional nearby systems over the air**, including any segregated or air-gapped devices that happen to be Bluetooth-enabled.

"Basically, it's an airborne delivery method or attack vector that could be very easily abused," said Nadis Izrael, CTO and co-founder of Armis, in an interview with SC Media.

Dubbed BlueBorne, the collection of vulnerabilities – eight in total, three of which are critical – was discovered by researchers from Internet of Things security company Armis. The flaws potentially impact at least 5.3 billion Bluetooth-enabled devices, including computers, smartphones, and IoT devices such as watches, smart TVs, and some automobile systems. "These silent attacks are invisible to traditional security controls and procedures. **Companies don't monitor these types of device-to-device connections in their environment, so they can't see these attacks or stop them**," said Yevgeny Dibrov, CEO of Armis, in a company press release. "The research illustrates the types of threats facing us in this new connected age."

Because phones compromised via BlueBorne bugs can quickly infect nearby devices over the air, attacks can quickly spread like wildfire, creating potentially unprecedented scenarios. Michael Parker, VP of marketing at Armis, used the WannaCry ransomware attack as an example. "You had WannaCry. Now imagine WannaCry 'Blue,'" said Parker to SC Media. "It is ransomware that is spread through Bluetooth...It can spread from device to device, unnoticed by current security measures, locking down smartphones, desktops, laptops, and it can't be stopped by traditional methods." Or, the attacker could stay under radar, perhaps delivering botnet malware that "just lays and waits to be activated" at just the right moment.

Between April and August 2017, Armis researchers contacted Apple, Google, Linux, and Microsoft Corporation to disclose the various BlueBorne vulnerabilities. In response, Google has developed a patch for Android 6 and 7 devices, and has notified its manufacturing partners of the update. Microsoft announced today that it released a security update back in July that addressed BlueBorne vulnerabilities in devices running on all supported Windows versions. (Windows Phones were not impacted by the flaws.) "...Customers who have Windows Update enabled and applied the security updates, are protected automatically," a Microsoft spokesperson told SC Media via email. "We updated to protect customers as soon as possible, but as a responsible industry partner, we withheld disclosure until other vendors could develop and release updates." The Linux kernel security team has confirmed that it will release a patch as well, but there is no confirmation on when this will happen. And Apple is well ahead of the game, as

the specific BlueBorne vulnerability that Armis researchers discovered in iOS was actually fixed with the distribution of version 10 of the mobile operating system. However, any devices running on iOS versions 9.3.5 and earlier, as well as AppleTV devices using version 7.2.2 or lower, remain vulnerable. [see the article for all of the technical details on Android and Linux vulnerabilities and more]

U.S. Government Bans Use of Kaspersky Software

http://www.esecurityplanet.com/endpoint/u.s.-government-bans-use-of-kaspersky-software.html

U.S. Acting Secretary of Homeland Security Elaine Duke this week issued a Binding Operational Directive requiring all Federal Executive Branch departments and agencies to stop using any products, solutions or services from Russia's Kaspersky Lab. Departments and agencies have 30 days to identify any presence of Kaspersky products on their information systems, 60 days to develop detailed plans to remove and discontinue all use of the products, and 90 days to begin to implement those plans to remove and discontinue use of Kaspersky products.

Security Risks. The decision was made, according to the Department of Homeland Security (DHS), "based on the information security risks presented by the use of Kaspersky products on federal information systems," particularly since Kaspersky products generally provide broad access to files and elevated privileges on the computers on which they're installed. "The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks," the DHS said in a statement. "The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security," the DHS added.

Kaspersky's Answer. In response, Kaspersky said in a statement that it has no inappropriate ties with any government, and said the DHS allegations regarding ties to Russian intelligence and other agencies are "completely unfounded." "Kaspersky Lab has never helped, nor will help, any government in the world with its cyberespionage or offensive cyber efforts, and it's disconcerting that a private company can be considered guilty until proven innocent, due to geopolitical issues," Kaspersky said. "The company looks forward to working with DHS, as Kaspersky Lab ardently believes a deeper examination of the company will substantiate that these allegations are without merit."

Christopher Krebs, a senior DHS official in the National Protection and Programs Directorate, told the Washington Post that **the department is giving Kaspersky 90 days to prove that its products don't present a security risk**. "We've determined that [the software] poses an unacceptable amount of risk based on our assessment," he said. "If they want to provide additional information or mitigation strategies, our door is open." U.S. officials told the Post that at least a half dozen federal agencies run Kaspersky software.

In an interview with the BBC, Kaspersky Lab founder Eugene Kaspersky said, "When they say we have strong ties with Russian espionage it's not true." "We cooperate with many law enforcement agencies around the world - in the past with the U.S. as well," Kaspersky added.

A Loss of Trust. Venafi CEO Jeff Hudson told *eSecurity Planet* by email that this is part of a much larger pattern. "U.S. government officials are pressuring software companies to implement encryption backdoors because they think it will help them catch potential terrorists," he said. "At the same time, they banned security software from a Russian company for use in the U.S. government because they are concerned about security backdoors," Hudson added. "They want to have it both ways, which is understandable." It's not even controversial at this point, Hudson said, to suggest that other governments will inevitably take the same steps against U.S. software manufacturers if they're required to include encryption backdoors, and U.S. software companies will suffer. "The net result is that the entire Internet will become completely untrustable - there will be backdoors everywhere, and governments and bad guys will use them at will," Hudson said. "We have to hold ourselves to a higher standard and lead the way to show the rest of the world the right way to secure the Internet."

Hackers Backdoored CCleaner for a Month: Over 2 million Infected with Malware

https://www.csoonline.com/article/3225914/security/hackers-backdoored-ccleaner-for-a-month-over-2-million-infected-with-malware.html

Hackers backdoored the popular CCleaner Windows utility. For nearly a month, two malware-tainted versions collected computer names, IP addresses, lists of installed and active software, as well lists of

network adapters before sending the data to the attacker's server. Cisco Talos, which discovered the malware on Sept. 13, while a customer was beta testing new exploit detection technology, warned that the tainted versions of CCleaner were being distributed for nearly a month. CCleaner 5.33 was released on Aug. 15, and a newer version without compromised code wasn't released until Sept. 12. A cloud version released in August was similarly infected. The backdoored version was even signed using a valid certificate issued to Piriform, which was acquired by antivirus firm Avast in July.

Cisco Talos researchers said, "It is likely that an external attacker compromised a portion of their development or build environment and leveraged that access to insert malware into the CCleaner build that was released and hosted by the organization. It is also possible that an insider with access to either the development or build environments within the organization intentionally included the malicious code or could have had an account (or similar) compromised which allowed an attacker to include the code."

Piriform confirmed the attack, saying Avast "determined on the 12th of September that the 32-bit version of our CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 products, which may have been used by up to 3% of our users, had been compromised in a sophisticated manner." A non-backdoored version of CCleaner was released the same day. As for the compromised cloud version, CCleaner Cloud v1.07.3191, which was released on Aug. 24, the company released a non-malware tainted version on Sept. 15. Law enforcement is involved. Piriform said, "It would have been an impediment to the law enforcement agency's investigation to have gone public with this before the server was disabled and we completed our initial assessment."

An estimated 2.27 million systems installed the infected CCleaner. Although Avast doesn't want users to panic, it admitted to Forbes that an estimated *2.27 million* systems installed the backdoored versions. Piriform previously claimed that there have been 2 billion total CCleaner downloads with an additional 5 million weekly installs. Cisco Talos said, "The impact of this attack could be severe given the extremely high number of systems possibly affected." If even a small fraction of those systems were compromised, an attacker could use them for any number of malicious purposes. **Affected systems need to be restored to a state before August 15, 2017, or reinstalled. Users should also update to the latest available version of CCleaner to avoid infection. At the time of this writing that is version 5.34**.

The freebie version won't automatically update to a version without a backdoor. If you installed it, then go grab a clean version of CCleaner now if you intend to keep using the software. **CCleaner has been popular for years, trusted by tech-savvy users. Taking advantage of that trust is partially why this attack is so distressing. That and you don't expect an antivirus firm to infect you with malware**.

Cisco Talos concluded: This is a prime example of the extent that attackers are willing to go through in their attempt to distribute malware to organizations and individuals around the world. By exploiting the trust relationship between software vendors and the users of their software, attackers can benefit from users' inherent trust in the files and web servers used to distribute updates.

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

****