Security News Digest
October 10, 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".

Smart Devices Can Share Your Private Data, but Canada's Privacy Laws Offer Little Protection: Report

https://globalnews.ca/news/3791571/canada-privacy-laws-internet-of-things/

The rise of high-tech smart devices that store and share personal data poses a serious threat to Canadians' privacy, and one that is not adequately addressed by existing privacy laws, according to a new report from Western University [London, Ontario]. Law professor Samuel Trosow examined security and data collection protocols of an array of consumer smart devices, combing their fine print and putting them up against Canadian privacy laws. **He found that many products have inherent security flaws that leave them vulnerable to intrusions, while others may be intentionally stockpiling personal data for marketing purposes, unbeknownst to consumers.** What's more, the pace of technological development has left Canadian data privacy laws, many of which were implemented at the turn of the century, trailing in the dust.

Smart devices, which range from lightbulbs and kitchen appliances to fitness wearables and even sex toys, harness the internet to bring the benefits of network connectivity to a plethora of activities, chores and hobbies. Many of these gadgets utilize the Internet of Things (IoT), a system for connecting physical electronic devices via WiFi, Bluetooth and companion smartphone apps. Whether it's using a grocery-tracking gadget to streamline your grocery shopping, or using an app-connected smart lock to thwart bicycle thieves, the conveniences are unquestionable. But they come at the cost of privacy, whether consumers are aware of it are not.

Exacerbating this problem is the fact that Canadian privacy laws simply haven't caught up to the complexity of data collection and storage by smart devices. For instance, the law prohibits product manufacturers from divulging identifying personal information to outside parties. Trouble is, **modern statistical algorithms make it possible to take humongous chunks of anonymous data and break them down to identify individual information, a process known as re-identification**. "The re-identification can be accidental, but can also be intentional," the report says. It points to the case of a teenage Target customer who was sent ads for maternity products after the retail giant used sophisticated analytics to deduce that she was pregnant.

Among privacy policies of 20 product lines studied by Trosow, only one - the Fitbit fitness tracker - explicitly said it prevented recipients of consumer data from re-identification. To get around the blurred lines between supposedly identifying and non-identifying data, Trosow's report recommends that privacy law be altered to consider all consumer data as identifying and sensitive. He also suggests that a standard format be developed to make privacy terms and conditions easier to read and understand, and that information pertaining to use of customer data "be specified with greater clarity." The report also takes issue with products forcing consumers to agree to share their personal data if they want to take advantage of the product. "For example, in the case of wearable devices that generate health data, consumers should have the option of turning off the data collection that is reported back to the vendor," the report states.

Further complicating matters is the fact that **many smart devices used by Canadians are manufactured by U.S. companies; their products often require Canadian consumers to effectively waive their privacy rights**. Despite this being legally questionable, current privacy laws aren't anywhere near clear and strong enough, which emboldens U.S. tech vendors to continue the practice.
To tackle these and other privacy challenges, the report calls on Canada's privacy commissioner to proactively update privacy laws to bring them up to speed. "Like other technological developments in the past, the Internet of Things presents compelling evidence that laws need to adopt to changing circumstances." It's a task that the report warns will require considerable funding and resources. But with Canadians increasingly embracing connected devices - and exposing their personal data to tech companies, marketers and other third parties - it's something that will need to happen if Canadians' privacy and security interests are to be protected, the report concludes.

Vancouver Police Remind Online Daters to be Wary of Predators

http://vancouversun.com/news/local-news/vancouver-police-to-launch-online-dating-safety-campaign
The person on the other side of your dating app may seem like your soulmate, but they are still a stranger. That is the reminder the Vancouver Police Department is putting out in a new safety campaign that seeks to arm eligible singles with tips on approaching the world of online dating. **In recent years, police have noticed an increase in online dating as the reason for initial contact in sexual assault and fraud cases, spurring the campaign announced Wednesday.**
"Particularly on dating sites, women are finding themselves at higher risk for sexual assault, violent crime and fraud," said Det. Const. Michelle Grandbois at a news conference on Wednesday. "But these crimes are under-reported and **we want to hear from victims** so they can access the resources and help prevent others from being victimized." The campaign features a series of posters mimicking online dating profiles with the slogan, "They don't always fit the profile." As well, police have shared a number of tips for how to approach online dating and stories from those who have been victimized by online predators at catchyou.ca.
Those who date online are reminded: (1) not to give out personal information too freely, (2) not to use a profile photo that can be used to reverse Google image search for other personal details, (3) not to "friend" a stranger too quickly on Facebook and other platforms, (4) arrange for their first interaction to take place in public, and (5) to let a friend know where they will be and with whom.
Grandbois, who works with the VPD's sex crime unit, said there was not any particular site that was of concern, but that predators might be on multiple websites at a time, adapting their profile as needed. "They can happen on any dating site and there are dating sites for everybody," said Grandbois, noting it wasn't just women on traditional dating sites who were at risk. When asked whether there were any "mistakes" that daters could avoid, Grandbois was quick to point out these crimes were not the fault of the victims. "I would never call it a mistake that a women makes. This is a legitimate thing - lots of people meet online, on dating sites, and it's unfortunate that predators have found this out. It's a perfect platform for them to look through and basically select potential victims," she said.

Kelowna Residents Arrested in Darkweb Fentanyl Trafficking Investigation

https://globalnews.ca/news/3787575/kelowna-residents-arrested-in-darkweb-fentanyl-trafficking-investigation/
Police are calling it one of the most sophisticated drug organizations involving fentanyl and carfentanil in Canada and it has been shut down by the RCMP. Dubbed "project E-Neophile", Kelowna RCMP have arrested two people. Police say the accused are a 35-year-old Kelowna man and a 28 year-old Kelowna woman. Global Okanagan has learned their identities. James Nelson and his spouse Cassie Bonthoux were arrested in connection with the investigation, but there has not been a decision whether charges are warranted. They're not in custody but have a court date scheduled for December. They own a street/urban clothing store on Pandosy Street in Kelowna called Duke and Duchess Apparel. The store was raided on August 10. It was shut down after the raid but has since reopened. Police also raided their home in the Black Mountain area. The City of Kelowna posted a 'do not occupy or enter' poster on the door of the home because it had been used as a controlled substance operation.
Police say the pair were allegedly using the dark-web - a layer of the internet where criminals have been known to sell their wares. **"The drugs were then trafficked utilizing the dark-web throughout Canada, the United States, Europe and Australia,"** Corporal Jesse O'Donaghey said. The investigation began in September 2016 when police allege the two suspects were mailing packages

across North America. Police say the alleged criminal activity went silent up until July 2017 when police allege the suspects created a new account on the dark-web and resumed selling drugs. Several police enforcement agencies became involved in the investigation including Calgary Police and the US Drug Enforcement Agency (DEA). Police allege the suspects were selling fentanyl and carfentanil from a business they own in downtown Kelowna and from their home.

"It was as many as 25 packages that were seized by our investigators and they were allegedly destined for Canadian addresses, as well as internationally through the United States, Europe and Australia. Two unsecured firearms were also seized during the execution of those search warrants along with $68,000 in Bitcoin," O'Donaghey said. Police say the arrest will put a significant dent in the selling of fentanyl and carfentanil. **"This may be one of the most significant and perhaps the most sophisticated fentanyl/carfentanil trafficking and exportation enterprises that has been uncovered in Canada to date,"** Sgt,. Alex Lynch of the Kelowna RCMP Street Enforcement Unit said. RCMP say the bust may have saved lives. "It's likely prevented many deaths," Cpl. O'Donaghey said.

Video Streams Leak What You're Watching to Attackers With Over 95% Accuracy

https://www.bleepingcomputer.com/news/security/video-streams-leak-what-youre-watching-to-attackers-with-over-95-percent-accuracy/

Even if a video streaming service is using HTTPS to encrypt its traffic, an attacker can still determine with a very high accuracy what content a user might be watching. This type of snooping is possible because of an information leak discovered by a team of researchers in MPEG-DASH, a popular streaming technique implemented by today's top video platforms, such as Amazon, Netflix, YouTube, Vimeo, and others. The "information leak" is so immanent [inherent] to MPEG-DASH's design that it cannot be avoided without revamping the entire standard.

In the earlier days of the Internet, whenever a user wanted to view a video online, the streamer would deliver the entire file to the user's computer for playback. To avoid bandwidth waste, various techniques were invented to improve online video delivery. One of them was MPEG-DASH (Dynamic Adaptive Streaming over HTTP), which breaks the original video stored on a streamer's server into smaller segments holding a few seconds of video. Based on what portion of a video a user is watching, his browser or video player would download only the segments needed to display that particular section of the stream. For obvious reasons, the standard became really popular.

According to three researchers, these segments are unique enough to create fingerprints for the video streams a user might be watching. Each video stream has a "download fingerprint". The idea is that each video segment is encoded with a variable bitrate that produces downloadable video segment files of various lengths. When users download these files - that are later assembled into the final stream - a packet download pattern takes shape for anyone watching network traffic.

Leak occurs for HTTPS streams as well. According to researchers, these fingerprints are observable even if the traffic is encrypted, and an attacker can detect the download pattern even in video streams protected via HTTPS. An attacker only needs to create a database of fingerprints for streamable video files he wants to keep an eye out. To carry out such massive surveillance, the attacker needs to be in a position to intercept and sniff the user's traffic, such as an ISP, nation-state, traffic moderator, or malware present on smaller LANs. **The attack's success rate is way above similar techniques, with an average success rate of over 95%. In tests, the research team says it successfully identified videos a user was watching with a 99.5% success rate for YouTube, 98.6% for Vimeo, 98.5% for Netflix, and 92.5% for Amazon.** Furthermore, researchers also demonstrated a technique that ports this attack to JavaScript code hidden in an ad, when an attacker cannot obtain a role to directly observe a stream.

MPEG-DASH leak has good and bad side. While there are clear privacy implications for this attack - such as oppressive governments keeping an eye on who watches anti-government videos - there are also good uses for the MPEG-DASH leak. For example, law enforcement agencies could use the leak to track down people who watch child abuse or terrorist videos. More details about the MPEG-DASH leak are available in a research paper titled "Beauty and the Burst: Remote Identification of Encrypted Video Streams," available for download. The research team also set up a dedicated website and presented their work at the USENIX security conference.

Mattel Thinks Again About AI Babysitter [follow up]

http://www.bbc.com/news/technology-41520732

[Last week's Security News Digest featured an article on the privacy and security implications of having this device in a baby's bedroom. This is great news!]

Mattel has decided against releasing its AI-powered "babysitter" following concerns over privacy and other implications. Campaigners said artificial intelligence should not be used in place of real parenting, even if only briefly. The toy company announced the device in January and said it would sing lullabies and tell bedtime stories. Mattel said the device was no longer part of its strategy. At the CES technology show in January, Mattel billed its device - Aristotle - as a major leap in parenting technology. … Among its features, Aristotle would automatically "reorder or look for deals and coupons on baby consumables, formula and other baby products when it detects you are likely running low on the specific item". In July, Mattel replaced its chief technology officer with Sven Gerjets, who is understood to have reviewed Aristotle and decided against releasing it. The company said it had decided not to sell Aristotle "as part of an ongoing effort to deliver the best possible connected product experience to the consumer". **Mattel had been under pressure to pull the product**. The US-based Campaign for a Commercial-Free Childhood said: "Aristotle isn't a nanny, it's an intruder. **Children's bedrooms should be free of corporate snooping**." US politicians also had concerns about the data being gathered by the device and asked for more detail about how it would be stored or shared. Smart devices designed for children are a growing cause of concern for those worried about the as-yet unknown effects such technologies may have on young children's emotional development. Another Mattel product, a talking Barbie doll that would remember details from conversations, was poorly received when released early last year.

Deloitte Hack Hit Server Containing Emails from Across US Government

https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government

The hack into the accountancy giant Deloitte compromised a server that contained the emails of an estimated 350 clients, including four US government departments, the United Nations and some of the world's biggest multinationals, the Guardian has been told. **Sources with knowledge of the hack say the incident was potentially more widespread than Deloitte has been prepared to acknowledge and that the company cannot be 100% sure what was taken.** Deloitte said it believed the hack had only "impacted" six clients, and that it was confident it knew where the hackers had been. It said it believed the attack on its systems, which began a year ago, was now over.

However, sources who have spoken to the Guardian, on condition of anonymity, say the company red-flagged, and has been reviewing, a cache of emails and attachments that may have been compromised from a host of other entities. The Guardian has established that a host of clients had material that was made vulnerable by the hack, including: the US departments of state, energy, homeland security and defence, the US Postal Service, the National Institutes of Health, and "Fannie Mae" and "Freddie Mac", the housing giants that fund and guarantee mortgages in the US. Football's world governing body, FIFA, had emails in the server that was breached, along with four global banks, three airlines, two multinational car manufacturers, energy giants and big pharmaceutical companies.

The Guardian has been given the names of more than 30 blue-chip businesses whose data was vulnerable to attack, with sources saying the list "is far from exhaustive". Deloitte did not deny any of these clients had information in the system that was the target of the hack, but it said none of the companies or government departments had been "impacted". It said "the number of email messages targeted by the attacker was a small fraction of those stored on the platform". This assurance has been contested by sources that spoke to the Guardian. They said Deloitte's public position belied concern within the company about exactly what had happened and why.

The Guardian first revealed the existence of the hack on 25 September. Since then, the Guardian has been provided with further details of the attack, which seems to have started in autumn last year at a time Deloitte was migrating and updating its email from an in-house system to Microsoft's cloud-based Office 365 service. The work was being undertaken at Deloitte's Hermitage office in Nashville, Tennessee. The hackers got into the system using an administrator's account that, theoretically, gave them access to the entire email database, which included Deloitte's US staff and their correspondence with clients. Deloitte realised it had a substantial problem in spring this year, when it retained the Washington-based law firm, Hogan Lovells, on "special assignment" to review and advise about what it called "a possible cybersecurity incident".

In addition to emails, the Guardian understands the hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information. It is also thought

that some emails had attachments with sensitive security and design details. Deloitte has insisted its internal inquiry, codenamed Windham, found that only six clients had information that had been compromised. The review had also been able to establish "precisely what information was at risk", the company said. However, that analysis has been contested by informed sources that have spoken to the Guardian. They say the investigation has not been able to establish definitively when the hackers got in and where they went; nor can they be completely sure that the electronic trail they left is complete. "The hackers had free rein in the network for a long time and nobody knows the amount of the data taken," said one source. "A large amount of data was extracted, not the small amount reported. The hacker accessed the entire email database." Another source added: "There is an ongoing effort to determine the damage. There is a team looking at records that have been tagged for further analysis. It is all deeply embarrassing."
The Guardian has been told **Deloitte did not at the time have multi-factor authentication as standard on the server that was breached. A cybersecurity specialist told the Guardian this was "astonishing"**. The expert said the migration to the new email system would have "utterly complicated the kind of forensic investigation required to see what had happened". …In recent months, Deloitte has introduced multi-factor authentication and encryption software to try to stop further hacks.

Iranian Hackers Targeted Deloitte Via A Seriously Convincing Facebook Fake [catfishing]

https://www.forbes.com/sites/thomasbrewster/2017/10/05/facebook-fake-hacks-deloitte-employee-iran-cyber-spies-suspected/#2f9ca17e188c
As America frets over Russians running rampant on Facebook, other adversaries have been exploiting the social network as a way into some of the world's biggest businesses. An employee at Deloitte, one of the Big Four accounting firms, fell victim to a fake Facebook account in late 2016, *Forbes* can reveal. And the attacks, believed to have been perpetrated by Iranian government spies, **occurred around the same time as a separate hack, recently disclosed by *The Guardian,* which affected Deloitte data in Microsoft's Azure cloud-hosting service**.
The lovely and disarming "Mia Ash" is a fictional female created by the highly-active hacker crew known as OilRig, which, as *Forbes* reported in July, cybersecurity firm SecureWorks believes is sponsored by the Iranian regime. In July 2016, Mia's puppeteers targeted a Deloitte cybersecurity employee, engaging him though the social network in conversations about his job, *Forbes* learned from sources with direct knowledge of the attack. As the online relationship grew, the employee offered to help his new friend Mia set up a website for her alleged business. **Eventually, the entity behind Mia exploited the positive rapport to convince the Deloitte employee to open a malicious document sent by Mia on his work computer**. [social engineering] Though it's not believed that particular malware infected the wider company network, according to the sources, **it illustrated the ability of the puppeteers to gain the employee's trust**. *Forbes* will not reveal the individual's name here, but **he was one of the firm's cybersecurity staffers assisting clients with their digital defenses, making the attack that much more startling**. "This kind of thing is effective because men can't help themselves apparently," [women too – it's a human nature thing..] said James Lewis, a former U.S. diplomat and cybersecurity expert at the Center for Strategic and International Studies.
A Facebook fraud unravels. The Mia Ash persona was built on the photos and profile information of a real photographer from Romania, Cristina Mattei. With alluring images and active avatars across Facebook, WhatsApp and LinkedIn, Mia was a convincing fraud, described previously by SecureWorks cybersecurity researcher Allison Wikoff as **one of the most developed fake personas she'd ever seen**. (SecureWorks declined to comment for this article). Certainly, Mia was convincing enough to gain the internet friendship of an Asia-based cybersecurity professional and, after sending messages from summer last year through to February 2017 when she disappeared from Facebook, to convince him to open a file purportedly containing some of her photos on a work laptop. **Fortunately for Deloitte, the malware inside, a tool dubbed PupyRat designed to pilfer credentials for corporate systems, didn't make it onto the company network, sources said.** [RAT = Remote Access Technology]

Equifax Says 15.2 Million UK Records Accessed in Cyber Breach

http://www.reuters.com/article/us-equifax-cyber/equifax-says-15-2-million-uk-records-accessed-in-cyber-breach-idUSKBN1CF2JU
U.S.-based credit reporting agency Equifax Inc said on Tuesday that the massive cyberattack it disclosed in September compromised the sensitive personal details of nearly 700,000 consumers in the United

Kingdom. Equifax said that 15.2 million UK records dating from 2011 to 2016 were exposed in the incident, which affected 145.5 million people overall, but that 14.5 million of the exposed UK records did not contain information that put consumers at risk.

U.S. Banking Regulator Hit by 54 Breaches in 2015, 2016

http://www.securityweek.com/us-banking-regulator-hit-54-breaches-2015-2016

The U.S. Federal Deposit Insurance Corporation (FDIC) in the last two years may have suffered as many as 54 data breaches involving personally identifiable information (PII), revealed a report from the FDIC Office of Inspector General (OIG). Created in response to the thousands of bank failures in the 1920s and 1930s, the FDIC is an independent agency that provides insurance to depositors. The standard insurance amount is $250,000 per depositor, per insured bank. The report, made public last week, focuses on the FDIC's processes for responding to data breaches, and it's based on an audit conducted in response to concerns raised by the chairman of the Senate Committee on Banking, Housing, and Urban Affairs.

The OIG's audit focused on 18 of 54 suspected or confirmed breaches discovered by FDIC between January 1, 2015 and December 1, 2016. The 18 incidents reviewed by auditors affected more than 113,000 individuals. The audit found that in 13 of the 18 cases the FDIC did not complete some key breach investigation activities, such as assessing impact and convening the data breach management team, within the timeframe established in the agency's Data Breach Handling Guide (DBHG). It took the organization, on average, more than 9 months to notify affected individuals after discovering a breach. It took between 145 days and 215 days to send out notifications to impacted people after the decision was made to notify victims. In one incident that affected nearly 34,000 people, the FDIC sent out the notifications exactly one year after the breach was discovered.

The failure to notify affected individuals and investigate the breaches in a timely manner was due to the lack of an incident response coordinator, the failure to provide adequate training to information security managers, and insufficient privacy staff for managing incident response activities, the OIG said in its report. The audit also found that the FDIC failed to adequately document key assessments and decisions; failed to clearly define the purpose, scope, governance structure and key operating procedures of its data breach management team; and it did not track and report key breach response metrics. A report published last year by the House of Representatives Science, Space and Technology Committee revealed that threat actors believed to be from China breached the systems of the FDIC in 2010, 2011 and 2013, and planted malware on a significant number of servers and workstations. The committee concluded that the agency's CIO had attempted to cover up the incident.

Millions of Pornhub Users Targeted in Malvertising Attack

https://www.theguardian.com/technology/2017/oct/10/pornhub-adult-site-users-targeted-malvertising-attack-malware-kovcoregs-kovter

Millions of Pornhub users were targeted with a malvertising attack that sought to trick them into installing malware on their PCs, according to infosec firm Proofpoint. By the time the attack was uncovered, it had been active "for more than a year", Proofpoint said, having already "exposed millions of potential victims in the US, **Canada**, the UK, and Australia" to malware by **pretending to be software updates to popular browsers**. Although **Pornhub, the world's largest pornography site with 26 billion yearly visits** according to data from ranking firm Alexa, and its advertising network have shut down the infection pathway, the attack is still ongoing on other sites.

The hack was carried out by a group known as KovCoreG, Proofpoint said, who hoped to infect users with an ad fraud malware known as Kovter. **This type of malicious software is traditionally used as a form of online advertising fraud to generate money through clicks on fake adverts.** In this particular attack, visitors to Pornhub were redirected to a website which claimed to be offering a software update for their web browser, including Chrome and Firefox, or to the Adobe Flash plugin. If they downloaded and opened the file it installed Kovter, taking over their machine and using it to click on fake adverts. **Those fake clicks then generated real money for the websites the adverts are hosted on - typically spam-filled sites no normal user would ever visit.** "While the payload in this case is ad fraud malware, it could just as easily have been ransomware, an information stealer, or any other malware," Proofpoint said. "Regardless, threat actors are following the money and looking to more effective combinations of social engineering, targeting and pre-filtering to infect new victims at scale." Pornhub did not reply to a request for comment.

Malvertising campaigns are a popular way for malware authors to spread their infections, said Javvad Malik, security advocate at AlienVault. “In 2016, Google removed 112 million bad ads which aside from malware, included illegal product promotion and misleading ads,” he said. “The issue being that there are insufficient controls to place an advert with an ad network, making it far easier to get a malicious app accepted by an official app store. This has led to an upturn in the number of reputable organisations distributing malvertising.” Mark James, a security specialist at IT firm ESET, said that Pornhub was likely a preferred target for the bad actors. “The audience is possibly less likely to have security in place or active as people’s perception is that it’s already a dark place to surf,” he said. “Also, the user may be less likely to call for help and try to click through any popups or install any software themselves, not wanting others to see their browsing habits.”

Fast-Food Chain Sonic Hacked, Millions of Card Numbers for Sale on Dark Web

https://hotforsecurity.bitdefender.com/blog/fast-food-chain-sonic-hacked-millions-of-card-numbers-for-sale-on-dark-web-19023.html

With 3,500 locations in 45 states across the US, fast-food chain Sonic Drive-In confirmed falling victim to a data breach that exposed customer credit and debit card numbers. The company was informed about a potential data breach by its credit card processor, after detecting a pattern in a number of fraudulent transactions. The company hasn’t revealed the exact number of hacked cards, but security researcher Brian Krebs first reported that he came across millions of card numbers for sale on a dark web marketplace called Joker’s Stash, including some that had been recently used at a number of Sonic locations. Following the investigation, Krebs informed the fast-food chain that the data was for sale on the dark web.

Private Data of More Than 1,100 NFL Players, Agents Exposed

http://thehill.com/policy/cybersecurity/353664-private-data-of-more-than-1100-nfl-players-agents-exposed

The personal data of more than 1,100 NFL players and agents was **exposed as the result of a misconfigured online database**, a cybersecurity company has revealed. Bob Diachenko, the chief communications officer for Kromtech Alliance, wrote in a blog post on the company's website Monday [Oct2] that researchers had identified a publicly accessible database with players' and their agents' private information. The database, operated by the NFL Players Association, could have been accessed by "anybody with Internet connection," Diachenko wrote in the blog post.

He also said that researchers had discovered that the server had been the victim of a ransomware attack, with hackers attempting to lock up the information and require a payment of 0.01 Bitcoin - worth about $427 - to unlock it. “IF PAYMENT IS NOT MADE WITHIN 120 HOURS WE WILL LEAK THE DATABASE TO PUBLIC,” a ransom message left inside the database read. So far, it does not appear that anyone has paid the ransomware demand.

Forbes first reported the private data exposure, which affected 1,133 players and agents. Among the players whose information was exposed was former San Francisco 49ers quarterback Colin Kaepernick, who stirred controversy last year by kneeling during the national anthem to protest police misconduct and racial inequality. According to Kromtech, Kaepernick's email, home address and phone number were exposed by the database. Kaepernick, who's currently an NFL free agent, has said that he has received multiple death threats for his protests.

North Korea Hacked Seoul's War Plans: Report

http://www.securityweek.com/north-korea-hacked-seouls-war-plans-report

North Korean computer hackers have stolen hundreds of classified military documents from South Korea including detailed wartime operational plans involving its US ally, a report said Tuesday. Rhee Cheol-Hee, a lawmaker for the ruling Democratic party, said the hackers had broken into the South's military network last September and gained access to 235 gigabytes of sensitive data, the Chosun Ilbo daily reported. Among the leaked documents was Operational Plans 5015 for use in case of war with the North and including procedures for "decapitation" attacks on leader Kim Jong-Un, the paper quoted Rhee as saying. Rhee, a member of parliament's defence committee, could not be reached for comment but his office said he had been quoted correctly.

The report comes amid heightened fears of conflict on the Korean peninsula, fuelled by US President Donald Trump's continued threats of military action against Pyongyang to tame its weapons ambitions. In his latest tweet over the weekend, Trump reiterated that diplomatic efforts with North Korea have

consistently failed, adding that "only one thing will work". Citing Seoul's defence ministry, Rhee said that 80 percent of the leaked documents had yet to be identified. But the contingency plan for the South's special forces was stolen, he said, as well as details about annual joint military drills with the US and information on key military facilities and power plants. A ministry spokesman declined to confirm the report, citing intelligence matters.
In May the ministry said North Korea had hacked into Seoul's military intranet but did not say what had been leaked. **Pyongyang has a 6,800-strong unit of trained cyber-warfare specialists**, according to the South Korean government. It has been accused of launching high-profile cyber-attacks including the 2014 hacking of Sony Pictures. The Chosun Ilbo story was the second report Tuesday of military-related cyber-attacks in the Asia-Pacific. Australia's government said separately an unidentified defence contractor had been hacked and a "significant amount of data" stolen. There were 47,000 cyber-incidents in the last 12 months, a 15 percent increase from the previous year, Minister for Cyber Security Dan Tehan said in Canberra as he launched a report by the Cyber Security Centre. The defence contractor was exploited via an internet-facing server, with the cyber-criminals using remote administrative access to remain in its network, the report said. The Australian newspaper reported that the hacker was based in China but Tehan told the Australian Broadcasting Corporation that "we don't know and we cannot confirm exactly who the actor was".

Google Uncovers Russia-Backed Ads on YouTube, Gmail

http://www.cbc.ca/news/technology/russia-election-ads-google-microsoft-1.4347242

Google has discovered Russian operatives spent tens of thousands of dollars on ads on its YouTube, Gmail and Google Search products in an effort to meddle in the 2016 U.S. presidential election, a person briefed on the company's probe told Reuters on Monday. **The ads do not appear to be from the same Kremlin-affiliated entity that bought ads on Facebook Inc, but may indicate a broader Russian online disinformation effort, according to the source**, who was not authorized to discuss details of the confidential investigation by Alphabet Inc's Google.
Microsoft Corp said separately on Monday that it was looking at whether Russians bought U.S. election ads on its Bing search engine or other Microsoft-owned products and platforms. A spokeswoman for the company declined to comment further. The revelation about Google is likely to fuel further scrutiny of the role that Silicon Valley technology giants may have unwittingly played during last year's election. **U.S. intelligence agencies have concluded that Moscow's goal was to help elect Donald Trump.**
Google has uncovered less than $100,000 in ad spending potentially linked to Russian actors, the source said. Both Twitter Inc and Facebook recently detected and disclosed that suspected Russian operatives, working for a content farm known as the Internet Research Agency in St. Petersburg, Russia, used their platforms to purchase ads and post content that was politically divisive in a bid to influence Americans before and after the November 2016 presidential election. The Internet Research Agency employ hundreds of so-called "trolls" who post pro-Kremlin content, much of it fake or discredited, under the guise of phony social media accounts that posed as American or European residents, according to lawmakers and researchers.

4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

****