Security News Digest
October 17, 2017

October is Cyber Security Awareness Month

Another day, another data breach…. Learn more with the
October Breaches Everywhere Quiz

Visit the Information Security Awareness - Cyber Security Awareness Month page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/cyber-security-awareness-month
The theme this year for the National campaign is “Our Shared Responsibility”.

Poor Security Blamed After School Surveillance Images Broadcast on Russian Site

http://www.cbc.ca/news/canada/nova-scotia/russian-public-stream-webcam-cape-breton-school-children-1.4351372
Security protocols on surveillance cameras at a Cape Breton school remain out of date, months after images of its students were unintentionally broadcast on the internet, Nova Scotia's privacy commissioner Catherine Tully says. Tully's report on the matter found there were "inadequate passwords and insufficient technical controls" behind the initial breach. While passwords have been changed, Tully said the school has still not placed the streams behind a firewall or equivalent protection, and two of the cameras are no longer supported by manufacturer security updates. "Security problems arise constantly, they change, people hack things in different ways, so you have to be nimble, you have to adjust your technology to adapt to those risks, and they can no longer do that with the existing cameras," she said. "Reasonable security requires that they [those cameras] be behind a firewall. The manufacturers of the camera recommend them, but they haven't done that yet."
However, on Thursday, Beth MacIsaac, superintendent of the Cape Breton-Victoria Regional School Board (CBVRSB), said all cameras in the board are behind a firewall. "We would like our parents and students to know that we take their privacy very seriously, which is why we've passworded all of our security cameras and they're now behind firewalls as well," said MacIsaac. This was news to Tully, who said the school board received an advance, embargoed copy of her report on Sept. 18. The board then asked for an extension of three weeks to respond to the report. During that time, the board did not inform Tully that the cameras were behind the firewall, but Tully said she was "delighted" to hear the board complied with the recommendation.
Tully's report follows a CBC News investigation in May that showed how insecure web cameras at Rankin School of the Narrows, in Iona, broadcast hundreds of thousands of high-definition pictures of students. One camera was pointed towards the school's yard and parking lot. …."When video surveillance images from the Rankin School were streamed on the internet for all to see, this was a violation of Nova Scotia's privacy laws. Video surveillance images of schoolchildren streaming unsecured to the internet created a risk to student safety." **The security lapse led to images ending up on the Russian-registered website insecam.org, and included images of children near washrooms, in hallways and in the schoolyard.** The cameras were only made secure after CBC News alerted the school and CBVRSB of the problem….
Recommendations. Tully has recommended several changes, including that the board: Develop a privacy breach policy, Further secure its cameras, for example, using a firewall, Provide privacy training, Disable the camera located outside the boys' washroom at Rankin School, and Replace two exterior cameras that are no longer supported by the manufacturer. She also said the board should take a look at its rationale for having the cameras in the first place. Tully said in the report that the board had not established that video surveillance is authorized under the Privacy Act.

RCMP Says Free Trial Scams are Fraudulent, but Credit Card Companies Make Victims pay

http://www.cbc.ca/news/business/marketplace-skin-cream-trials-1.4349777

Every week, *Marketplace* [CBC TV investigative reports] ….. has received hundreds of emails from viewers who've been stung by surprise credit card charges they couldn't get reversed after signing up for what they thought were "risk-free" product trials. **What they actually signed up for is an online scheme known as a subscription trap, which uses sneaky fine print and deceptive marketing techniques**, such as fake articles, bogus endorsements from respected celebrities like Ellen DeGeneres and Céline Dion and phoney surveys from legitimate companies, to trick people into paying for products and services they don't want. *Marketplace* has uncovered exactly how it works, including the motives and methods of the mysterious merchants and marketers involved; why it continues to work despite **more than 26,000 complaints to the Better Business Bureau in the last year alone**; and what credit card companies could do to stop it.

Costly terms. Judy Mayer of Aurora, Ont., is one of those Canadians who paid a steep price for signing up for what appeared to be a great offer. Mayer was on Facebook back in January when she noticed an ad for an anti-aging cream featuring an endorsement from *Dragons' Den* star Arlene Dickinson. Mayer paid the shipping in order to get the "free trial." A few months later, Mayer discovered charges totalling nearly $400 on her MasterCard. The charges were from Rejuva Essence, so she called the company's customer service line and was told that **because she hadn't cancelled her subscription and returned the original sample within 14 days, she was charged for three more bottles, as set out in the offer's terms and conditions**. "I had no idea that I was to cancel a subscription," Mayer told *Marketplace.* "They did not tell me anything about it." Mayer insists she never saw any mention of a 14-day trial period and the recurring charges when she signed up for the offer - which is precisely the goal of a subscription trap, authorities say.

When *Marketplace's* Asha Tomlinson called Rejuva Essence's customer service, she was told "once you place the order, you start the trial period. If the trial period passes and you haven't cancelled, the system believes you wish to continue your treatment." When Tomlinson pointed out those details weren't easy to find, she was told "those are the terms and the conditions" and they're outlined on the Rejuva Essence website. As with other face cream offers, details about Rejuva Essence's recurring charges and trial period are accessible only via a small, faint "Terms" hyperlink at the bottom of the page. MasterCard told Mayer it was "very aware" of these face cream companies, but there was nothing it could do because the additional charges were explained on Rejuva Essence's website. And, as *Marketplace* has learned, Mayer's experience is far from unique.

How the scam works. The scam starts with a merchant who decides to sell a product online, whether it's face cream, garcinia cambogia, weight-loss pills or teeth-whitening products. **As the U.S.-based Federal Trade Commission has pointed out, the products used in subscription traps are largely irrelevant; the primary purpose, after all, is to acquire credit card numbers.** The merchant creates a website or landing/checkout page offering free trials of, in this case, anti-aging face cream. The merchant then buries the recurring fees in the fine print of the terms and conditions. After what is usually a 14-day trial period, the customer automatically becomes enrolled in a subscription if they don't cancel, and their credit card gets billed every month, sometimes for hundreds of dollars. The merchants are constantly changing their product names to avoid bad online reviews, according to the RCMP's anti-fraud unit and the Better Business Bureau. Abella Mayfair, Image Revive, Face Replen, Hydroluxe, Chantel St Claire, Renuvica, Nuvella and Skin Balance are **just some of the 371 product names the Mounties have uncovered**. RCMP fraud investigator Jeff Thomson says the merchants will also use different bank processor names on credit card statements. He says **authorities have found more than 312 accounts linked to the scheme at 84 different banks in 14 different countries, particularly in China, Latvia, the U.S. and Canada**.

Door-to-door salespeople of the internet. But the sellers also need advertising to direct people to their offers, so **they harness the power of what's called affiliate marketing**. Sometimes referred to as the door-to-door salespeople of the internet, cost-per-action (CPA) affiliate marketers are often a creative and highly motivated bunch since they don't get paid unless you sign up for whatever offer they're pushing. *Marketplace* has found commissions for CPA affiliate marketers ranging from $30 to $50 for promoting and getting people to sign up for face cream trials. While many affiliate marketers do legitimate and ethical work for upstanding businesses, authorities say some CPA affiliate marketers use deceptive tools like fake news articles with phoney celebrity endorsements, or fake pop-up surveys that appear to come from reputable sources such as Costco, Air Canada and Rogers, to catch people in subscription traps.

….**What does the law say?** There are laws on the books that, at least in theory, should protect

Canadians from subscription traps. Sections 74.01 and 52 of the Competition Act outlaw misleading advertising, which can include deceptive marketing as well as "recurring charges" in the terms and conditions. In the case of face cream trials, it's misleading for consumers to see the word "free" everywhere and then discover there are hidden charges - the overall impression is the offer is for a free trial. In these kinds of subscription traps, both the merchant and the affiliate marketer can be held responsible; the merchant for hiding the charges and the affiliate marketer for creating misleading advertising. But Barry Elliott of the RCMP's anti-fraud unit says finding and policing those merchants and marketers is no easy task….

Role of credit card companies. Compounding the frustration for victims is the fact credit companies rarely reverse the charges. Most of the consumers who contacted *Marketplace* about the scam, including Mayer, failed to get their money back. [see article for more]

B.C. Casinos Knowingly Accepted 'Banned' Cash: Report

http://www.timescolonist.com/news/b-c/b-c-casinos-knowingly-accepted-banned-cash-report-1.23065455

River Rock Casino in Richmond knowingly accepted millions in suspicious cash that was provided to VIP gamblers by lenders who were banned from B.C. casinos, an internal audit obtained by Postmedia News alleges. The June 2016 audit by the B.C. gaming policy and enforcement branch suggests that River Rock staff in 2015, for some reason, allowed high-rollers to buy chips with funds from Richmond private lenders who were under B.C. Lottery Corp. anti-money-laundering restrictions and who were subject of a major RCMP investigation.

The audit and other enforcement branch documents, obtained by Postmedia through freedom of information requests, also conclude that banned high-rollers used "proxy" bettors in schemes to skirt anti-money-laundering measures. Also, a review of play at high-limit tables at River Rock concluded a money-laundering process known as "refining" - which may allow gamblers to buy chips with wads of street-cash $20 bills and cash out with neat bundles of $100 bills suitable for banking - was believed to be occurring, even though casino staff had measures in place to block these transactions.

The June 2016 audit of "provincially banned cash facilitators" asserts that, in 2015, three B.C. casinos allowed gamblers to purchase chips with $6.7 million from illegitimate lenders. River Rock Casino accepted $5.37 million of that total - or 79 per cent. "Sites knowingly accepted cash that they acknowledged was obtained from questionable sources," documents say. "Industry indicators of suspicious activity were present in all incidents in which the cage accepted the cash." Sonja Mandic, spokeswoman for River Rock Casino operator Great Canadian Gaming Corp., referred all questions for this story to the B.C. Lottery Corp.

"As part of our commitment to continuous improvement, we will be undertaking a review of this matter to determine if further direction is required," BCLC spokeswoman Laura Piva-Babcock said. Edgewater Casino in Vancouver accepted $700,000 in cash from banned individuals, and Starlight Casino in New Westminster accepted $690,000, the audit says. Most of the $6.7 million in cash from banned individuals was in $20 bills.

The findings shed more light on processes within B.C. casinos that may have allowed casino money-laundering, as alleged in an RCMP probe. Postmedia News has reported that investigators believe organized criminals loaned suspected drug cash from an illegal cash house in Richmond to VIP high-rollers recruited from Macau. These "whale" gamblers could pay back the loans in China through an alleged underground banking network, thus avoiding China's tight capital-export controls and ending up with cash to invest in Canada. The reason for the cash audit, documents say, "was to determine if any of the individuals identified on the alleged fugitive list are gambling … The scope was to quantify the dollar amount of buy-ins conducted at casinos from cash sites … obtained/connected to individuals provincially banned for cash facilitation." [article has more details on the money laundering operations]

Drone Strikes Commercial Aircraft in Quebec: Garneau

http://www.ctvnews.ca/canada/drone-strikes-commercial-aircraft-in-quebec-garneau-1.3633035

A Skyjet flight heading to Quebec City's Jean Lesage International Airport was struck by a drone on Oct. 12, according to Minister of Transport Marc Garneau. Emergency measures were immediately put in place and the plane was able to land safely. No injuries were reported.

"This should not have happened," Garneau told reporters Sunday. "The drone should not have been there." "It is important to point out aircraft are particularly vulnerable when they are coming in [for landing] … and during take-off," he added. Garneau issued a written statement earlier Sunday in which he said

the incident was the first time a drone has hit a commercial aircraft in Canada. "I am extremely relieved that the aircraft only sustained minor damage and was able to land safely," he added.
Transport Canada advises that drones should be flown below 90 metres and at least 5.5 kilometres away from any airport, seaplane base or areas where aircraft take-off and land.
Thursday's collision reportedly happened about three kilometres from the airport at an altitude of 450 metres. "Transport Canada is monitoring the situation and is in contact with its transportation partners including Skyjet, the Jean Lesage International Airport and NAV CANADA. My department is in contact with the Service de police de la Ville de Québec and we will cooperate with the Transportation Safety Board should they decide to investigate," Garneau said.
Garneau introduced interim safety measures regarding drone flights earlier this year, which restrict where recreational drones can be flown. Final regulations regarding drone usage will be in place in 2018, says Garneau. "I would like to remind drone operators that endangering the safety of an aircraft is extremely dangerous and a serious offence," he said. Penalties for violating these safety measures include fines of up to $25,000 and possible face jail time. Anyone who wishes to operate a drone is required to follow the Canadian Aviation Regulations. There have been 1,596 drone incidents reported in 2017, of which 131 were deemed an "aviation safety concern," Garneau said in the statement.

Flaw Lets Hackers Read Data Over Secure Wi-Fi [KRACK Attack]

http://www.cbc.ca/news/technology/wifi-flaw-wpa2-1.4356404

The U.S. Department of Homeland Security on Monday warned of cyber risks associated with a widely used system for securing Wi-Fi communications after Belgian researchers discovered a flaw that could allow hackers to read information thought to be encrypted, or infect websites with malware. The alert from the DHS Computer Emergency Response Team said **the flaw could be used within range of Wi-Fi using the WPA2 protocol to hijack private communications**. It recommended installing vendor updates on affected products, such as routers provided by Cisco Systems Inc or Juniper Networks Inc.
Belgian Researchers Mathy Vanhoef and Frank Piessens of Belgian university KU Leuven disclosed the bug in the WPA2 protocol, which secures modern Wi-Fi systems used by vendors for wireless communications between mobile phones, laptops and other connected devices with internet-connected routers or hot spots. "If your device supports Wi-Fi, it is most likely affected," they said on a website, www.krackattacks.com, that they set up to provide technical information about the flaw and methods for attacking vulnerable devices. It was not immediately clear how difficult it would be for hackers to exploit the bug, or if the vulnerability has previously been used to launch any attacks.
The Wi-Fi Alliance, an industry group that represents hundreds of Wi-Fi technology companies, said the issue "could be resolved through a straightforward software update." The group said in a statement it had advised members to quickly release patches and recommended that consumers quickly install those security updates.

Vendors Race to Fight KRACK Wi-Fi Attacks

http://www.securityweek.com/vendors-race-fight-krack-wi-fi-attacks

Technology companies worldwide have released or are working on releasing patches to address the dangerous Wi-Fi vulnerabilities publicly disclosed this week. Setting the stage for a new attack method called Key Reinstallation Attack, or **KRACK**, these vulnerabilities affect the Wi-Fi standard itself and potentially expose all Wi-Fi Protected Access II (WPA2) protocol implementations. An attacker capable of exploiting the issues could steal sensitive information transmitted over Wi-Fi, including credit card numbers, passwords, chat messages, emails, photos, and more. All major operating systems, including Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others, are affected.
The good news, however, is that the attacker needs to be in within range of an affected wireless access point, and that only data encrypted using the WPA2 protocol is exposed. Data encrypted using other standards, including HTTPS, TLS, and the like, should be safe from this attack. What's more, **the Wi-Fi Alliance says that there is no evidence that the vulnerabilities have been exploited maliciously and confirmed that a straightforward software update should resolve them**. However, the industry organization has already released a vulnerability detection tool for use by any Wi-Fi Alliance member.
As the US-CERT noted in its advisory, the issues affect the Wi-Fi standard itself, meaning that all correct implementations are exposed. Thus, there's a general consensus of urgency among top vendors to address the bug through software updates, and some of them have already released patches. Microsoft

has already addressed the issue its October 2017 patches and published an advisory on the matter. Apple is reportedly taking steps in this direction by including patches in the latest beta releases of macOS, iOS, tvOS, and watchOS. Android 6.0 and above and Linux were said to be affected the most, with the attack being "exceptionally devastating" against them. While security updates have been released for Linux, Google seems determined to address the issue in the coming weeks, most likely with the November 2017 monthly Android patches.
The issue is being addressed in Debian, Fedora, Red Hat, and Ubuntu. Patches are available for OpenBSD as well, and are being prepared for the FreeBSD Project. Intel has released an advisory listing all affected products, while Netgear has released fixes for some products and is working on updates for others. Cisco too has released patches for affected products, the same as Fortinet, MikroTik, Ubiquiti Networks, WatchGuard, and Aruba. Zyxel also confirmed that some of its products are affected. The list of affected and potentially affected vendors is much more extensive than that, as US-CERT has revealed. Most of the vendors were notified of the vulnerabilities in late August, but it's yet unclear how many of them are affected.

New Android Ransomware Permanently Changes PIN, Demands Ransom

https://www.hackread.com/new-android-ransomware-permanently-changes-pin-demand-ransom/

DoubleLocker - ESET's security researchers have identified a new kind of ransomware, which infects Android devices by using a technique that so far was used by Trojans. It not only encrypts your mobile phone but also modified its PIN. The ransomware has been named DoubleLocker because it performs a two-way action to lock the phone, that is, it encrypts all the files and changes the PIN as well so that victims run out of options and give in to the ransom demands of hackers. **The ransomware is being distributed as a fake update of Adobe Flash while compromised websites are being used to spread it.** When DoubleLocker is downloaded on your device, the fake Adobe Flash app requests Google Play Services activation because it needs to exploit the phone's accessibility services. This particular option is present for disabled people so that they could easily use their phones.
It must be noted that the tactic of abusing accessibility services was used previously by Android data-stealing Trojans and it is the very first time that some cybercriminals have employed this approach on ransomware. DoubleLocker then starts exploiting the permissions by retrieving Windows content, enabling advanced web accessibility for installation of scripts and monitoring the text that the victim types. **When permissions are granted, the ransomware is installed as the default Home app. This means when the user will visit Home screen the next time the ransom note will be there.** According to ESET's malware researcher Lukáš Štefanko, the default Home app is a launcher and is present to enhance the persistence of the malware. The user believes the malware to be default Android launcher, which is the software that controls the appearance of the device, as well as the way apps and widgets, are launched. It also is responsible for creating invisible shortcuts to self-activate when the victim clicks on Home button, and this is how the device gets locked. It happens every time the victim tries to use the mobile's Home screen.
The two ways in which DoubleLocker attempts to lock the phone include encryption of the files stored on the device and changing the PIN of the device. It encrypts data using the AES encryption algorithm through ".cryeye" extension. The encryption is highly effective, and without the decryption key, it becomes impossible to unlock the files. On the other hand, the PIN is changed effectively by setting it to a random number, which even the attackers do not store. This means, recovering access to the device is not possible. The PIN is then reset after the ransom has been paid and the device is unlocked. Attackers give 24 hours deadline to the victims for payment of ransom.
It is worth noting that hackers are demanding 0.0130 bitcoins (approx. $73) as ransom, which is a comparatively low figure if we observe what other ransomware schemes are demanding. However, it is quite possible that hackers have set the ransom amount low deliberately so that victims easily pay the ransom to regain access to their device. **The only option victims have if they don't want to pay ransom amount, is to run factory reset. This will fully format the phone, and all the data that is not backed up will be permanently deleted.** The chances that the rooted phone can successfully get past the PIN without needing to be reset are not bright. It can only happen if the device had to debug mode on before the installation of ransomware. In that case, it is possible to remove the system file through accessing Android Debug Bridge (ADB) as this is where the PIN is stored. This would allow the user to reset the device manually. However, we suggest that it is better to avoid installing apps and software from third-party websites and only choose reliable, authentic platforms. DoubleLocker is a dangerous

threat to all Android devices since it doesn't need a rooted phone to run its code and it can effectively affect the phone rendering it useless unless the victim pays the ransom.

Hackers Use New Flash Zero-Day Exploit to Distribute FinFisher Spyware

https://thehackernews.com/2017/10/flash-player-zero-day.html

FinSpy - the infamous surveillance malware is back and infecting high-profile targets using a new Adobe Flash zero-day exploit delivered through Microsoft Office documents. Security researchers from Kaspersky Labs have discovered a new zero-day remote code execution vulnerability in Adobe Flash, which was being actively exploited in the wild by a group of advanced persistent threat actors, known as **BlackOasis**. The critical type confusion vulnerability, tracked as CVE-2017-11292, could lead to code execution and affects Flash Player 21.0.0.226 for major operating systems including Windows, Macintosh, Linux and Chrome OS.

Researchers say BlackOasis is the same group of attackers which were also responsible for exploiting another zero-day vulnerability (CVE-2017-8759) discovered by FireEye researchers in September 2017. Also, the final FinSpy payload in the current attacks exploiting Flash zero-day (CVE-2017-11292) shares the same command and control (C&C) server as the payload used with CVE-2017-8759 (which is Windows .NET Framework remote code execution). So far BlackOasis has targeted victims in various countries including Russia, Iraq, Afghanistan, Nigeria, Libya, Jordan, Tunisia, Saudi Arabia, Iran, the Netherlands, Bahrain, United Kingdom and Angola.

The newly reported Flash zero-day exploit is at least the 5th zero-day that BlackOasis group exploited since June 2015. **The zero-day exploit is delivered through Microsoft Office documents, particularly Word, attached to a spam email, and embedded within the Word file includes an ActiveX object which contains the Flash exploit.** The exploit deploys the FinSpy commercial malware as the attack's final payload.

"The Flash object contains an ActionScript which is responsible for extracting the exploit using a custom packer seen in other FinSpy exploits," the Kaspersky Labs researchers say. FinSpy is a highly secret surveillance tool that has previously been associated with Gamma Group, a British company that legally sells surveillance and espionage software to government agencies across the world. **FinSpy, also known as FinFisher, has extensive spying capabilities on an infected system, including secretly conducting live surveillance by turning ON its webcams and microphones, recording everything the victim types on the keyboard, intercepting Skype calls, and exfiltration of files.** To get into a target's system, FinSpy usually makes use of various attack vectors, including spear phishing, manual installation with physical access to the affected device, zero-day exploits, and watering hole attacks.

….Kaspersky Lab reported the vulnerability to Adobe, and the company has addressed the vulnerability with the release of Adobe Flash Player versions 27.0.0.159 and 27.0.0.130. Just last month, ESET researchers discovered legitimate downloads of several popular apps like WhatsApp, Skype, VLC Player and WinRAR (reportedly compromised at the ISP level) that were also distributing FinSpy. So, businesses and government organizations around the world are strongly recommended to install the update from Adobe as soon as possible. Microsoft will also likely be releasing a security update to patch the Flash Player components used by its products.

Payment Cards Stolen in Pizza Hut U.S. Website Hack

http://www.securityweek.com/payment-cards-stolen-pizza-hut-website-hack

Pizza Hut U.S. informed customers over the weekend that their payment card and contact information may have been compromised after cybercriminals breached its website. Emails sent out by the restaurant chain to affected individuals describe the incident as a "temporary security intrusion" on PizzaHut.com. According to the company, the hackers only had access to the site between the morning of October 1, 2017 through midday on October 2, 2017 for a total of roughly 28 hours. Customers who used the Pizza Hut website or mobile app to place an order during this period could be affected.

Pizza Hut said the breach was quickly detected and addressed, and it estimates that less than one percent of website visits during that week were impacted. McClatchy learned that roughly 60,000 people across the United States are affected by the incident. The restaurant chain said its external cybersecurity consultants determined that the attackers may have obtained information such as name, billing ZIP code, delivery address, email address, and payment card data, including card number, expiration date and CVV. Affected customers are being offered free credit protection services for one year. However, several

people reported on social media that their payment cards have already been used for fraudulent transactions, possibly as a result of this breach.

Hyatt Hotels Hit by Another Card Breach

http://www.securityweek.com/hyatt-hotels-hit-another-card-breach

Chicago-based hotel operator Hyatt Hotels Corporation informed customers this week that their credit card information may have been stolen by cybercriminals. This is the second data breach discovered by the company within a period of two years. The incident affects three hotels in the United States (all in Hawaii), three in Puerto Rico, 18 in China, four in Mexico, three in Saudi Arabia, three in South Korea, and one each in Brazil, Colombia, Guam, India, Indonesia, Japan and Malaysia. According to Hyatt, malware planted by cybercriminals on certain hotel IT systems harvested information from payment cards manually entered or swiped at some hotel front desks between March 18, 2017 and July 2, 2017. The malware was designed to steal data such as cardholder name, card number, expiration date, and internal verification code. No other information appears to have been compromised.

…. Back in 2015, Hyatt suffered a payment card breach that affected 250 of its hotels worldwide. The company claimed at the time that it had strengthened the security of its systems. "Our enhanced cybersecurity measures and additional layers of defense implemented over time helped to identify and resolve the issue," Floyd said this week. However, the company's enhanced security measures were obviously not enough, given that hackers had access to its systems for well over three months.

"The harvested customer payment card data – including expiration dates and verification codes - is extremely valuable data that will be sold on the Dark Web or used in credit card cycling scams. It's also easily combined with other stolen data to build entirely new synthetic personas for all manner of fraud," explained Lisa Baergen, marketing director at NuData Security.

"The travel and leisure industry – like so many consumer-facing sectors - has time and again shown itself extremely vulnerable to breaches," Baergen added. "This latest concerning breach is just one more reason why companies such as Hyatt must adopt more advanced security and authentication measures based on trusted identity, and consumers must diligently, routinely check their credit files for suspicious credit applications and consider freezing their credit profiles."

Secret Microsoft Database of Unfixed Vulnerabilities Hacked in 2013

http://www.cbc.ca/news/technology/microsoft-hack-1.4358025

Microsoft Corp's secret internal database for tracking bugs in its own software was broken into by a highly sophisticated hacking group more than four years ago, according to five former employees, in only the second known breach of such a corporate database. The company did not disclose the extent of the attack to the public or its customers after its discovery in 2013, but the five former employees described it to Reuters in separate interviews. Microsoft declined to discuss the incident.

The database contained descriptions of critical and unfixed vulnerabilities in some of the most widely used software in the world, including the Windows operating system. Spies for governments around the globe and other hackers covet such information because it shows them how to create tools for electronic break-ins. The Microsoft flaws were fixed likely within months of the hack, according to the former employees. Yet speaking out for the first time, these former employees as well as U.S. officials informed of the breach by Reuters said it alarmed them because the hackers could have used the data at the time to mount attacks elsewhere, spreading their reach into government and corporate networks. "Bad guys with inside access to that information would literally have a 'skeleton key' for hundreds of millions of computers around the world," said Eric Rosenbach, who was U.S. deputy assistant secretary of defense for cyber at the time.

Companies of all stripes now are ramping up efforts to find and fix bugs in their software amid a wave of damaging hacking attacks. Many firms, including Microsoft, pay security researchers and hackers "bounties" for information about flaws, increasing the flow of bug data and rendering efforts to secure the material more urgent than ever. …Sometime after learning of the attack, Microsoft went back and looked at breaches of other organizations around then, the five ex-employees said. **It found no evidence that the stolen information had been used in those breaches.** Two current employees said the company stands by that assessment. Three of the former employees assert the study had too little data to be conclusive. **Microsoft tightened up security after the breach, the former employees said, walling the database off from the corporate network and requiring two authentications for access.**

Another AWS [Amazon Web Services] Leak Exposes 150,000 Patient Home Monitoring Corp. Client Records

https://www.scmagazine.com/patient-home-monitoring-corp-exposed-475-gb-worth-of-patient-data/article/699640/

Another publicly accessible Amazon S3 repository has been once again been left exposing sensitive consumer information, this time affecting approximately 150,000 U.S. patients. Kromtech Security Researchers discovered the exposed server belonging to Patient Home Monitoring Corp. which contained 47.5 GB worth of data in the form of 316,363 PDF reports detailing weekly blood test results including patient and doctor names, case management notes, other client information and the Development Server Backup, according to an Oct. 10 Mac Keeper blog post.

The vulnerable server was spotted on Sept. 29 and researchers said they notified the company on Oct 5. and by Oct. 6, the bucket had been secured. Kromtech pointed out that the company's privacy page stated that patients have the right to be notified when their information is being accessed and that it's unclear how or if patients will be notified of the incident. HIPAA requires covered entities to notify affected individuals, and in some cases the media, when patient data is breached without unreasonable delay and no later than 60 days following the discovery of a breach. Patient Home Monitoring has yet to respond to SC Media for comment.

Some researchers aren't surprised that admins are misconfiguring Amazon S3 buckets and leaving them exposed with the rapid adoption of the new technology. **"The Amazon S3 bucket can be easily switched from private to public access – with public being the default."** Josh Mayfield, platform specialist, Immediate Insight at FireMon said. "With the speed that organizations are moving to AWS and cloud infrastructure, it is only natural to miss something." Mayfield said companies should have policy controls that are automated irrespective of future technology so that admins don't have to sacrifice security for speed and added that policy management consoles with the flexibility to handle heterogeneous infrastructures and devices are invaluable.

Other researchers weren't as forgiving. AlienVault Security Advocate Javvad Malik said **the issue of misconfigured cloud services is a growing problem and a lack of skill may be to blame**. "As more and more companies migrate datasets to the cloud, it is becoming apparent that many lack the cloud skills needed to secure the cloud infrastructure, gain assurance that the cloud infrastructure is secured appropriately, or monitor their cloud environments for unauthorized access," Malik said. **"While cloud can bring benefits of having a resilient infrastructure, security cannot be outsourced, and much of the responsibility remains with the customer."** Malik added that unfortunately, the people affected the most are the patients who have had their sensitive information exposed. Researchers agreed mistakes like this emphasize the impact breaches like this can have on individuals.

The narrative surrounding breaches is so often defined by the financial implications, but the impact of medical records being leaked on individuals could be equally if not more damaging, DomainTools Senior Sybersecurity Threat Researcher Kyle Wilhoit said. "Revealing potentially sensitive personally identifiable information could impact an individual's employment or **it could be used by criminals/state entities for targeted attacks, such as spear phishing**." Wilhoit said Medical organizations need to start taking the data they have access to as seriously as financial organizations, all assets must be discovered and tested against current vulnerabilities and patches must be deployed quickly.

How Russia Used Social Media to Divide Americans

https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook

For the past year, the world has reeled over escalating reports of how Russia "hacked" the 2016 US presidential election, by stealing emails from Democrats, attacking voter registration lists and voting machines and running a social media shell game. Such is the focus on Russian meddling that **congressional investigators are increasingly aggressive in asking the big tech companies to account for how their platforms became the staging grounds for an attack on American democracy**. Early next month that scrutiny will intensify, with executives from Facebook, Google and Twitter formally invited to appear before the House intelligence committee on Capitol Hill in Washington.

What has now been made clear is that Russian trolls and automated bots not only promoted explicitly pro-Donald Trump messaging, but also used social media to sow social divisions in America by stoking disagreement and division around a plethora of controversial topics such as immigration and Islamophobia. **And, even more pertinently, it is clear that these interventions are continuing as Russian agents stoke division around such recent topics as white supremacist marches and NFL**

players taking a knee to protest police violence. The overarching goal, during the election and now, analysts say, is to expand and exploit divisions, **attacking the American social fabric where it is most vulnerable, along lines of race, gender, class and creed**. "The broader Russian strategy is pretty clearly about destabilizing the country by focusing on and amplifying existing divisions, rather than supporting any one political party," said Jonathon Morgan, a former state department adviser on digital responses to terrorism whose company, New Knowledge, analyzes the manipulation of public discourse. "I think it absolutely continues."

Urgent threat, slow response. In the last month – mostly through vigorous reporting and academic research – we have also learned that the impact of Russia's Facebook infiltration was far more widespread than Mark Zuckerberg claimed when Barack Obama pulled him aside at a conference in Peru last November to inform the young titan he had a problem on his hands. As more evidence emerges revealing the extent of the Russian web invasion, it is clear that its footprint is far larger than the tech giants have ever conceded.

On Facebook alone, Russia-linked imposters had hundreds of millions of interactions with potential voters who believed they were interacting with fellow Americans, according to an estimate by Jonathan Albright of Columbia University's Tow Center for Digital Journalism, who broke the story wide open with the publication of a trove of searchable data earlier this month. Those interactions may have reinforced the voters' political views or helped to mold them, thanks to the imposter accounts' techniques of echoing shrill views and presenting seemingly sympathetic views with counterintuitive, politically leading twists. During the election, for example, an imposter Facebook page called "Being Patriotic" used hot-button words such as "illegal", "country" and "American" and phrases such as "illegal alien", ″Sharia law" and "welfare state", according to an analysis of Albright's data by the Associated Press. The page racked up at least 4.4 million interactions, peaking between mid-2016 and early 2017.

A reference to Russia in an April Facebook draft report about election influence was inexplicably cut, the Wall Street Journal reported last week. **Only last month did Facebook acknowledge that Russia-linked pages had bought thousands of ads on the platform**. According to the Washington Post this week, Google has detected similar ad-buying activity, of unknown scope, on YouTube, Gmail and its search engine – though the company has made nothing public. **The Russian imposters have also been detected on Instagram, Twitter and even Pokémon Go.** Facebook did not reply to repeated requests for comment. But the gravity of the situation, whose dimensions are still unknown, was underscored on Thursday in an interview that Facebook's chief operating officer, Sheryl Sandberg, gave to Axios. "Things happened on our platform that shouldn't have happened," Sandberg said, adding that the company owed the American public "not just an apology, but determination" to address the problem.

'Poor leadership ability'. The attackers appear to have a handy, if unwitting, ally in Trump, who is generous in spreading bile online. In certain recent cases, social media accounts linked with Russian influence operations appear to have taken cues directly and immediately from the @realdonaldtrump Twitter account, according to analysis by the Washington-based Alliance for Securing Democracy, which maintains a daily tracker of the networks in question. After Trump criticized the "poor leadership ability" of Carmen Yulín Cruz, mayor of San Juan, Puerto Rico, on 30 September, for example, Russian-linked Twitter accounts disseminated articles with "the primary theme of either discrediting" Cruz "or accusing the media of spreading 'fake news'", the alliance said.

The week before that, the clandestine network poured accelerant on the fight picked by Trump with the mostly African American players in the NFL who kneeled during the national anthem in protest of police violence. Instead of simply echoing the president's demand for a boycott unless the players stood, however, the Russian accounts took both sides of the issue, spreading both the hashtags #TakeaKnee and #BoycottNFL. **"The ads and accounts appeared to focus on amplifying divisive social and political messages across the ideological spectrum – touching on topics from LGBT matters to race issues to immigration to gun rights,"** said Alex Stamos, the chief security officer at Facebook, in the first public statement the company made on the matter.

Albright's data encompasses six Facebook pages previously linked by media investigations to Russia. The pages were not clumsily partisan, pro-Trump or anti-Hillary Clinton sites. Instead they worked by crafting identities around hot-button issues in US politics, and by wielding a crafty sympathy, in some cases, with causes seen as antithetical to Trump such as LGBTQ pride and opposing police violence. "There's some really intricate maneuvering going on," said Albright. "It's definitely set up not to directly force issues but to identify people that fall into the wedge categories that can be used to influence others or to push conversations elsewhere." The imposter pages included Secured Borders, an anti-immigrant

account that grew to 133,000 followers; Texas Rebels, which parroted Lone Star state pride while criticizing Clinton; Being Patriotic, which attacked refugees while defending the Confederate battle flag; LGBT United, which subtly espoused "traditional" family values; and Blacktivists, a faux satellite of the Black Lives Matter movement. "It seems Americans should be wary of police brutality more than of Isis terrorists," read a typical Blacktivists post, which was liked thousands of times. "Why there's so many privileges and benefits for refugee kids, but American kids forced to grow up in poverty?" asked one September 2016 post by Secured Borders. "That's absolutely unacceptable!!" "More than 300,000 vets died awaiting care," read a post on Being Patriotic. "Do liberals still think it is better to accept thousands Syrian refugees than to help our veterans?"

Owners of the imposter pages could post controversial – or seemingly sympathetic – messages or event announcements, and then, by inviting and observing interactions such as "likes", comments or merely views, gather information about genuine American Facebook users, and potential voters. Those voters could then be targeted with political content that appealed to some of their most closely held sympathies. The strategy was highly effective, in terms of penetration. Albright's research showed that **the six Russia-linked Facebook pages had generated more than 18 million interactions – a conservative estimate, he said – before Facebook shut them down**. But those were just six accounts among "dozens and dozens and dozens of pages" that bore obvious markings shared by other accounts linked with Russia, said Albright.

"Those 18 million interactions are only for those six pages, just on Facebook" and not Instagram or other social media, Albright said. "So what are we talking about here, overall? We're talking about hundreds of millions of interactions." The accounts and others have since been removed by Facebook. But "I don't think they've even begun to find" all the imposter accounts, Albright said, owing to the imposters' verisimilitude.

Russian Troll Factory Paid US Activists to Help Fund Protests During Election

https://www.theguardian.com/world/2017/oct/17/russian-troll-factory-activists-protests-us-election

Russian trolls posing as Americans made payments to genuine activists in the US to help fund protest movements on socially divisive issues, according to a new investigation by a respected Russian media outlet. On Tuesday, the newspaper RBC published a major investigation into the work of a so-called Russian "troll factory" since 2015, including during the period of the US election campaign, disclosures that are likely to put further spotlight on alleged Russian meddling in the election.

The existence of the troll factory, which has a history of spamming Russian and English blogs and comment forums, has been reported on by many outlets including the Guardian, but the RBC investigation is the first in-detail look at the organisation's activity during the election period. **RBC said it had identified 118 accounts or groups in Facebook, Instagram and Twitter that were linked to the troll factory**, all of which had been blocked in August and September this year as part of the US investigation into Russian electoral meddling. Many of the accounts had already been linked to Russian disinformation efforts in western outlets, but RBC said **its sources at the troll factory had provided screenshots of the internal group administration pages of some of the groups, as proof they were run from Russia. It also spoke to former and current employees of the troll factory**, all of whom spoke anonymously.

Perhaps the most alarming element of the article was the claim that employees of the troll factory had contacted about 100 real US-based activists to help with the organisation of protests and events. RBC claimed the activists were contacted by Facebook group administrators hiding their Russian origin and were offered financial help to pay for transport or printing costs. About $80,000 was spent during a two-year period, according to the report.

Hundreds of Websites Mining Cryptocurrency Without User Consent

https://www.hackread.com/hundreds-of-websites-mining-cryptocurrency-without-user-consent/

Previously it was reported that torrent search platform The Pirate Bay and other popular sites have been using visitor PCs to mine cryptocurrency and new reports have revealed that these are not the only websites that are exploiting our PCs but hundreds of websites are mining cryptocurrency without notifying the users. Bitcoin or Monero are some types of cryptocurrencies that can be mined and received through computation. When a site that is mining cryptocurrency is visited, there is a surprising surge in the CPU usage, which can prove to be beneficial for website owners because when a large number of PCs donates their powers, the mining is successful in earning revenues.

The report published by Adguard states that within merely weeks since the revelation about The Pirate Bay, there is an astounding increment in sites that mine cryptocurrencies through PCs of their site's visitors. Reportedly, 0.22% of the top 100,000 sites on Alexa List are discovered to be mining cryptocurrency, which means about 220 sites are involved in mining while the average of visitors on these sites is nearly 500 million and this audience arrive from various parts of the world from the USA and Europe to Asia and South America. While JSEcoin and CoinHive are the two most common and popular scripts that are employed to acquire cryptocurrency.

Adguard explains that around $43,000 have been raked in by these domains without any expenditure and within only three weeks. Reports also reveal that The Pirate Bay made $12,000 per month through cryptocurrency as the traffic flow is quite heavy on its domain. It is worth noting that most of the websites that are using miners are not as reliable and come from the blurry background. These include torrent search sites, pornographic sites, domains that host pirated content and similar other sites. As per the analysis of Adguard, websites having "shady reputation" are involved in browser mining; these sites otherwise find it difficult to make money through standard advertising practices, therefore, they use such tactics. Sites offering video-based content are most likely to generate income through mining more than any other. However, if handled appropriately, mining of cryptocurrency has immense potential as many users would agree to lend their CPUs so that they could get rid of annoying ads; but consent of users must be given importance. Domain operators need to respect end users and seek permission. Without user consent, domain operators are putting their reputation at risk, which might prove to be detrimental to their image in the long run.

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

****

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:

Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****