Security News Digest
July 25, 2017

Canada will remain where it is for a long time to come, but the Canada's Security Scene Quiz will move to the Information Security Awareness previous quizzes page at the end of July. Watch this space for the August feature!

August 1st is acknowledged across the globe as World Wide Web Day!

World Wide Web Day, marks the birth of the Web in August 1990 at the Europe Laboratory for Particle Physics (CERN) in Switzerland. Tim Berners-Lee and Robert Cailliau developed a prototype Web browser and introduced Hypertext Markup Language, HTML. *The first ever website was published on August 6, 1991 and served up a page explaining the World Wide Web project and giving information* on how users could setup a web server and how to create their own websites and web pages, as well as how they could search the web for information. The URL for the first ever web page put up on the first ever website was http://info.cern.ch/hypertext/WWW/TheProject.html

The World Wide Web ('WWW' or simply the 'Web') is a global information medium which users can read and write via computers connected to the Internet. *The term [web] is often mistakenly used as a synonym for the Internet itself, but the Web is a service that operates over the Internet, just as e-mail also does*. The history of the Internet dates back significantly further than that of the World Wide Web.

On July 21st, the Google "Doodle" honoured Canadian Marshall McLuhan! ["the Medium is the Message"]

Who is Marshall McLuhan? Meet the Canadian Media Theorist Who Predicted the Internet

http://nationalpost.com/news/canada/who-is-marshall-mcluhan-how-a-canadian-media-theorist-predicted-the-internet/wcm/194cb7e2-e778-4780-9aba-6eb94831fcc5

Canadian professor Marshall McLuhan rose to prominence as a media theorist while teaching at the University of Toronto in the 1960s. He is celebrated as the man who predicted the rise of the internet, and on his 106th birthday, Google is honouring him with his own doodle. Here's what you need to know about McLuhan and his ideas. …McLuhan didn't live to see the internet [he died in 1980], but many have argued his concept of the "global village" predicted its rise. The gist of his global village idea was that, with the rise of electronic media, the information system would become global, putting people in contact with information from everywhere. McLuhan said the emergence of the global village was already shifting behaviour as he was writing about it. .."One of the effects of living with electric information is that we live habitually in a state of information overload. There's always more than you can cope with," he said.

CRA Educates Canadians on How to Identify Tax-Related Phone and Text Scams

http://mobilesyrup.com/2017/03/29/cra-educates-canadians-on-how-to-identify-tax-related-phone-and-text-scams/

The Canada Revenue Agency is campaigning to make Canadians aware of the many impostors that use the tax agency's name to solicit money through fraudulent calls, texts, emails, letters and online forms. The CRA held a "fraud chat" on Twitter on March 29th to bring more attention to the issue and is offering a comprehensive package of information concerning fraud prevention. To begin with, the agency says if you receive a call saying you owe money to the CRA, you should call or check your online account [i.e. MyAccount if you have created it] to ascertain whether there's any truth behind the statement.

One way to check if the communication is fishy is to see if its breaking any of the CRA's rules for communicating with Canadians. The agency promises that it will never do any of the following: ask for personal information of any kind by email or text message, request payments by prepaid credit cards, give taxpayer information to another person (unless formal authorization is provided by the taxpayer) or leave personal information on an answering machine. The CRA also does not condone using threats or vulgar language.

Additionally, it doesn't generally send emails with links asking for specific personal or financial information, though there is an exception: CRA phone representatives may send email links if you

request them over the course of a call. To give Canadians a sense of the forms these scams might take, the CRA provided some specific examples of scams, from real-world phone call transcripts to realistic-looking online refund forms.
The agency also notes that **Canadians should report deceptive telemarketing** to the Canadian Anti-Fraud Centre, **contact the police if they believe themselves to be the victims of fraud or contact the CRA if they believe their log-in credentials are compromised**, among other steps. Find more information on fraud prevention in the source link: CRA.

Enhanced Security for Flights to the U.S.: What You Need to Know

http://www.cbc.ca/news/canada/airport-security-canada-u-s-1.4212727
Starting Wednesday [July19], **Canadian travellers to the United States could be subject to "heightened screening" of their electronic devices when passing through airport security**. …A spokesperson for the Canadian Air Transport Security Authority (CATSA), the group that handles security checkpoints at Canadian airports, explained how their officers will carry out those measures.
What's changing? Not much. The way it works now, travellers going through airport security might be randomly selected for additional screening, or you might also undergo additional screening if you or your belongings trigger a metal detector or X-ray alarm. That might mean letting a screening officer physically search through your bag, or swab your belongings for traces of explosive materials. *The difference now, according to CATSA spokesperson Mathieu Larocque, is that travellers might also be randomly selected to remove electronic devices larger than smartphones - think tablets and e-readers - from their carry-on baggage and present them for additional screening, too*. *That would involve removing any protective casing around devices to allow for a more thorough physical inspection and proving to officers that the device can be turned on*. "All of the rest of the screening process remains the same," Larocque said. Laptops will still have to be removed from bags and placed in bins individually as before.
Is the data on my device at risk? No more than usual. *The contents of your devices can still be searched by U.S. border agents, for those attempting to enter the U.S., and by Canadian border officers on your way into Canada. But that would typically be separate from a security screening*. Refusal to unlock your device or give a U.S. border agent your password could deny you entry into the country. And while Canadian border officers can't deny Canadian citizens entry into Canada, refusal to co-operate could result in the seizure of your device.
Security inspectors, on the other hand, are tasked with examining the physical integrity of the device itself - looking for signs that a tablet or laptop has been modified or tampered with, with the intent to cause harm. "They're [security inspectors as opposed to customs officials] not going to be looking at the content of the device," said Larocque. "They're not going to ask you to input your password or look at files. That's not the intent."
What should I expect at the airport?
Larocque says that all travellers - even those flying within Canada - should be prepared to have their devices examined. That means charging devices before arriving at the airport, and ensuring that protective cases can be easily removed, or even better, removed ahead of time. "Electronic devices that cannot be taken out of their cases or powered on when requested during enhanced screening will not be permitted beyond the screening checkpoint," according to CATSA's site. If all this sounds familiar, it's because there was a time when screening officers could ask travellers to power on devices such as laptops, but Larocque said the practice was discontinued for several years - until now. And don't forget that airlines are advising travellers to get to the airport two hours before their scheduled flight to the U.S., to allow time for the screening.
Here's what border agents can search for on your phone (and more): (video) *This two-minute video explains that electronic devices are classed as "goods". Border agents can inspect the Contacts, Apps, Email, Location information, Photos, Selfies, and anything else on the device, and can copy it as well. In Canada, they can only inspect what is on the device, but US agents can look at the social media and whatever is stored in the Cloud. The video recommends you encrypt the contents, and Turn Off the device before going. In Canada, you cannot be compelled to give your passwords*.

Canadian Firm Pays $425,000 to Recover from Ransomware Attack

http://www.itworldcanada.com/article/canadian-firm-pays-425000-to-recover-from-ransomware-attack/394844
[July13] A major Canadian company was forced to pay $425,000 in Bitcoin over the weekend to restore its computer systems *after suffering a crippling ransomware attack that not only encrypted its production*

databases but also the backups as well. "They literally had no choice but to pay" because the backups were frozen, said Daniel Tobok, CEO of forensics firm Cytelligence, which is helping with the investigation. *Tobok wouldn't identify the company for reasons of confidentiality. He believes it to be the largest ransomware payment in Canada to date*. By comparison last month a South Korean Web hosting firm reportedly paid the equivalent of US$1 million in ransomware, believed to be the biggest publicly reported payment so far in the world.

Although the forensic investigation is in its early stages, the attack was very sophisticated. **It started with spear phishing** targeting six senior company officials who were sent a PDF attachment with a malicious payload. *Staff apparently fell for two old ploys: Two of the messages purported to be from a courier company and told recipients the attachments were invoices for packages to be picked up, while the other messages asked officials to open and print the attached document. That led to the insertion of malware*. "It appears from early investigation **there were vulnerabilities in unpatched systems in their Windows environment**," said Tobok. "They had **a couple of outdated database servers** that had not had all the recent patches on them."

It is believed *the attackers then spent several months hunting around the network to find data stores before releasing the ransomware, which spread across the corporate network including backed up data*. "They knew where the databases were, the confidential information," said Tobok. *"They knew everything."* Before handing over the money the company demanded the attackers prove they had the decryption key. The incident is another warning that Canadian organizations aren't immune from being attacked.

The early lessons from the attack, Tobok said, are if the CIO/CISO can afford it have a third party do a full penetration test. "A real security audit would have discovered some of these vulnerabilities," he said. "You can never control phishing because that's a human element," he said, although adding that awareness programs are still essential. **Another lesson apparently is to ensure backups aren't connected to the primary system**. And, as Tobok says, **"patch, patch, patch."** At this stage, Tobok said, **no enterprise should be caught off guard by this kind of attack**. "When you look at [recent ransomware attacks] Petya, WannaCry, if that's not a wake-up call for companies, I don't know what else is."

Flash Loses Final Appeal: Adobe Sentences Its Web Tech to Death

https://www.cnet.com/news/adobe-kills-flash-web-browser-tech-2020/

The pioneering software paved the way for YouTube and countless games, but Adobe will kill Flash in 2020. Here's what it means for you.

The Flash Player has been there for you all along, inside your browser, making it possible for you to play online games, stream radio station music and watch YouTube videos. But after a two-decade run, Adobe is killing it off. Countless nails have been hammered in Flash's coffin in recent years, most notably by Apple's Steve Jobs and also by Adobe itself. **Now, though, there's a date for the funeral: Dec. 31, 2020**. *Flash has been a website workhorse* - online gaming site Kongregate has more than 100,000 Flash games - *but don't fret over the demise of the pioneering software. It's more appropriate to rejoice, since the software today is a security risk and major source of browser crashes*. Indeed, Adobe's move is momentous enough that the biggest names in web tech - Apple, Google, Facebook, Mozilla and Microsoft - coordinated announcements to tell us what's going on and **to reassure us all that it's going to be fine**.

What's it mean for me?

For the time being, you'll have to jump through some hoops to play Crush the Castle. In the coming years, depending on what browser you use and how it's configured, the Flash phase-out could be anything between no biggie and a serious problem. Some games will stop working. Schools and businesses that rely on Flash-based instruction modules will have to move into the future. Some websites, especially old ones that are no longer updated, might stop working.

Today's workarounds all will break on mainstream browsers by the end of 2020. Here's a rundown of what you can expect:

Chrome: Google's browser has begun asking us for permission to run Flash on some websites last year, and it'll do so more often and later disable Flash by default. "We will remove Flash completely from Chrome toward the end of 2020," Google said.

Firefox: Mozilla's browser will start asking you in August which sites you want to enable Flash on, it'll disable Flash altogether by default in 2019, and there will be lingering support through the end of 2020 only in Firefox's less frequently updated Extended Support Release.

Edge: The newest version of Microsoft's browser uses a click-to-run option that asks if you want to run Flash on a website, a policy that will continue through mid-2018. *The company's older Internet Explorer browser won't give you any grief*. In mid-2018, Edge will be more aggressive about requiring you to authorize Flash. In 2019, Microsoft will disable Flash by default, and by the end of 2020, Microsoft will disable it completely in both browsers.
Safari: Starting last year, Apple's Safari started blocking Flash from running. If you really want it, you can re-enable it on websites that offer to download Flash, an action Safari notices and that will give you an offer to run Flash for the site.
Facebook, which hosts lots of Flash-based games, urged programmers to get with the program so ordinary folks don't have to suffer through any of these problems. "While games built in Flash will run on Facebook until the end of 2020, we strongly advise developers to follow the timelines set by browsers," Facebook said in a blog post.
Countdown to 2020. …Flash exploded into popularity shortly after Microsoft's Internet Explorer won the early browser wars of the 1990s. IE was the default browser in the world's most widely used operating system, but Microsoft left the software mostly dormant. Filling the void was Flash creator Macromedia, acquired by Adobe in 2006. *Flash brought animation technology that was good for games, interactivity that let people build features like photo galleries, the ability to use webcams for video chat and multimedia features that wiped out an earlier confusing array of options. People installed Flash in their browsers, programmers didn't need to worry about differences between IE, Mozilla Firefox, Apple Safari and other browsers, and lots of advanced web features just worked. "Few technologies have had such a profound and positive impact in the internet era," Balakrishnan said*.
Flash's downside. But Flash came at a cost. **The fact that it could run full-fledged programs exposed browsers to a large number of security vulnerabilities**. It was responsible for a sizable percentage of browser crashes, too. It used battery power that became precious as we moved from plugged-in desktop computers to laptops and then phones. And importantly for Jobs' decision to ban Flash from iPhones and iPads, it was born in the era of PCs with keyboards and mice, not phones with touch-screen controls. [article has more tech-history]

US Company to Implant Microchips in Employees

https://www.bleepingcomputer.com/news/technology/us-company-to-implant-microchips-in-employees/
Three Square Market (32M), a Wisconsin-based business, will become the first US company to implant RFID microchips in employee's hands. *[Yuck!]* The decision is nothing more than a media stunt orchestrated by 32M in partnership with BioHax, a Swedish-based company that provides bio-friendly implantable RFID microchips. 32M is a provider of break room food dispensers and has recently added support for *implantable RFID microchips, allowing anyone to pay for food just by waving their RFID-implanted hand near one of their devices*.
Company holding a "chip party". To show that RFID implants are safe, the company will provide free RFID implants to all employees during a "chip party" on August 1. *Implants are optional*. Besides the benefit of using Jedi-like tricks when buying food from office break rooms, *32M and BioHax say the chip has secondary benefits, such as opening access doors, activating office copy machines, automatic login for work computers, unlocking work phones, sharing business cards, and even storing critical medical/health information. 32M hopes their stunt will garner enough media attention, so other companies will consider the benefits of employee implants*. The benefit for 32M is that once companies adopt RFID implants - for any other reasons - they'll be able to push their RFID-friendly food dispensers to those companies' office break rooms.
Implants work similarly to contactless payment cards. RFID implants work on the same NFC (Near-Field Communications) technology used by today's contactless payment cards and mobile wallet solutions. The RFID chip is implanted between the thumb and forefinger underneath the skin. An implant takes seconds, and the body's reaction varies from person to person. In a press release, the company says it views RFID implants as the future in micro-payments. "We see this as another payment and identification option that not only can be used in our markets but our other self-checkout / self-service applications that we are now deploying which include convenience stores and fitness centers," said 32M COO Patrick McMullan. *[new product opportunity: protective gloves to prevent unauthorized scanning!]*

This Scary Android Malware Can Record Audio, Video and Steal Your Data

http://www.zdnet.com/article/this-scary-android-malware-can-record-audio-video-and-steal-your-data/

A new form of malware has proved to be one of the most advanced Android information-stealers ever discovered, enabling attackers to open a backdoor in order to monitor data, steal information, record audio and video, and even infect the phone with ransomware. **Dubbed GhostCtrl**, the malware can stealthily control many of the infected device's functions - *and researchers have warned that this is just the beginning, and the malware could evolve to become a lot worse*. This new malware appears to be based on OmniRAT, a form of spying software capable of giving hackers full remote control of devices running Windows, Mac, Linux, and Android - although, unlike its apparent predecessor, GhostCtrl focuses purely on Android.

Mobile devices have become an increasingly valuable target for cybercriminals and those conducting espionage, not only because they can provide information about virtually every aspect of a target's lives, but because the device will almost always be with them. Discovered by researchers at Trend Micro, GhostCtrl forms part of a wider campaign targeting Israeli hospitals with the information-stealing Windows RETADUP worm - but the mobile arm of the attack represents an even more dangerous threat to victims. *In total, there are three versions of GhostCtrl* - one which steals information and controls some of the device's functions, a second which adds more features to hijack, and now the malware is on its third version which combines the most advanced capabilities of previous incarnations while adding further malicious capabilities. Those include monitoring the phone's data in real time, and the ability to steal the device's data, including call logs, text message records, contacts, phone numbers, location, and browser history. *GhostCtrl can also gather information about the victim's Android version, Wi-Fi, battery level, and almost any other activity*.

The most worrying aspect of the malware isn't just its ability to intercept messages from contacts specified by the attacker, as *GhostCtrl can also stealthily record audio and video, enabling the attackers to conduct full-on espionage on victims*. **Users become infected with the malware by downloading fake versions of legitimate popular apps, including WhatsApp and Pokemon Go**. When launched, GhostCtrl installs a malicious Android application package (APK) in order to take over the device. *This APK contains backdoor functions named 'com.android.engine' designed to trick the user into thinking it's a legitimate application, when what it's really doing is connecting to a command and control server to receive instructions on what information to steal*. ...Trend Micro researchers also recommend that Android devices should be kept as updated as possible and that enterprises should restrict permissions on company devices to prevent the installation of malware.

Your Roomba May Have a Map of Your Home, and Now Companies Want to Sell that Data

http://globalnews.ca/news/3621154/roomba-house-map-selling/

The Roomba robotic vacuum has been whizzing across floors for years, but its future may lie more in collecting data than dirt. That data is of the spatial variety: the dimensions of a room as well as distances between sofas, tables, lamps and other home furnishings. To a tech industry eager to push “smart” homes controlled by a variety of Internet-enabled devices, that space is the next frontier. Smart home lighting, thermostats and security cameras are already on the market, but Colin Angle, chief executive of Roomba maker iRobot Corp, says they are still dumb when it comes to understanding their physical environment. He thinks the mapping technology currently guiding top-end Roomba models could change that and is basing the company’s strategy on it. “There’s an entire ecosystem of things and services that the smart home can deliver once you have a rich map of the home that the user has allowed to be shared,” said Angle.

That vision has its fans, from investors to the likes of Amazon.com Inc, Apple Inc and Alphabet who are all pushing artificially intelligent voice assistants as smart home interfaces. *According to financial research firm IHS Markit, the market for smart home devices was worth $9.8 billion in 2016 and is projected to grow 60 percent this year*. *Angle told Reuters that iRobot, which made Roomba compatible with Amazon’s Alexa voice assistant in March, could reach a deal to sell its maps to one or more of the Big Three in the next couple of years*. Amazon declined to comment, and Apple and Google did not respond to requests for comment.

Guy Hoffman, a robotics professor at Cornell University, said detailed spatial mapping technology would be a “major breakthrough” for the smart home. Right now, smart home devices operate “like a tourist in New York who never leaves the subway,” said Hoffman. “There is some information about the city, but the tourist is missing a lot of context for what’s happening outside of the stations.” *With regularly updated maps, Hoffman said, sound systems could match home acoustics, air conditioners could schedule airflow by room and smart lighting could adjust according to the position of windows and time of day. Companies*

like Amazon, Google and Apple could also use the data to recommend home goods for customers to buy, said Hoffman.
One potential downside is that selling data about users' homes raises clear privacy issues, said Ben Rose, an analyst who covers iRobot for Battle Road Research. Customers could find it "sort of a scary thing," he said. [see article for more discussion]

FBI Issues Warning on IoT [Internet of Things] Toy Security

http://www.darkreading.com/cloud/fbi-issues-warning-on-iot-toy-security/d/d-id/1329373

IoT toys are more than fun and games and can potentially lead to a violation of children's privacy and safety, the Federal Bureau of Investigation warned Monday. Internet-connected toys carry the potential of violating children's privacy and safety, *given the amount of information the toys can collect and store*, the Federal Bureau of Investigation warned on Monday. The sensors, microphones, data storage capabilities, cameras, and other multi-media features of IoT toys could potentially gather information on a child regarding their name, school, activity plans and physical location. And if those toys are hacked, the information and data collected could potentially be used by attackers to do a child harm, the FBI warned. The FBI advisory offered advice on selecting an IoT toy, such as only connecting it to a secure and trusted WiFi network, research the toy to ensure it can receive firmware and software updates, and investigate where the information entered into the toy is stored.
[Read more about the FBI advisory here. The following is excerpted from the FBI Advisory.]
Why Does This Matter to My Family?
The features and functions of different toys vary widely. In some cases, *toys with microphones could record and collect conversations within earshot of the device*. Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. **The collection of a child's personal information combined with a toy's ability to connect to the Internet or other devices raises concerns for privacy and physical safety**. *Personal information (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/IPs*. The exposure of such information could create opportunities for child identity fraud. Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks. **Consumers should examine toy company user agreement disclosures and privacy practices, and should know where their family's personal data is sent and stored, including if it's sent to third-party services**. Security safeguards for these toys can be overlooked in the rush to market them and to make them easy to use. Consumers should perform online research of these products for any known issues that have been identified by security researchers or in consumer reports.
What Makes Internet-Connected Toys Vulnerable?
Data collected from interactions or conversations between children and toys are typically sent and stored by the manufacturer or developer via server or cloud service. In some cases, it is also collected by third-party companies who manage the voice recognition software used in the toys. *Voice recordings, toy Web application (parent app) passwords, home addresses, Wi-Fi information, or sensitive personal data could be exposed if the security of the data is not sufficiently protected with the proper use of digital certificates and encryption when it is being transmitted or stored*. Smart toys generally connect to the Internet either: Directly, through Wi-Fi to an Internet-connected wireless access point; or Indirectly, via Bluetooth to an Android or iOS device that is connected to the Internet.
The cyber security measures used in the toy, the toy's partner applications, and the Wi-Fi network on which the toy connects directly impacts the overall user security. Communications connections where data is encrypted between the toy, Wi-Fi access points, and Internet servers that store data or interact with the toy are crucial to mitigate the risk of hackers exploiting the toy or possibly eavesdropping on conversations/audio messages. Bluetooth-connected toys that do not have authentication requirements (such as PINs or passwords) when pairing with the mobile devices could pose a risk for unauthorized access to the toy and allow communications with a child user. It could also be possible for unauthorized users to remotely gain access to the toy if the security measures used for these connections are insufficient or the device is compromised.
[Note: FBI Advisory encourages consumers to consider the following recommendations, at a minimum, prior to using Internet-connected toys. –see article]

U.S., European Police Say 'Dark Web' Markets Shut Down

http://www.securityweek.com/us-european-police-say-dark-web-markets-shut-down

Washington - US and European police on Thursday announced the shutdown of two huge "dark web" marketplaces that allowed the anonymous online trade of drugs, hacking software and guns. *Underground websites AlphaBay and Hansa Market had tens of thousands of sellers of deadly drugs like fentanyl and other illicit goods serving more than 200,000 customers worldwide. AlphaBay, the largest dark web market, had been run out of Thailand* ***by a 25-year-old Canadian, Alexandre Cazes****, who was arrested two weeks ago*. It had filled the gap left behind by the notorious Silk Road online market, shut down by authorities in 2013. Since then AlphaBay had grown to ten times the size of Silk Road, offering more than 250,000 listings for illegal drugs and toxic chemicals, and 100,000 advertisements for guns, stolen and fraudulent personal documents, counterfeit goods, malware and computer hacking tools, according to the US Department of Justice.

AlphaBay's shutdown in early July sent traffic flooding into the smaller Hansa marketplace. *But the tens of thousands of users that flocked to Hansa were unaware that Dutch police had already secretly taken control of the market's server, giving them the ability to identify and track buyers and sellers of illicit goods*. Netherlands police said Thursday they had recently arrested Hansa market's administrators, and had this week arrested a key vendor on the market as well.

Officials said shutting down the two markets and the arrests of the administrators had enabled them to collect extensive intelligence on buyers and sellers, including criminal gangs. Their names were being distributed to law enforcement in 37 countries. They also seized millions of dollars' worth of digital currencies like Bitcoin used exclusively on the websites. "This case, pursued by dedicated agents and prosecutors, says you are not safe, you cannot hide. We will find you, dismantle your organization and network, and we will prosecute you," US Attorney General Jeff Sessions said in a warning to dark web entrepreneurs. "This operation is an example of the improving concerted ability of law enforcement to strike against criminals, even on the dark net," said Europol executive director Rob Wainwright. "This coordinated hit against these two marketplaces is just a taste of what is to come in the future."

Lamborghini, Porsche seized

According to a US indictment opened Thursday, Cazes created AlphaBay in July 2014 to host, via the anonymizing Tor network, a wide range of illicit trade and money laundering. It required users to trade in digital currencies, which helps mask identities. *AlphaBay took a commission on all transactions, earning Cazes tens of millions of dollars, the indictment said. Thai police arrested Cazes on July 5, discovered his laptop open and logged onto the server that hosted AlphaBay as the administrator. By seizing the unlocked, unencrypted computer, authorities gained access to passwords used by Cazes, and to all the information and cryptocurrencies on the AlphaBay server. Last week Cazes was found dead in a police cell in Thailand, with authorities saying he had hanged himself with a towel*. Police seized a Lamborghini, a Porsche, three houses and a hotel in Thailand owned by Cazes and his wife, as well as accounts scattered across Thailand, Switzerland, Cyprus, and Antigua. According to the indictment, investigators found a file on his computer saying his net worth was more than $23 million. The documents also showed that he had gained citizenship in Antigua and was seeking the same in Cyprus via significant investment in real estate.

Netherlands police said they were able to gain control of the Lithuania-based server for Hansa in June after arresting the two administrators, who they said were from Germany. They transferred the market to Dutch servers and operated it for weeks, collecting messages between buyers and sellers, whom they say mostly traded drugs. The number of vendors rose eight-fold after AlphaBay closed, with transactions hitting 1,000 a day.

'DarkHotel' APT Uses New Methods to Target Politicians

http://www.securityweek.com/darkhotel-apt-uses-new-methods-target-politicians

The DarkHotel threat group has been using some new methods in attacks aimed at government employees with an interest in North Korea, according to a report published this week by security firm Bitdefender. The activities of the DarkHotel advanced persistent threat (APT) actor came to light in November 2014, when *Kaspersky published a report detailing a sophisticated cyber espionage campaign targeting business travelers in the Asia-Pacific region. The group has been around for nearly a decade and some researchers believe its members are Korean speakers*.

The attackers targeted their victims using several methods, including through their hotel's Wi-Fi, zero-day exploits and peer-to-peer (P2P) file sharing websites. Nearly one year later, the threat group was observed using new attack techniques and an exploit leaked from Italian spyware maker Hacking Team. *DarkHotel victims have been spotted in several countries, including* North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, Taiwan, China, *the United States*, India, Mozambique, Indonesia and Germany. *Up until recently, the attacks appeared to focus on company executives, researchers and development personnel from sectors such as defense industrial base, military, energy, government, NGOs, electronics manufacturing, pharmaceutical, and medical*.
In more recent DarkHotel attacks it has dubbed "Inexsmar," security firm Bitdefender said the hackers targeted political figures, and they appeared to be using some new methods. Bitdefender's analysis is based on samples from September 2016. The initial Trojan downloader, **delivered via phishing emails**, collects information on the infected device and sends it back to its command and control (C&C) server. If the compromised system meets requirements (i.e. it belongs to an individual who is of interest), the first stage DarkHotel downloader, disguised as a component of OpenSSL, is fetched. In the meantime, in an effort to avoid raising suspicion, the malware opens a document titled "Pyongyang e-mail lists - September 2016," which provides a list of email contacts for various organizations in North Korea's capital city. If the system profile does not match what the attackers are looking for, the C&C server returns a "fail" string and the attack stops. *If the attack continues, a second payload is retrieved*.

Microsoft Sued Fancy Bear to Gain Control of the Domains Used in the Cyber Espionage Campaigns

https://securityaffairs.co/wordpress/61232/cyber-crime/fancy-bear-lawsuit.html

Microsoft used the lawsuit to disrupt a large number of cyber espionage campaigns conducted by infamous Fancy Bear APT hacking group (APT28, Sofacy, Sednit, and Pawn Storm). The experts, with the help of the authorities, took over the command and control infrastructure of the group in order to analyze the traffic and the targets of the malware by using the lawsuit as a tool.
"A new offensive by Microsoft has been making inroads against the Russian government hackers behind last year's election meddling, identifying over 120 new targets of the Kremlin's cyber spying, and control-alt-deleting segments of Putin's hacking apparatus." reported the Daily Beast. "How are they doing it? It turns out Microsoft has something even more formidable than Moscow's malware: Lawyers." Microsoft sued Fancy Bear in a US federal court, accusing the APT group of computer intrusion, cybersquatting, and reserving several domain names that violate Microsoft's trademarks.
Fancy Bear is active since at least 2007 and was one of the APT groups involved in the numerous cyber-attacks against the US Democratic National Committee and 2016 US Presidential Election. Numerous reports published by security firms linked the APT group to the GRU (General Staff Main Intelligence Directorate), the Russian secret military intelligence agency. The experts at Microsoft observed Fancy Bear hackers often using domain names that look-alike Microsoft products and services, such as livemicrosoft[.]net and rsshotmail[.]com, for its cyber espionage campaigns. This abuse was exploited by Microsoft to sue the hacking group with "unknown members" into the court of justice and gain the ownership of domains used by Fancy Bear to deliver malware. *"These servers can be thought of as the spymasters in Russia's cyber espionage, waiting patiently for contact from their malware agents in the field, then issuing encrypted instructions and accepting stolen documents," the report reads.*
Last year, the U.S. District Judge Gerald Bruce Lee granted Microsoft's request and issued a then-sealed order to domain name registrars *"compelling them to alter"* the DNS of at least 70 Fancy Bear domains. The traffic was redirected to servers controlled by Microsoft. Technically the procedure is called **'sinkholing'** and allows investigators to monitor the traffic from the infected systems to track the botnet infrastructure.
This is the precious work done by the Digital Crimes Unit that has identified the potential victims of the Russian APT. "*By analyzing the traffic coming to its sinkhole, the company's security experts have identified 122 new cyber espionage victims, whom it's been alerting through Internet service providers," the report reads.* Microsoft is still waiting for a final judgment on the Fancy Bear case. The hearing has been scheduled on Friday in Virginia court. *"Microsoft concludes in court filings that its efforts have had "significant impact" on Fancy Bear's operations. On Friday, the company is set to ask Magistrate Judge Theresa Carroll Buchanan for a final default judgment against Fancy Bear, and for a permanent injunction giving Microsoft ownership of the domains it's seized."*

45,000 Facebook Users Leave One-Star Ratings After Hacker's Unjust Arrest

https://www.bleepingcomputer.com/news/security/45-000-facebook-users-leave-one-star-ratings-after-hackers-unjust-arrest/

Over 45,000 users have left one-star reviews on a company's Facebook page after the business reported a security researcher to police and had him arrested in the middle of the night instead of fixing a reported bug. The arrest took place this week in Hungary after *an 18-year-old found a flaw in the online ticket-selling system of Budapesti Közlekedési Központ (BKK), Budapest's public transportation authority*.

Teen hacks company using browser's DevTools. The young man discovered that he could access BKK's website, press F12 to enter the browser's developer tools mode, and modify the page's source code to alter a ticket's price. Because there was no client or server-side validation put in place, the BKK system accepted the operation and issued a ticket at a smaller price. As a demo, the young man says he bought a ticket initially priced at 9459 Hungarian forints ($35) for 50 Hungarian forints (20 US cents).

BKK calls police and has the teenager arrested. The teenager - who didn't want his name revealed - reported the issue to BKK, but the organization chose to contact the police and file a complaint, accusing the young man of hacking their systems. Police arrested the teenager in the middle of the night shortly after, even if the young man didn't live in Budapest, nor did he ever use the fraudulently obtained ticket.

BKK management made a fatal mistake when they brazenly boasted in a press conference about catching the hacker and declaring their systems "secure." *Since then, other security flaws in BKK's system have surfaced on Twitter*. *As details of the case emerged, public outrage grew against BKK and its manager Kálmán Dabóczi, especially after it was revealed that BKK was paying around $1 million per year for maintenance of its IT systems, hacked in such a ludicrously simple manner*. The beneficiary of this humongous contract is a local company called T-Systems, which ironically sponsored an "ethical hacking" contest. Talking to Hungarian press, the young hacker said he only had the best intentions when he reported the issue to BKK and said he hopes the organization withdraws its report.

Hungary's Facebook community reacts with vitriol. In the meantime, tens of thousands of Hungarians have shown their solidarity and support for the teenager by going on Facebook and leaving one-star reviews on BKK's page. While initially, reviews came from Hungarians, international users started leaving their own thoughts on BKK's page after the incident become a trending topic on Reddit. "You should partner with better companies managing the security and reliability of your online purchase systems! Shame on you BKK!," said one user.

And Now, This:

A Smart Fish Tank Left a Casino Vulnerable to Hackers

http://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html

Most people know about phishing - but one casino recently learned about the dangers of actual fish tanks. *Hackers attempted to steal data from a North American casino through a fish tank connected to the internet*, according to a report from security firm Darktrace. Despite extra security precautions set up on the fish tank, hackers still managed to compromise the tank to send data to a device in Finland before the threat was discovered and stopped.

"Someone used the fish tank to get into the network, and once they were in the fish tank, they scanned and found other vulnerabilities and moved laterally to other places in the network," Justin Fier, director for cyber intelligence and analysis at Darktrace, explained to CNN Tech. As internet-connected gadgets and appliances become more common, there are more ways for bad guys to gain access to networks and take advantage of insecure devices. *The fish tank, for instance, was connected to the internet to automatically feed the fish and keep their environment comfortable - but it became a weak link in the casino's security*.

The unnamed casino's rogue fish tank is *one of nine unusual threats that Darktrace identified on corporate networks published in a report Thursday*. ...In another example of an unusual attack, smart drawing pads connected to insecure Wi-Fi were used to send data to websites around the world in what's called a "denial of service" attack. A hacker had scanned the internet looking for vulnerable devices, and exploited them to try and flood other websites with too much traffic.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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 Technology, Innovation and Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****