Security News Digest
July 11, 2017

For Canada's 150th anniversary of Confederation, check out
Canada's Security Scene Quiz

Drone Operators Cautioned to Stay Away from B.C. Wildfires

http://www.cbc.ca/news/canada/british-columbia/wildfires-drone-restrictions-1.4198378

As firefighters battle hundreds of wildfires across B.C., drone enthusiasts are being reminded to keep their equipment far away from the flames. *Flying an unmanned aerial vehicle (UAV) near an active wildfire can result in thousands of dollars in fines and even possible jail time, but that hasn't always stopped some operators from taking the risk*.

That's why drone operator and instructor Sterling Cripps had stern words for anyone who defies provincial and federal regulations and flies a drone near a wildfire. "You are putting people at risk when you are flying a drone in a smoky fire area," Cripps said. Two years ago, eight helicopters and five skimmers fighting a wildfire near Oliver had to be grounded for hours when a stray drone flew too close. There were also reports last year of drones being spotted near wildfires in B.C. and Alberta.

So far this year, there have been no reports of UAV flying in the vicinity of wildfires in British Columbia, but Cripps is concerned about getting the message out to people who may not be aware of the rules and potential consequences. "It would be a very selfish act on anyone's part who wants to go in and fly a drone in these areas," Cripps said. He pointed out that firefighting aircraft are flying in low visibility conditions, at low altitudes and low speeds, often with heavy loads of water or retardant. "There's no way they would ever see a drone. If one was ever ingested into an engine or [smashed] into a windscreen or something like that, the results would be catastrophic," Cripps said.

Jail time, heavy fines for violators

The legal repercussions can also be severe. *B.C.'s Wildfire Act was amended last year to include sanctions of up to a year in jail and fines of as much as $100,000 for interfering with wildfire control efforts*. *Under Transport Canada regulations, the penalties can include up to 18 months in jail and fines as high as $25,000 for unauthorized aircraft found flying within a radius of about nine kilometres of a fire or below an altitude of about a 900 metres*.

Anyone who is unsure about whether it's safe to put a drone in the air can check NavCanada's notices to airmen for the legal boundaries around wildfires. Those notices are available online or by calling 1-866-541-4102.

Apologies, Cheques Issued for Health Ministry Firings

http://www.timescolonist.com/news/local/apologies-cheques-issued-for-health-ministry-firings-1.20913644

[Please note: The Security News Digest has followed this story since it broke in 2012. This 'resolution' article appears here in its entirety.] Health researchers wrongly fired in 2012 have received letters of apology and cheques, ranging from $15,000 to $125,000, from the head of the B.C. Public Service. The payouts, based on recommendations by the B.C. ombudsperson, were delivered in the final week of June - just in time for the ombudsperson's recommended deadline of June 30.

A letter accompanying a cheque for $75,000 to Ramsay Hamdi details the ways in which the Ministry of Health failed him. Among them, it said Hamdi was not informed of the allegations against him, he was not given a full opportunity to respond to those allegations and there were no reasonable grounds for his dismissal. "As a valued Ministry of Health employee of over 28 years and a Senior Economist who was a team member, trusted co-worker and expert in the proper use of administrative health data and economic modeling, you deserved to be treated fairly and respectfully. On behalf of the government, I apologize that you did not receive this fair and respectful treatment, and for your suspension and dismissal. I further apologize for the stress and harm, including harm to your finances and reputation, you suffered as a result of this investigation and its aftermath," the letter says. The letter is signed by Kim Henderson, deputy minister to the premier, under Christy Clark, and head of the B.C. Public Service. Hamdi said he

appreciated the apology, but it should have come from those directly responsible. He said he didn't believe the ombudsperson's conclusion that there had been no political interference in the process. He said he deposited his $75,000 cheque in line behind Mark Isaacs, a wrongly fired contractor. "This touched us all like a fire," Hamdi said. "It was the same teller. He had quite a day."
Ron Mattson, another wrongly-fired employee, said the cash and apology don't make up for the damage caused by the firings - including the death of researcher Roderick MacIsaac. MacIsaac, a 46-year-old University of Victoria co-op student, killed himself in December 2012, about four months after he was fired in connection with allegations of inappropriate conduct involving government drug research. "I believe they did what they were required to do or what was recommended to do through the [ombudsperson's] report. Did I feel warm and fuzzy after receiving it? No. It's very nice that the civil service provided us the apology, but it should have come from the government and from the former premier [Christy Clark]," Mattson said. Mattson said that while he was pleased to receive $125,000, it doesn't make things right. "I can't even think of a proper way to describe how badly they treated us," he said. "No money in the world will bring back Roderick," he said. Mattson said he'd still like to see some of the responsible individuals "receive their just rewards."
The ombudsperson's report did not recommend firing those who were still employed in government. Since the report was released, some senior managers have left the government, although it is not clear whether they were fired, let go, or left on their own accord. A spokesperson for the Ministry of Finance confirmed that Barb Walman, Lindsey Kislock and Wendy Taylor had left their positions. "As this is a personnel matter, we can't go into further details. In all personnel matters we're limited in what we can say due to privacy considerations. We can confirm that the individuals are not with the B.C. Public Service." Taylor was one of the lead investigators in the process that led to the firings. Walman and Kislock were assistant deputy ministers in the Ministry of Health, and helped set the terms of the investigation.

Facebook and Google Will Participate in [July 12th] ~~Next Week's~~ Big Net Neutrality Protest

https://www.theverge.com/2017/7/7/15938022/facebook-goolge-net-neutrality-protest-day-of-action-fcc
Facebook and Google have confirmed their participation in a wide-scale net neutrality protest scheduled for July 12th, according to *Fortune*. *The protest is being called the* ***"Internet-wide Day of Action to Save Net Neutrality," or "Day of Action" and "Battle for the Net" for short****. It's designed to be an illustrative example of the breadth and magnitude of opposition to the Federal Communication Commission's [FCC's] recent regulatory behavior (or lack thereof) that open internet advocates fear could roll back years of legislative progress,* in a fashion similar to the SOPA and PIPA protests of 2012.
It's unclear how Facebook or Google plan to participate. However, a number of other tech companies have also confirmed their support, including Amazon, Netflix, Reddit, Mozilla, Kickstarter, and Spotify. *"Websites, Internet users, and online communities will come together to sound the alarm about the FCC's attack on net neutrality," reads the protest's official website*. "We'll provide tools for everyone to make it super easy for your followers/visitors to **take action**. From the SOPA blackout to the Internet Slowdown, we've shown time and time again that when the Internet comes together, we can stop censorship and corruption."
The protest organizers, which include activism groups like Fight for the Future and Demand Progress, have suggestions for these alarm-sounding measures that include everything from in-app push notifications and letter-sending website prompts to profile pic alternatives for Facebook users to deploy. Some companies, like voice chat app Discord and publishing platform Medium, have already confirmed they'll be using in-app alerts and other means to send the message out.

Alarming Percentage of Employees Hide Security Incidents: Report

http://www.securityweek.com/alarming-percentage-employees-hide-security-incidents-report
The human factor, also often known as the insider threat, has long been known but rarely quantified. Kaspersky Lab has attempted to do just that - to answer the question, 'What role do employees play in a business's fight against cybercrime?' Kaspersky used the B2B International market research company to query 5,000 businesses around the globe; and the results are alarming. "Fifty-two percent of businesses admit that employees are their biggest weakness in IT security, with their careless actions putting business IT security strategy at risk," explains the Kaspersky report.

The extent of the issue is illustrated by the top three vulnerability concerns all being related to the human factor or employee behavior: inappropriate sharing (47%); data on lost mobile devices (46%); and inappropriate use of IT resources (44%). The supply chain, increasingly used by advanced hackers as an entry point, figures fourth at 43%. This concern is verified by actual cybersecurity incidents. "Among the businesses that faced cybersecurity incidents in the past 12 months, one-in-ten (11%) [of] the most serious types of incidents involved careless employees," states the report. This is second only to incidents involving malware, standing at 23%.

Even here, however, the human factor is important. Forty-nine percent of businesses reported being attacked by malware this year (an increase of 11% over last year). The top contributing factors behind the reported incidents are all human factors: careless/uninformed employees (53%); accidental loss of hardware (38%); and phishing/social engineering (36%). The more dangerous targeted attacks are also increasing, with 27% of businesses reporting incidents (up 6% on the previous year). *"Of these attacked businesses, over a quarter (28%) believe phishing/ social engineering contributed to the attack," notes the report*. Here Kaspersky makes an additional point: it isn't enough to simply increase social engineering and phishing awareness, it is also important to create an environment in which employees are willing to own up to errors. Kaspersky calls this the 'hide and seek' problem: employees sometimes hide their mistake leaving the business to seek the source of the problem.

"Employees," the report explains, "don't always take action when their company is hit by a security incident. In fact, in 40% of businesses around the world, employees hide an incident when it happens." This tendency varies by size of company: as low as 29% of very small businesses; at 42% of SMBs; and as high as 45% of enterprises with more than 1,000 employees. Kaspersky warns against a big stick approach to this problem. "If employees are hiding incidents, there must be a reason why. In some cases, companies introduce strict, but unclear rules and impose extra responsibility on employees, warning them not to do this or that, or they will be held responsible if something goes wrong. Such policies only foster fears, and leave employees with just one option - to avoid punishment whatever it takes."

BYOD is another area where the human factor continues to cause concern. "Almost half (48%) of businesses overall," says Kaspersky, "are worried about employees inappropriately sharing company data via the mobile devices that they bring to work." This is a particular concern for small businesses, where it rises to 57%. *The concern is justified in practice: according to the research, more than half (54%) of businesses have had data exposed because employees have lost devices*.

Kaspersky warns that policy alone is not enough to defend against the human factor. "A policy, alone, will not protect a business from threats - partly because IT security policies are not always followed by the staff that they are designed for, and partly because they cannot cover every possible risk." In fact, 44% of respondents admitted that employees simply do not properly follow policy. *Kaspersky's solution is to find the right balance of policy and engagement: policy to define correct behavior; and engagement to make employees want to follow policy. "**Staff training is essential in raising awareness** among personnel and motivating them to pay attention to cyberthreats and countermeasures - even if they are not part of their specific job responsibilities. Installing updates, ensuring that anti-malware protection is on, and managing personal passwords properly shouldn't always be at the bottom of an employee's to-do list."*

CopyCat Malware Infects 14M Android Devices, Steals Credits for App Downloads

https://www.scmagazine.com/copycat-malware-infects-14m-android-devices-steals-credits-for-app-downloads/article/673361/

A mobile malware that roots Android devices and commits both ad and app fraud has infected at least 14 million devices, at one point raking in $1.5 million during a peak two-month period in 2016, Check Point Software Technologies has reported. *Dubbed CopyCat, the malware is the first known adware that injects its code into Zygote, a daemon tasked with launching apps on Android devices. This dangerous technique gives the malware an extremely strong foothold on affected devices, allowing it to infiltrate the activity of all running apps*, Check Point explained in a blog post and accompanying technical report.

Significantly, *CopyCat steals credits earned by legitimate advertisers whenever one of their ads results in an application download*. *The malware accomplishes this by swapping out the ad company's real referrer ID with a fraudulent one. These credits are ultimately exchanged for revenue*. According to Check Point researcher Daniel Padon, this technique has never been seen before, and is more lucrative than traditional ad fraud.

"There are many efforts by ad networks to detect and stop fraud from happening and this is actually a... way to do it without being detected," said Padon, in an interview with SC Media. "You have to be on the device itself [and monitoring] device activity to understand that fraud has actually taken place." Otherwise, the ad transaction "will look like a legitimate one from end to end." *CopyCat specifically scams Tune, a mobile analytics platform that tracks advertisements that result in a viewer downloading an app*. According to Check Point's blog post, when an infected user visits Google Play, "CopyCat retrieves the package name of the app that the user is viewing on Google Play, and sends it to its command and control server. The server sends back a referrer ID suited for the package name. *This referrer ID belongs to the creators of the malware, and will later be used to make sure the revenue for the installation is credited to them*. CopyCat blocks all install_referrer intents and replaces them with its own referrer ID, which was received from the command and control server previously."

Victims of Copycat were infected by downloading malicious apps distributed by third-party stores unaffiliated with Google Play. Upon reporting CopyCat to Google in March 2017, Check Point learned from Google that the company had been aware of the campaign and had already taken steps to curtail its damage. Consequently, there are now fewer current infected devices than there were during CopyCat's two month peak period from April to May 2016, when it generated the vast majority of its revenue. (The earliest evidence of CopyCat traces back to March 2016, said Padon.)

"CopyCat is a variant of a broader malware family that we've been tracking since 2015," a Google spokesperson told SC Media in an emailed statement. "Each time a new variant appears, we update our detection systems to protect our users. Play Protect secures users from the family, and any apps that may have been infected with CopyCat were not distributed via Play. As always, we appreciate researchers' efforts to help keep users safe."

The 14 million devices found infected by CopyCat are all linked to one command and control server, meaning there could be additional C&Cs linked to millions more victims. Of this lot, 55 percent of devices are based in Asia, with a heavy concentration in the Southeast Asia region, including India (3.84 million infections), Pakistan (1.06 million), Bangladesh (1.03) and Indonesia (1.01 million). Africa saw 18 percent of infections and *the Americas experienced 12 percent, with 280,000 infections in the U.S*. Eight million of the infected devices, or about 54 percent, were successfully rooted, an usually high share, Check Point noted.

In addition to stealing credits for app downloads, CopyCat also makes money by fraudulently delivering ads and downloading apps. Of the 14 million phones infected with the malware, 4.9 million were made to serve up apps, 4.4 million stole credits for app downloads and 3.8 million issued ads to their owners, Check Point reported. The app fraud activity generated $735,000 in ill-gotten revenues, while the credit stealing activity yielded at least $660,000 by very conservative estimates. The ad fraud activity has been responsible for displaying around 100 million ads, collectively worth around $120,000.

Regarding attribution, Check Point said that its researchers found some notable links between CopyCat and MobiSummer, an ad network based in China. For instance, the malware contains code signed by MobiSummer and uses remote services created by the ad network. Also, the two entities share a common server. While previous adware campaigns have been linked to Chinese online ad companies, it is also possible that CopyCat's authors could have simply borrowed MobiSummer's various assets without permission.

POS Malware Steals Card Data, Maybe Fingerprints, from Workplace Food Kiosks

https://www.scmagazine.com/pos-malware-steals-card-data-maybe-fingerprints-from-workplace-food-kiosks/article/673798/

Avanti Markets, a leading "micro market" vending company, has suffered *a malware attack that allowed adversaries to steal payment and possibly fingerprint data from customers who used its self-service payment kiosks to purchase goods in various corporate workspaces*. According to an online statement from Avanti, the company on July 4 discovered a "sophisticated malware attack" that affected kiosks at some, but not all, micro market locations. Stolen data may include the full names, card numbers and expiration dates of credit and debit card users, the names and possibly email addresses of Market Card pre-paid card users, *and potentially the biometric information of customers who used the kiosks' fingerprint-based verification technology to authorize a purchase*.

Security expert Brian Krebs reported in a blog post over the weekend that *hackers specifically breached the internal networks of Tukwila, Wash.-based Avanti and subsequently pushed out the malicious software to the kiosks*. Krebs also referenced a July 7 blog post from RiskAnalytics, whose analysts

found that *a client's break room vending kiosks from Avanti were infected by what appears to be the POS malware PoSeidon (aka FindPOS). RiskAnalytics made this assessment based on malicious traffic patterns and specifically the discovery of a SSL certificate linked to this malware family*.
According to the Avanti website, the company operates micro markets in 46 states, serving 200 million products annually to 1.6 million customers. Avanti said that in response to the incident, it has taken steps to secure its internal systems, shut down payment processing at some locations, begun removing malware from infected systems, hired a forensic investigation firm and contacted the FBI and other authorities. The company said it will attempt to identify victims and offer credit monitoring and other helpful services to affected individuals.

FBI-DHS "Amber" Alert Warns Energy Industry of Attacks on Nuke Plant Operators

https://arstechnica.com/security/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/
The Department of Homeland Security and FBI have issued *a joint report providing details of malware attacks targeting employees of companies that operate nuclear power plants in the US, including the Wolf Creek Nuclear Operating Corporation*, *The New York Times* reports. *The attacks have been taking place since May*, as detailed in the report issued by federal officials last week and sent out to industry.
The "amber" alert to industry - the second-highest level of severity for these types of reports from the FBI and DHS - noted that the attacks had been focused on employees' personal computers but had not managed to jump to control systems. *Administrative computers and reactor control systems in most cases are operated separately, and the control networks are generally "air-gapped" - kept disconnected from networks that attach to the Internet*.
There is no evidence that information on plant operations was exposed. *FBI and DHS analysts have not been able to determine the nature of the malware planted by the attempted hacks, which used a "spear-phishing" campaign targeting senior industrial control engineers at nuclear facilities*. The tailored e-mails contained fake résumés and appeared to be from people seeking control engineering jobs, according to the report seen by the *Times*.
While nuclear power plant industrial controls are "air-gapped," that doesn't necessarily mean that they are secure. A 2015 study by the British think-tank Chatham House found nuclear control systems to be "insecure by design" and vulnerable to attack. Some did not keep control systems isolated from administrative networks connected to the Internet, and *others were vulnerable despite air-gaps because of the heavy use of USB thumb drives to move data and install software updates. Many of these systems run on older operating systems that are not regularly updated*.
While the report gave no indication of the source of the attack, unnamed sources cited by the *Times* said that the attacks are similar in approach to those staged over the past five years by a "threat group" known by some researchers as "Energetic Bear" - a Russia-based campaign against energy sector targets. In those attacks, the malware implanted by the malicious e-mail attachments specifically targeted industrial control systems. These attacks follow a much broader cyber-espionage campaign against critical infrastructure companies earlier this year. In April, the DHS warned of ongoing cyber-attacks on the energy sector as a whole, as well as healthcare, information technology, telecommunications, and infrastructure industries. Those attacks used Redleaves and other malware focused on stealing user credentials and providing a persistent backdoor to networks.

Is It Safer to Use an App or a Browser for Banking?

https://www.theguardian.com/technology/askjack/2017/jun/22/is-it-safer-to-use-an-app-or-a-browser-for-banking
[A Great Question from The Guardian's "Ask Jack" – Jack Schofield's column] Irene wants to know why she should use a banking app instead of logging into her bank accounts with the Edge browser in Windows 10. Which one would be more secure?
Jack's response: Over the past five years or so, I feel the consensus has changed to using apps. However, it depends on the devices, banking software and browsers, what else is loaded on the device (either knowingly or not), and the communications network. Browsers are risky because there are trojans designed to collect banking information. Apps are risky because most banking apps probably have security flaws, and because fake/malware apps sometimes appear in app stores.
If you are a careful user with a secure PC, and if you only use it on your secure home network, you should not have any problems. However, if you want to perform banking transactions from wherever you happen to be, without taking too many precautions, then it should be safest to use an app over 3G/LTE

(turn off Wi-Fi and Bluetooth). Systems that use two-factor authentication, preferably with a separate device that generates new passwords on demand, are really the way to go.

What is an app? ....When Microsoft redesigned Windows 8 to run on tablets and smartphones, it introduced a similar subsystem for apps. This enabled Windows to run sandboxed apps installed by the Windows Store. These apps are much safer than the old programs, because there are limits to what they are allowed to do. ..The Edge browser in Windows 10 is a new sandboxed app, so it's much better for banking than Internet Explorer. Otherwise, Chrome is the most secure alternative, because it runs in Google's own strong sandbox. Some security companies also provide add-ons, such as Kaspersky Safe Money and Bitdefender Safepay. The browsers on smartphones and tablets are also sandboxed, but like their desktop counterparts, they may be at risk from phishing and "man-in-the-middle" attacks.

Compromised devices

The biggest threat to banking security comes from using a compromised device: one with malware that captures logons etc and sends them to someone else without your knowledge. On Windows, the main banking malware comprises trojans such as "Zeus and its variants Neverquest and Gozi". Zeus has been around since 2007. *Zeus is usually delivered as an email attachment with a text that persuades some users to click on it [phishing!!]. It may say your bank or email account has been hacked and that you need to log on to confirm or change your password, etc*. Zeus collects your logon details, or puts up a fake screen that mimics a legitimate website, or redirects you to a fake website. The malware captures your keystrokes as you try to log into your bank. *Variants such as Gozi can even imitate your typing style and mouse movements, to defeat banks that use this kind of information to identify real users*. *Banking trojans can also be hidden in Microsoft Word documents, pdfs or fake invoices. Some are distributed as "drive by" installations from websites that host exploit kits*.

Smartphones and tablets are more likely to be compromised by fake or lookalike apps that have evaded the vetting process. Sometimes, devices are compromised by apparently simple apps that demand loads of "permissions" to run.

Insecure banking apps. Banking apps ought to be more secure than browsers, but it ain't necessarily so. In 2014, Ariel Sanchez *tested 40 home banking apps and found that 90% included insecure links (ones that didn't use SSL), 40% didn't check the validity of SSL certificates, 50% were vulnerable to cross-site scripting, and 40% were vulnerable to man in the middle attacks*. In a typical hack, the user might get a message to say that their session or password had expired and they needed to retype their user name and password. (Don't.) *Today's banking apps should be much more secure, but I wouldn't bet on it*.

Compromised networks. *If you use public hotspots, your communications could be monitored, or you could mistakenly log on to a copycat hotspot run from a nearby PC*. It's not always easy to identify the correct network for a coffee bar, hotel or airport. These networks make you potentially vulnerable to monitoring and "man in the middle" attacks. In fact, someone may be able to hijack an account without knowing your name or your password. ..*Whatever device you are using, the best solution is end-to-end encryption, shown by "https" addresses and a padlock in the browser. The whole of e-commerce – and e-government – is totally dependent on encryption, which is why it's insane to think about banning it*.

Secure booting and SSL. Online banking depends on secure booting and secure communications. The secure booting system tries to ensure that the device starts in an uncompromised state. To do this, it uses secure hardware on the device that uses cryptography to verify the bootloader code, which uses cryptography to verify the secure loading of the operating system. *This is built into smartphones and tablets. If buying a Windows PC, choose one with a UEFI system that securely boots Windows 10. The secure chain is broken when people use exploits to "jailbreak" devices. Banking systems should detect and block them, but 90% of Sanchez's 40 home banking apps didn't*.

Once the device is running, it must connect to your bank via an SSL/https connection, though it may not be easy to tell if does. (I assume that 3G and LTE mobile connections are secure enough.) The simplest solution is to install the EFF's "HTTPS Everywhere" extension in Chrome, Firefox or Opera. Not every website supports https, but if not, the extension should redirect you to the unencrypted site.

You can increase your banking security in Windows 10 by keeping one browser for financial transactions and never using it for anything else. *Also, either use a private browsing/incognito mode or delete all caches and cookies after use. Indeed, you could use a separate standard user account (not an administrator account) for financial transactions. Switching between accounts isn't arduous nowadays, and you can leave your original account open while you do it*.

Going even further, you could keep a password protected Apple iPad at home for banking. Do not download any other apps and, out of the box, that's one of the most secure home systems you can get. Government security services could hack you, but it's unlikely that they would. [Thanks Jack! Lots of security awareness info to consider]

Massive WWE Leak Exposes 3 Million Wrestling Fans' Addresses, Ethnicities And More

https://www.forbes.com/sites/thomasbrewster/2017/07/06/massive-wwe-leak-exposes-3-million-wrestling-fans-addresses-ethnicities-and-more/#4e0c1c5975dd

WWE [World Wrestling Entertainment] fans take note: an IT error may have left your personal information open to anyone, including addresses, educational background, earnings and ethnicity. Earlier this week, *Bob Dyachenko, from security firm Kromtech, told Forbes he'd uncovered a huge, unprotected WWE database containing information on more than 3 million users, noting it was open to anyone who knew the web address to search. Looking at samples of the leaked information provided by Dyachenko, all data was stored in plain text*. The data - which also included home and email addresses, birthdates, as well as customers' children's age ranges and genders where supplied - was sitting on an Amazon Web Services S3 server without username or password protection, Dyachenko said. *It's likely the database was misconfigured by WWE or an IT partner as in other recent leaks on Amazon-hosted infrastructure*. WWE said it was investigating.

It's unclear what branch of the WWE Corporation the database came from, though Dyachenko suspects it belonged to one of its many marketing teams, given it was accompanied by reams of social media tracking data, including posts from superstars and fans. The kinds of data in the leak are the same as those in the account details section for customers of the WWE Network, a subscription-based video streaming service for wrestling events. ..Shortly after WWE was alerted to the leak by Dyachenko on July 4, the company moved swiftly to remove them from the web, making them inaccessible. "Although no credit card or password information was included, and therefore not at risk, WWE is investigating a potential vulnerability of a database housed on a third party platform," a spokesperson from the wrestling giant said. "*In today's data-driven world, large companies store information on third party platforms, and unfortunately have been subject to similar vulnerabilities*. WWE utilizes leading cybersecurity firms to proactively protect our customer data." WWE didn't say where the information came from or how long the database was open on Amazon. The spokesperson said the firm was working with "a leading cybersecurity firm" to determine the cause of the leak.

…Joseph Lorenzo Hall, chief technologist at the Center for Democracy & Technology called on Amazon to do more for those leaving data open on its cloud servers. "It's unfortunate Amazon doesn't have a 'neighborhood patrol' of sorts for S3 that checks for open buckets with sensitive data - jiggling the locks, checking for apparent misconfigurations - and then takes them offline." Amazon hadn't responded to a request for comment at the time of publication.

Multiple leaks have occurred on Amazon in recent months, largely thanks to misconfigurations of servers. The most notable was that of a Republican Party marketing contractor that left data on more than 198 million voters on an open database in June. In that case the information appeared to be amassed from a wide range of sources, and included addresses, birthdates, phone numbers and sentiment analyses for predicting individuals' opinions, religion and ethnicity.

66% of US Law Firms Reported a Breach in 2016

https://www.helpnetsecurity.com/2017/07/06/law-firms-data-breach/

The majority of US-based law firms are not only exposed in a wide variety of areas, but in many cases, unaware of intrusion attempts. These findings were based on Logicforce survey data from over 200 law firms, anonymous system monitoring data and results from their on-site assessments. The degree of preparation and vigilance within the industry at large will continue to place many law firms at unnecessary risk of losing valuable client data such as trade secrets and intellectual property. Such breakdowns in security could result in financial losses for the targeted firms and their clients. Approximately 40% of law firms in the study underwent at least one client data security audit, and Logicforce predicts this will rise to 60% by the end of 2018. Key findings: An average of 10,000 intrusions occur every day at law firms. Both large and small firms are equally at risk of being hacked. 95% of assessed law firms were not compliant with their own data security policies and 100% were not compliant with those of their clients. 40% of firms were breached without knowing it in 2016.

“Ultimately law firms don’t have the resources or enough expertise to take on their security alone and we want to illustrate the areas where there needs to be more focus. We need to effectuate a shift in thinking from ‘it won’t happen to me’ to ‘it will happen to me’, and until that happens, cybersecurity will never be given the level of attention it deserves,” said John Sweeney, President at Logicforce.

NATO will Respond with ‘Conventional Military Assaults’ to Future Cyber Attacks

http://securityaffairs.co/wordpress/60852/cyber-warfare-2/nato-article-5.html

NATO has warned that in the future any cyber attack against a member state could trigger a military response according to the alliance’s Article 5, mutual defence clause. The NATO announcement follows the massive NotPetya ransomware-based attacks that hit systems worldwide with most of them in Ukraine. The Petya ransomware hit systems in several industries, including banks, transport, telecommunications, and energy. Among the hardest hit were Ukr telecom, Dniproenergo, Ukrzaliznytsia, Kiev-Boryspil Airport, and the Cabinet of Ministers of Ukraine. Popular aircraft manufacturer Antonov was also reportedly hit. ..The malware infected over 12,000 devices in around 65 countries, the malicious code hit major industries and critical infrastructure.

Experts from NATO CCD COE believe the attack was likely launched by a nation-state actor, or it was commissioned to a non-state actor by a state. The attackers were well funded and the attack they conducted was very complex and expensive. The experts observed that despite the operation was complex, the attackers did not spend much effort for managing the payments, *a circumstance that suggests hackers were not financially motivated*. ..This declaration could have serious consequences, the cyber attack could be interpreted as an act of war, and can trigger a military response of the alliance under the Article 5 of the North Atlantic Treaty, the principal of collective defense. According to the NATO secretary-general Jens Stoltenberg, NATO is threatening to respond to cyber-attacks against member states with a conventional military strike. Stoltenberg highlighted that NATO leaders officially recognized the cyberspace as the fifth domain of a warfare so the alliance could respond with conventional weapons in case of a powerful cyber attack.

M.E.Doc Software Was Backdoored 3 Times, Servers Left Without Updates Since 2013

https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/

[July6] Servers and infrastructure belonging to Intellect Service, the company behind the M.E.Doc accounting software, were grossly mismanaged, being left without updates since 2013, and getting backdoored on three separate occasions during the past three months. The information comes from several security researchers that have analyzed the servers, but also from Ukrainian authorities, who on Tuesday, two days ago, seized the company's servers.

Attackers gained access to M.E.Doc via employee login. One of the most credible sources for this information is Cisco, who sent on-the-ground experts to analyze the M.E.Doc servers, the origin point of the NotPetya ransomware outbreak. *In a report released last night, Cisco experts say that the NotPetya group - suspected to be a cyber-espionage group named TeleBots - had infiltrated the company's infrastructure by gaining access to an employee's credentials*. Cisco says the NotPetya gang used these credentials to embed a backdoor in the M.E.Doc software package, but also place a PHP webshell on the company's web server.

NotPetya group inserts backdoor in M.E.Doc software. The M.E.Doc software backdoor was hidden in a file named "ZvitPublishedObjects.dll," part of the M.E.Doc software installation/update package. ESET has an in-depth report on how this backdoor works. Both ESET and Cisco confirmed that the TeleBots crew shipped this backdoor part of three M.E.Doc software updates, on three separate occasions. ..The backdoor in the code allowed attackers to execute code on computers where M.E.Doc was installed, which is how they sent the NotPetya ransomware to users and companies that installed these booby-trapped updates. The first of these tainted M.E.Doc software updates appear to have been a test, while the second and third were used to push the XData and NotPetya ransomware.

Backdoor was very sophisticated, incredibly stealthy. According to ESET researcher Anton Cherepanov, the backdoor is very sophisticated and used a few ingenious tricks. For example, the backdoor didn't communicate with an external command-and-control server. The TeleBots (NotPetya) group hosted their C&C server right on Intellect Service's M.E.Doc update server at upd.me-doc.com[.]ua. *Furthermore, all communications with these servers were disguised as regular cookies. This allowed the*

group to hide any malicious operations as legitimate traffic that would have never caught the eye of any researcher. [go to the article for the tech details on why/how the attack evolved]

Russian Hacker Living in U.S. Sentenced to Prison

http://www.securityweek.com/russian-hacker-living-us-sentenced-prison

A Russian-born U.S. citizen has been sentenced to 110 months in prison for running a sophisticated cybercrime operation that involved botnets, stolen financial data and money laundering. Alexander Tverdokhlebov, 29, has been living in Los Angeles. He emigrated from Russia in 2007 and later obtained U.S. citizenship. According to U.S. authorities, Tverdokhlebov was an active member on several exclusive Russian-speaking cybercrime forums since at least 2008. He is said to have offered various services, including for laundering illegal proceeds.

The man also operated botnets that allowed cybercriminals to steal payment cards and other data. Investigators said Tverdokhlebov boasted about possessing 40,000 credit card numbers and controlling as many as half a million computers between 2009 and 2013. The hacker sold the stolen card data to individuals who used it to make fraudulent purchases or withdrawals from the victims' accounts. He is also said to have recruited Russian students visiting the U.S. to receive money from victims and then forward it to Tverdokhlebov and his accomplices. Authorities believe Tverdokhlebov's activities resulted in losses between $9.5 and $25 million. When he was arrested, investigators found $275,000 in cash distributed across several safety deposit boxes in Las Vegas and Los Angeles. They also seized Bitcoin and other assets valued at roughly $5 million. Tverdokhlebov pleaded guilty to wire fraud in late March and he has now been sentenced to 110 months in prison and three years of supervised release, which includes the monitoring of his computer use.

Several Russian nationals have been charged or convicted recently for cybercrimes in the United States. Yevgeniy Aleksandrovich Nikulin has been charged for hacking into the systems of LinkedIn, Dropbox and Formspring and will be extradited from the Czech Republic, two Russian Federal Security Service (FSB) officers have been indicted over the 2014 Yahoo hack, and the author of the Citadel malware recently pleaded guilty. A lengthy prison sentence was given recently to 32-year-old Roman Valeryevich Seleznev, convicted on 38 counts in relation to a point-of-sale (PoS) hacking scheme.

Authorities Shut Down Major Dark Web Child Porn Platform

https://www.hackread.com/authorities-shut-down-major-dark-web-child-porn-platform/

Law enforcement authorities in Germany have shut down a major Dark Web child pornography website known as "Elysium." The website which had around 87,000 members was a popular platform for people to exchange explicit images of children displaying physical and sexual abuse including toddlers. According to German federal police, Elysium was not a regular child abuse platform since its users also arranged meetings to abuse children physically. Elysium was run by a 39-year-old man from Hesse region of Germany while most of its visitors were from Austria and Germany. He was arrested on 12th June when his apartment was raided, and the police seized a server. The police haven't disclosed his identity. *However, the site was shut down on June 13, 2017, while several other suspects were also arrested*.

A further digging into the site by HackRead researchers discovered that Elysium was formed in November 2016 and opened in December 2016. The site was owned and operated by Noctua, Ovidius, and Scorpion. A fourth administrator account, "Elysium", was used by the other 3 administrators to post important announcements. As of now limited information has been revealed by the authorities, however, on Friday both German and Austrian authorities are expected to hold a press conference about the bust. This is the second major bust of 2017 by authorities fighting against explicit platforms. Just two months ago, the FBI arrested a man in Florida for running "Playpen," one of the biggest child porn sites on Dark Web. *The site has been shut down and the operator is now in jail for the next 30 years*. *Also, five months ago; the online hacktivist group Anonymous shut down thousands of Dark Web sites for hosting child porn*. In total over 10,000 (around 20%) websites on the Dark Web were hacked by the hacktivists. [Note: while this crime will never stop, and perpetrators will just set up other sites, it is good to know that there are continuous efforts to take down these sites, and that some of the criminals are being arrested and jailed.]

Thousands of New Zealand Airport Passengers Forced to Surrender Device Password

https://www.hackread.com/nz-airport-passengers-to-surrender-device-password/

Law enforcement authorities at airports in Israel and United States are known for asking for social media details of those visiting their countries. But it looks like New Zealand has been taking notes. According to 1 News, New Zealand has been facing a new surge of security protocols where the customs at some of New Zealand's airports forcefully ask incoming travelers to provide passwords to their digital devices as part of a security check.

All in the name of national security. According to the customs, *what has now come to be known as the **'digital strip,'** is carried out for national security reasons*. Essentially, they do so in order to prevent smugglers from entering the country. Jamie Bamford, the general manager of Intelligence Investigations Customs, stated that the examination of a passenger's device could be quick or it can take longer than that….

Taking data forcefully. *Apart from the fact that the customs sometimes copies the traveler's data and passes it onto the government agencies for further inspection, the general manager also revealed that the department has all the necessary tools to break into an individual's device if he/she refuses to provide the password*. Up till now, around 1,350 people have been subject to the digital strip since 2015 with New Zealanders accounting for the majority. That is, of the total, 296 were from New Zealand followed by 269 Chinese. The rest belonged to Taiwan. The primary airports in which it has taken place are those in Auckland, Wellington, and Christchurch. Whether this behavior is legal is a matter of debate. *The customs, however, claims that it carries out the procedures in line with New Zealand's privacy act*.

The proposal to fine those who resist. 1 News reports that the Customs has proposed a bill in which passengers who refuse to comply with the customs' requests shall be fined with a $5,000 penalty. Kennedy Graham, MP of the Green Party, says that passengers have the right to seek legal advice before they can allow the officials to pry into their digital devices. However, it all comes down to practicality as many passengers do not want to go through the hassle of engaging a lawyer for having their private data searched.

Two Hackers Arrested After a Decade of Selling Malware

https://www.hackread.com/two-hackers-arrested-after-a-decade-of-selling-malware/

Ruslan Bondars and Jurijs Martisevs were identified as the main culprits behind a crime in which they were selling malware over the dark web. The malware sold was meant to disrupt many U.S businesses. According to an indictment released by the Federal court in Alexandria, Virginia, *the two men were selling malicious software that included hacking tools to exploit vulnerabilities by creating files with malware, Remote Access Trojans to hijack a victim's computer, malware that could bypass detection from antivirus software and keyloggers which would monitor every keystroke made by a victim*. There is also an accomplice who lives in Virginia but has not yet been identified. The tools were being sold using Tor so as to avoid detection and were being sold in bulk.

What is surprising is that Bondars and Martisevs have been doing this since 2006. This implies that it is well after a decade that they have been caught. Furthermore, the FBI says that it is the first time it has come across malware which is so wide-spread and high in volume. In fact, the user base of the malware is reported to be 30,000. Although the malware was meant to intrude the systems of the major American corporations, the specific names of the victims have not been revealed. The accomplice who has not yet been found has been described as Z.S. and is alleged to be based in the Great Falls, Virginia. The accused is charged for having created the keylogger malware which has reportedly been sold to 3,000 customers to date. Also, around 16,000 systems have been infected with this keylogger in 2012 alone. ..The duo is charged with conspiracy and for committing wire fraud.

And Now, This:

Pokemon Go Turns One [on July 6th] -- and It's Not the Fad You Thought

https://www.cnet.com/news/pokemon-go-anniversary-john-hanke-niantic-interview/

One year ago today, Pokemon Go took the world by storm. *By many measures, it was the fastest growing app of all time*. One year later, is Pokemon Go dead? Was Pokemon Go a fad?

Not even close: According to developer Niantic, 65 million people play the game each month. To put that in perspective: Uber has only 40 million monthly active users. All of Blizzard's hit games - World of Warcraft, Overwatch, Hearthstone, Diablo, StarCraft and all the rest - only add up to 41 million monthly users *combined*.

You have to look at the most popular games in the world, like League of Legends (100 million), or apps as popular as Pandora (77 million) and Spotify (140 million) to understand Pokemon Go's sheer scale.

So for Pokemon Go's one-year anniversary, we thought we'd speak to the man at the eye of the storm: John Hanke, the founder and CEO of developer Niantic. [article has an edited transcript of the brief interview] **Where does this go next?** Hanke: Our focus for the duration of the summer is really around taking the gyms and raid feature we just launched and expanding on that with large events. *We have a plan for Chicago [Niantic's Pokemon Go Fest] which will allow people at the event and outside of the event to play together in interesting ways... The Pokemon Go Fest, coming July 22, will be the game's first official real-world event.*

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

****