BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest
January 30, 2018

You may have dropped some of your New Year's Resolutions already, but be sure to take this quiz and stick with security resolutions all year in 2018: 'Security New Year' Quiz
(Do you Love Your Online Life? Watch for our February Quiz…)

Metrolinx Claims Computers Hit by North Korean Cyberattack 🇨🇦

http://www.cbc.ca/news/canada/toronto/north-korean-cyber-attack-metrolinx-1.4500918
An Ontario transit agency says it was in the crosshairs of a North Korean cyberattack earlier this month. **The attack was a virus, routed through Russia, that infected computers at Metrolinx**, according to a source at the agency who spoke on condition of anonymity. Spokesperson Anne Marie Aikins confirmed to CBC Toronto that the attack took place, but said it did not result in any breach in privacy and did not compromise any safety systems. Aikins could not provide further details about the attack, citing "security reasons." Metrolinx is an arm's-length organization in charge of transportation for the Toronto and Hamilton area.

Implicated in recent hacks. North Korea has been implicated in recent hacks, including the WannaCry ransomware attack that infected hundreds of thousands of computers worldwide and crippled parts of Britain's National Health Service in May. U.S. Homeland security adviser Tom Bossert wrote in a Wall Street Journal op-ed last month that North Korea was "directly responsible" for the WannaCry ransomware attack and that Pyongyang would be held accountable for it. Bossert said the U.S. administration's finding of responsibility is based on evidence and confirmed by other governments and private companies, including the U.K. and Microsoft. American officials have also said that North Korea is responsible for the Sony cyberattack in 2014 that dumped personal information of tens of thousands of current and former workers online. North Korea has denied involvement in both cases.

Canada's Privacy Commissioner Proposes Right to Change Inaccurate Search Engine Results 🇨🇦

http://www.cbc.ca/news/technology/privacy-commissioner-de-indexing-forgotten-search-results-1.4505425
Canada's privacy commissioner thinks you should have the right to ask that inaccurate, incomplete or outdated information appearing in search engines be either amended or removed - and that under Canadian law, internet companies should have to comply. In cases where information about individuals has been posted by others to a website or social media platform, individuals should also have a right to challenge the accuracy and appropriateness of that information.

The proposed policy was announced Friday by the Office of the Privacy Commissioner of Canada. Although the proposal is similar in some ways to the European Union's right to be forgotten - which has been criticized for its potential to affect free expression - it isn't modelled on the EU's framework, but rather is **an interpretation of existing Canadian privacy law**. "There is little more precious than our reputation," Privacy Commissioner Daniel Therrien said in a statement announcing the policy proposal Friday. "But protecting reputation is increasingly difficult in the digital age, where so much about us is systematically indexed, accessed and shared with just a few keystrokes. **Online information about us can easily be distorted or taken out of context and it is often extremely difficult to remove.**"

If it isn't possible or practical for information to be modified or corrected, Therrien's office suggests two remedies: (1) De-indexing, which would require search engines such as Google, Bing, or Yahoo to remove links to pages that have been deemed inaccurate or inappropriate under the definition of Canada's *Personal Information Protection and Electronic Documents Act*. (2) Source takedown, as the name implies, would require a website or social media platform to remove inaccurate or inappropriate content from the internet completely. Individuals can lodge a formal complaint with the commissioner if the issue can't be resolved with a search engine or site operator directly.

A right to be forgotten. In the EU, a process to request the removal of results from search engines such as Google has existed since 2014. But de-indexing is not without its critics. Some have expressed concerned that the tactic could be used to crack down on legitimate speech and free expression, and that it won't stop people from finding the information at its source. There are also concerns about leaving such decisions to private companies, according to submissions to the commissioner. "Challenges should be evaluated on a case-by-case basis, and decisions to remove links should take into account the right to freedom of expression and the public's interest in the information remaining accessible," the OPC said. ….. In an email, University of Ottawa law professor Michael Geist said he isn't surprised by the commissioner's position. "We've seen many privacy commissioners move in this direction," he wrote. For its part, giving Canadians more control over their reputation online has been one of the commission's priorities since 2015. It launched a consultation and call for essays the following year, and drafted today's policy in response. The proposed measures have not yet been put into practice, and the commissioner plans to hold further consultations before finalizing a position. The commission believes that because search engines portray themselves as sources of the most relevant, reliable, authoritative sources of information online - effectively building ever-changing profiles of personal information around search queries in the process - they also have an obligation under Canada's personal information act to be accountable for the accuracy and appropriateness of their results. … Information that might be deemed inappropriate and subject to removal includes material that is unlawful or illegally published, or may cause significant harm to an individual and is not in the public interest to leave in place. The commissioner is also recommending that Parliament study the issue further "to determine whether we have struck the right balance," according to the draft policy report. [some content has been edited to shorten]

Proposed Class Action Claims Women Were Recorded in Saanich [B.C.] Grocery Store Bathroom 🇨🇦

http://www.iheartradio.ca/cfax-1070/news/proposed-class-action-claims-women-were-recorded-in-saanich-grocery-store-bathroom-1.3591835

A proposed class action lawsuit alleges several women were recorded in the washroom of the Mattick's farm Red Barn Market, in the Cordova Bay area [just outside of Victoria]. CTV Vancouver Island reports that two women claim video was recorded by a "sexually charged and disrespectful" co-worker between the years 2009 and 2014. **They only found out about it in 2016, when police contacted them about their images being posted to a Russian revenge porn website.**

The women claim at least six other victims were allegedly recorded in the washroom and they're proposing the class action lawsuit so other victims can join. The lawsuit names the former employee, and also alleges he exposed himself to a female co-worker. They're also suing the business for general damages from "negligence resulting in an invasion of privacy." Saanich police acknowledged a civil lawsuit was filed, and confirm they started a police investigation two years ago into multiple alleged incidents of a male co-worker secretly filming female co-workers in a staff bathroom at a store.

CBC, Big Telecom Join Forces To Push For Website Blocking In Piracy Fight 🇨🇦

http://www.huffingtonpost.ca/2018/01/29/cbc-big-telecom-join-forces-to-push-for-website-blocking-in-piracy-fight_a_23347007/

Canada's media industry is lining up behind an effort to institute mandatory blocking of websites accused of piracy. More than two dozen of Canada's largest media organizations, including the CBC and most of the country's major telecoms, have joined a coalition that on Monday asked the CRTC, Canada's telecom regulator, to start blocking websites believed to be engaged in piracy. Besides the CBC, the FairPlay Canada coalition includes Bell, Rogers Media, Corus Entertainment and Cogeco. It also includes cinema chains Cineplex, Guzzo and Landmark, and a number of unions involved in the media industry, including the Alliance of Canadian Cinema, Television and Radio Artists (ACTRA), Unifor and the Union des artistes (UDA).

"The jobs of hundreds of thousands of Canadians who work in the creative sector are at risk as a result of increasing online piracy, from songwriters and set builders to makeup artists and local news reporters," the coalition said in a press release issued Monday. **"Payments from legitimate streaming services, broadcasters, distributors, and exhibitors help support these artists and creators."** The coalition is asking the CRTC to create an "Independent Piracy Review Agency" (IPRA) that would maintain a blacklist of websites believed to be engaged in unauthorized use of copyrighted materials. The CRTC would be in charge of ensuring that Canadian internet providers comply with the blacklist and keep those websites inaccessible.

The new coalition represents a major expansion of a campaign initially started by Bell Canada, which has been advocating for website blocking for some time. The company pushed for website blocking to be included in NAFTA renegotiations. After Bell's proposals were published by Canadaland last fall, some IP critics expressed concern about a lack of court oversight in deciding which websites would be banned. But the coalition appears to have taken steps to address those concerns, and is now calling for the piracy agency to "be subject to oversight by the Federal Court of Appeal." "We support efforts to stop piracy of copyrighted content," CBC/Radio-Canada president Hubert Lacroix said in a statement. "Groups who steal and re-sell content without permission are breaking the law and undermining financial support for culture."

Consumer advocacy group OpenMedia said the proposal "would essentially create an official internet censorship committee within the federal government, and open the door for overreaching censorship in Canada." The proposal "is like using a machine gun to kill a mosquito," OpenMedia executive director Laura Tribe said. "It will undoubtedly lead to legitimate content and speech being censored online, violating our right to free expression and the principles of net neutrality, which the federal government has consistently pledged support for."

Other countries are doing it too. But the FairPlay coalition argues setting up an internet piracy agency would mean Canada is just playing catch-up with some other countries. "What we are proposing has been effective in countries like the U.K., France, and Australia," said Shan Chandrasekar, president and CEO of Asian Television Network International Limited (ATN), which filed the coalition's application to the CRTC. The push comes as Canada's media industry faces headwinds created by piracy and the shift to online media. TV providers are losing households to cord-cutting at a rate of some 200,000 a year, even as Canada's population grows. **Recently the industry has been trying to fight against the proliferation of unauthorized streaming services, which are often just affordable set-top boxes that allow users to stream channels and services without paying for them.**

Google Took Down Over 700,000 Bad Android Apps in 2017

https://www.theverge.com/2018/1/30/16951996/google-android-apps-removed-security-2017

Google’s numerous safeguards designed to prevent malicious apps from reaching Android users led to the removal of over 700,000 apps from the Google Play Store in 2017, the company said today. That’s a 70 percent increase over the total removals in 2016. “Not only did we remove more bad apps, we were able to identify and action against them earlier,” Google Play product manager Andrew Ahn wrote in a blog post. **“99 percent of apps with abusive contents were identified and rejected before anyone could install them.”**

Google attributes this success to its improved ability to detect abuse “through new machine learning models and techniques.” Copycat apps designed to resemble popular mainstays remain a popular method of trying to deceive users, according to Ahn. **Google removed over a quarter of a million of these impersonating apps last year.** The company also says it kept “tens of thousands” of apps with inappropriate content (pornography, extreme violence, hate, and illegal activities) out of the Play Store. Machine learning plays a key role here in helping human reviewers keep an eye out for bad apps and malicious developers.

“Potentially harmful applications” (PHAs) are apps that attempt to phish users’ personal information, act as a trojan horse for malware, or commit SMS fraud by firing off texts without a user’s knowledge. “While small in volume, PHAs pose a threat to Android users and we invest heavily in keeping them out of the Play Store,” Ahn said.

Last year, Google put all of its malware scanning and detection technologies under the umbrella of **Google Play Protect**. The Android operating system automatically performs scans on installed applications to hunt for anything that’s out of place, and users can also manually trigger scans of their Android smartphones right in the updates section. (I’ve finally managed to stop hitting this button when checking for new versions of apps, but it took some time.)

Still, bad apps do occasionally slip through Google’s defenses. In August, Google discovered and kicked out 30 apps that were secretly using the devices they were installed on to perform DDoS attacks. Just earlier this month, the company removed 60 games from the Play Store - some of them meant for children - that were found to display pornographic ads. Google says it will continue to upgrade its methods and machine learning models against bad actors trying to trick consumers with apps that violate its policies. Those efforts indeed seem to be paying off in helping Android’s security turn a corner.

Hawaii Fires Employee Who Sent False Ballistic Missile Alert

https://www.theverge.com/2018/1/30/16952202/hawaii-false-ballistic-missile-alert

Hawaii officials said Tuesday that they had fired the emergency management employee who sent a false ballistic missile alert earlier this month. The administrator of the Hawaii Emergency Management Agency has also resigned in the wake of the incident. The state released the details of its investigation into the incident, following an FCC report earlier today that included some overlapping details. The state's report said "insufficient management controls, poor computer software design, and human factors" contributed to the false alert being sent, and that protocol changes have been made to prevent similar incidents in the future.

State officials also revealed that the employee who was terminated on Friday "has performance issues," and had confused drills with real-world events in at least two previous incidents. The report said colleagues had complained about such issues in the past. As the FCC said in its report released earlier today [Jan30], the employee said in a statement that he believed there was a legitimate missile attack underway. The state's report noted that statement, but also said several other employees present correctly heard that the drill was not a real attack.

Jackpotting Attacks Hit U.S. ATMs; Spit Out Cash in Seconds

https://www.hackread.com/jackpotting-attacks-hits-us-atms-spit-out-cash-in-seconds/

Jackpotting is an attack/technique to exploit ATMs to make them dispense cash without withdrawing it from a bank account – Now, U.S. ATMs are under Jackpotting attack. The trend of hacking ATMs (automatic teller machines) is not new but with the passage of time, it is becoming a lot more persistent and sophisticated. In some parts of the world, cybercriminals use skimmers to steal card data while in some places they prefer using explosives to crack open ATMs to steal cash.

In the United States, however, two of the largest ATM manufacturers Diebold Nixdorf and NCR Corp. have warned citizens to be aware of an attack in which hackers are taking over ATMs to steal cash in a technique that was never seen before in the country. Dubbed 'Jackpotting,' the technique involves hackers to physically access the ATM, infect it with a malware/malicious software and use hardware including industrial endoscope which forces the machine to give away cash according to commands executed by hackers.

This was revealed by journalist Brian Krebs who got his hands on a confidential US Secret Service memo that reveals how jackpotting has hit the ATMs in the United States for the very first time. Before that, the attack was popular against ATMs in Asia and Europe. The memo further reveals that **once the hackers take over an ATM, the attack forces it to dispense money at the rate of 40 notes every 23 seconds and only stops once the machine is empty.** Currently, the prime targets of Jackpotting are Big-box stores, pharmacies and drive-thru ATMs. An alert issued by Diebold gives in-depth details about the attack and how it can be prevented.

"In a Jackpotting attack, the criminal gains access to the internal infrastructure of the terminal in order to infect the ATM PC or by completely exchanging the hard disk (HDD). In recent evolutions of Jackpotting attacks portions of a third-party multi-vendor application software stack to drive ATM components are included. In cases where the complete hard disk is being exchanged, encrypted communications between ATM PC and dispenser protects against the attack," the alert warns. According to the warning issued by NCR, the company said none of their ATMs have been compromised however **the attack itself is a big threat to the ATM industry in the country**. "This should be treated by all ATM deployers as a call to action to take appropriate steps to protect their ATMs against these forms of attack," said NCR.

Remember, for cybercriminals hacking an ATM machine is now a piece of cake since most of these machines are still running on Windows XP. Just a few months ago, a security researcher Leigh-Anne Galloway had demonstrated how one can hack an ATM by simply drilling a hole. She also highlighted the fact that since a majority of cash machines are Windows XP systems that are linked with a safe, therefore, the trick makes a varied range of machines vulnerable to hack attack. Moreover, it is very easy for anyone to buy ATM malware on the Dark Web, therefore, there is a need of a complete overhaul of the ATM industry to make its devices secure against cyber criminals and protect banks and customers from losing their cash.

Fitness Tracking App Strava Gives Away Location of Secret US Army Bases

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company. The details were released by Strava in a data visualisation map that shows all the activity tracked by users of its app, which allows people to record their exercise and share it with others.

The map, released in November 2017, shows every single activity ever uploaded to Strava – more than 3 trillion individual GPS data points, according to the company. **The app can be used on various devices including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns.** However, over the weekend military analysts noticed that the map is also detailed enough that **it potentially gives away extremely sensitive information about a subset of Strava users: military personnel on active service**. Nathan Ruser, an analyst with the Institute for United Conflict Analysts, first noted the lapse. The heatmap "looks very pretty" he wrote, but is "not amazing for Op-Sec" – short for operational security. "US Bases are clearly identifiable and mappable." "If soldiers use the app like normal people do, by turning it on tracking when they go to do exercise, it could be especially dangerous," Ruser added, highlighting one particular track that "looks like it logs a regular jogging route."

…. In locations like Afghanistan, Djibouti and Syria, the users of Strava seem to be almost exclusively foreign military personnel, meaning that bases stand out brightly. In Helmand province, Afghanistan, for instance, the locations of forward operating bases can be clearly seen, glowing white against the black map. **Zooming in on one of the larger bases clearly reveals its internal layout, as mapped out by the tracked jogging routes of numerous soldiers. The base itself is not visible on the satellite views of commercial providers such as Google Maps or Apple's Maps, yet it can be clearly seen through Strava.**

Outside direct conflict zones, potentially sensitive information can still be gleaned. For instance, a map of Homey Airport, Nevada – the US Air Force base commonly known as Area 51 – records a lone cyclist taking a ride from the base along the west edge of Groom Lake, marked on the heatmap by a thin red line. RAF Mount Pleasant in the Falkland Islands is lit up brightly on the heatmap, reflecting the exercise regimes of the thousand British personnel there – as are nearby Lake Macphee and Gull Island Pond, apparently popular swimming spots.

When Strava released the heatmap, an updated version of one it had previously published in 2015, it announced that "this update includes six times more data than before – in total 1 billion activities from all Strava data through September 2017. Our global heatmap is the largest, richest, and most beautiful dataset of its kind. **It is a direct visualisation of Strava's global network of athletes**."

Strava demonstrated that the new heatmap was detailed enough to see kiteboarding in Mexico, to track the route of the Camino de Santiago across northern Spain and to see the sea route of the Ironman triathalon in Kona, Hawaii. Perhaps the closest to the current operational security issues that it noted, however, was the layout of the Burning Man festival in the Nevadan desert. "The unique pentagonal pattern of Burning Man's pop-up city is forever etched into the Heatmap, thanks to all the runners and cyclists who have used Strava to explore it," the company wrote.

Strava Suggests Military Users 'Opt Out' of Heatmap as Row Deepens

https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban

Fitness-tracking company Strava has defended its publication of heatmaps that accidentally reveal sensitive military positions, arguing that the information was already made public by the users who uploaded it. Following the revelations, militaries around the world are contemplating bans on fitness trackers to prevent future breaches. **As well as the location of military bases, the identities of individual service members can also be uncovered, if they are using the service with the default privacy settings. The "global heatmap" shows, in aggregate form, every public activity uploaded to the app over its history.** In major cities, it lights up popular running routes, but in less trafficked locales it can highlight areas with an unusually high concentration of connected, exercise-focused individuals – such as active military personnel serving overseas.

In a statement, Strava said: "Our global heatmap represents an aggregated and anonymised view of over a billion activities uploaded to our platform. It excludes activities that have been marked as private and user-defined privacy zones. **"We are committed to helping people better understand our settings to give them control over what they share," the company said, sharing a blogpost from**

2017 which detailed eight things users can do to lock down their privacy on the service, including specifically opting out of the global heatmap by unchecking a box in the settings page.

AI Used to Face-Swap Hollywood Stars Into Pornography Films

https://www.theguardian.com/technology/2018/jan/25/ai-face-swap-pornography-emma-watson-scarlett-johansson-taylor-swift-daisy-ridley-sophie-turner-maisie-williams

Advanced machine learning technology is being used to create **fake pornography featuring real actors and pop stars, pasting their faces over existing performers in explicit movies**. The resulting clips, made without consent from the women whose faces are used, are often indistinguishable from a real film, with only subtly uncanny differences suggesting something is amiss. **A community on the social news site Reddit has spent months creating and sharing the images, which were initially made by a solo hobbyist who went by the name "deepfake".** When the technology site Motherboard first reported on the user in December last year, they had already made images featuring women including Wonder Woman star Gal Gadot, Taylor Swift, Scarlett Johansson, and Game of Thrones actor Maisie Williams. In the months since, videos featuring other celebrities including Star Wars lead Daisy Ridley, Game of Thrones's Sophie Turner, and Harry Potter star Emma Watson have been posted on the site, which has become the main location for sharing the clips.

While simple face swaps can be done in real time using apps such as Snapchat, the quality of the work posted by deepfake required much more processing time, and a wealth of original material for the AI system to learn from. But the computer science behind it is widely known, and a number of researchers have already demonstrated similar face swaps carried out using public figures from news footage. The creation of face-swapped pornography rapidly scaled up in late December, when another Reddit user (going by the name "deepfaceapp") released a desktop app designed to let consumers create their own clips. While not easy to use – the app takes eight to 12 hours of processing time to make one short clip – the release of the app galvanised the creation of many more images.

"I think the current version of the app is a good start, but I hope to streamline it even more in the coming days and weeks," deepfakeapp told Motherboard. "Eventually, I want to improve it to the point where prospective users can simply select a video on their computer, download a neural network correlated to a certain face from a publicly available library, and swap the video with a different face with the press of one button."

The ease of making extremely plausible fake videos using neural network-based technology has concerned many observers, who fear that it heralds a coming era when even the basic reality of recorded film, image or sound can't be trusted. "We already see it doesn't even take doctored audio or video to make people believe something that isn't true," Mandy Jenkins, from social news company Storyful, told the Guardian last year. "This has the potential to make it worse."

CrossRAT Keylogging Malware Targets Linux, macOS & Windows PCs

https://www.hackread.com/crossrat-keylogging-malware-targets-linux-macos-windows-pcs/

Another day, another malware – This time, it is CrossRAT malware targeting Linux, macOS and Windows devices without being detected by anti-virus software. Almost a week ago, the IT security researchers at OutLook along with the civil rights group, Electronic Frontier Foundation (EFF) exposed **a highly sophisticated cyber espionage campaign operated by Dark Caracal hackers from Lebanon in which the group used Android malware against journalists and government officials in 21 countries**. [the US is on the list; Canada is not]

In their findings, the researchers **also highlighted the presence of another dangerous malware called CrossRAT written in Java programming language** which they believe was developed by Dark Caracal to target OSX, Linux, and Windows-based devices. The malware is capable of evading anti-virus software and manipulate the file system of a targeted device, take screenshots, run arbitrary DLLs for secondary infection on Windows, and gain persistence on the infected system.

However now Patrick Wardle, a security researcher, and ex-NSA hacker has published a detailed report on CrossRAT according to which once infecting the computer, the malware performs a thorough scan on the machine. It can identify the kernel, the most basic layer that integrates the system with hardware, and the type of architecture. The purpose is to do the specific installation of the program according to each software. CrossRAT is so sophisticated that it can rummage through Linux systemmd to identify the distribution of the system including Arch Linux, Centos, Debian, Kali Linux, Fedora etc). In addition, CrossRAT has a built-in keylogger, software that records what is typed on the computer and send it to the command control center (C&C). However, Wardle did not find a way to activate the latter tool. **Moreover, according to Wardle, Windows and Linux computers are more susceptible to infection. This is because, as the malware is built in Java, it is necessary for the user to have this software on the computer. The two operating systems already bring a pre-installed version of Java, whereas, in macOS, it would be necessary to download**. When the researcher scanned the sample hmar6.jar file that installs CrossRAT on VirusTotal, it turned out that only 1 out of 58 anti-virus programs could detect the malware however at the time of publishing this article, 28/58 programs could detect the file as malicious.

Now that the malware is detected by most of the security software on VirusTotal, its threat has gone to a low level however following commands can also help you identify if your system is infected with CrossRAT [go to article for instructions]

Dutch Banks, Tax Agency Under DDoS Attacks a Week After Big Russian Hack Reveal

https://www.bleepingcomputer.com/news/security/dutch-banks-tax-agency-under-ddos-attacks-a-week-after-big-russian-hack-reveal/

At least three Dutch banks and the Dutch tax office reported on Monday suffering coordinated DDoS attacks against their respective infrastructures. ABN AMRO, Rabobank, and ING Bank officials reported suffering DDoS attacks that prevented customers from logging into web-based dashboards. The DDoS attack on ABN AMRO started on Saturday, per the bank's statement, while the other two banks were hit on Monday. Also on Monday, Belastingdienst —the Dutch Taxation Authority— also admitted suffering a DDoS attack that prevented users from logging into its web portal and filing tax-related documents. Citing sources, Dutch security researcher Rickey Gevers claimed the attacks **reached a peak of 40 Gbps** in volume. **He also said the attacks came mainly from IP addresses associated with home routers**. A report by NL Times citing sources with antivirus vendor ESET claimed **some of the DDoS attacks were also carried out using the Zbot malware**, a known (desktop-based) banking trojan based on the old ZeuS banking trojan. **The same report claimed the command and control servers for this botnet were based in Russia.**

Many fear DDoS attack is repercussion for last week's exposé. The Dutch media's obsession with Russia is not accidental. Last week, Dutch newspaper Volkskrant and TV station NOS published a report claiming that the country's AIVD intelligence service compromised the computer of a hacker part of Russian-based cyber-espionage group **Cozy Bear (also known as APT29)**. The report claim AIVD agents spied on the cyber-espionage unit since 2014 and observed how Russian intelligence services hacked into DNC servers during the 2016 US Presidential election. Journalists said AIVD identified individuals part of the Cozy Bear cyber-espionage unit and even watched Russian hackers through the webcams on the compromised PC.

Many Dutch officials now fear the DDoS attacks are just the first of the many Russian cyber-attacks that will come as retaliation for last week's revelations. Something similar happened in 2015 when the Dutch Safety Board (DSB) was attacked by another Russian cyber-espionage unit - Fancy Bear (aka APT28). Those attacks came as Dutch authorities were investigating and later issued a report blaming the crash of flight MH17 in Ukraine on a military missile fired at the aircraft by pro-Russian rebels.

Russian Trolls Created Facebook Events Seen By More Than 300,000 Users

http://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html

Posing as American activists, Russian government-linked trolls created 129 Facebook events between 2015 and 2017. On multiple occasions, the events prompted real Americans to take to the streets.

In a written statement Facebook gave to the Senate Intelligence Committee released on Thursday, the social media network said that the events created by one Kremlin-linked troll group were seen by more than 300,000 Facebook users. About 62,500 users marked that they would attend the event, and an additional 25,800 expressed an interest in attending. Facebook told Congress it does "not have data about the realization of these events," but CNN has previously found evidence that the Russian group successfully convinced Americans to attend the demonstrations. **The events were organized on a range of divisive issues and were designed to pit Americans against each other.** In one case, the troll group organized and promoted two opposing events on the same day at the same location in Houston, Texas.

"Heart of Texas," a page that posed as a pro-Texas secession organization, promoted a "Stop Islamization of Texas" protest at the opening of a library at an Islamic Center on May 21, 2016. The same troll group used another page, "United Muslims of America," to promote a "Save Islamic Knowledge" event at the same time. **The Russian group spent $200 promoting the events on Facebook, the company told Congress last fall.**

Executive director of the American-Islamic Relations in Texas, Mustafaa Carroll, told CNN that his organization had contacted the FBI about comments posted on the "Heart of Texas" page before the protest. One of them read: "Need to blow this place up. We don't need this shit in Texas." Both of the Russian-created events took place and local news footage shows a few dozen people from opposing groups taking part in the demonstrations. The protests were also discussed by Houston City Council three days after it took place.

In July 2016, just a day after the shooting of Philando Castile by police in a suburb of Saint Paul, Minnesota, **a Russian-run page designed to look like an organization run by American Black Lives Matter activists, promoted a protest** outside the police department where Jeronimo Yanez, the officer who shot Castile, worked. The protest was publicized on a Facebook page called "Don't Shoot Us," and had more than 250,000 followers as of September 2016. Local activists were confused when they saw the event, as they had organized a protest outside the Minnesota Governor's Mansion. When an activist group with ties to a local union reached out to the page, someone with "Don't Shoot Us" replied and explained that they were not in Minnesota but planned to open a "chapter" in the state in the following months. **The local group became more suspicious. After investigating further, they posted on their website to say that "Don't Shoot Us" was a "total troll job."** Eventually, the "Don't Shoot Us" demonstration went ahead, facilitated by local activists, who intervened to help ensure the event was held safely.

Local activists were not aware of Don't Shoot Us' Russian ties until CNN uncovered it in October. **More than 120 million Americans saw content from the Russian troll group, known as the Internet Research Agency (IRA), Facebook told Congress last fall.** In its answers to the Senate Intelligence Committee released on Thursday, Facebook said it does not believe it is in a position to "substantiate or disprove allegations of possible collusion" between the Trump campaign and Russian operatives.

Collusion? Facebook said it found "what appears to be insignificant overlap" between the targeting of its content by the Internet Research Agency and the Trump campaign. Trump has repeatedly denied allegations that there was any collusion between his campaign and Russian authorities to influence the 2016 election results.

"The targeting for the IRA ads that we have identified and provided to the Committee was relatively rudimentary, targeting broad locations and interests," Facebook said in the written statement it provided to the committee. "[W]e have seen only what appears to be **insignificant overlap** between the targeting and content used by the IRA and that used by the Trump campaign (including its third-party vendors)," Facebook said in its written statement.

May Calls Again for Tech Firms to Act on Encrypted Messaging

https://www.theguardian.com/technology/2018/jan/25/theresa-may-calls-tech-firms-act-encrypted-messaging

Theresa May has signalled her desire to crack down on encrypted messaging apps, arguing that the services provide a safe haven for terrorists and extremists and hinting that the government may take more concrete action if developers do not act themselves.

In 2015, as home secretary, May called for terrorists to be denied “safe spaces to communicate”, and said a future Conservative government would legislate to restore the “declining capabilities” of the British government to intercept communications. In March 2017, No 10 repeated a call by May’s successor as home secretary, Amber Rudd, for police and intelligence services to be given access to encrypted messages on services such as WhatsApp. “Where there are instances where law enforcement agencies wish to gain access to messages which are important to an investigation, they should be able to do so,” the prime minister’s spokesman said. In June, May declared “enough is enough” after the Westminster terror attack, and told the press that internet companies must not allow extremism a place to exist. “We cannot allow this ideology the safe space it needs to breed – yet that is precisely what the internet and the big companies that provide internet-based services provide.” And in September she told the UN that tech firms must go “further and faster” in removing extremist content. Finally, on Thursday May reiterated her calls for larger tech firms to take action voluntarily. “These companies simply cannot stand by while their platforms are used to facilitate child abuse, modern slavery or the spreading of terrorist and extremist content," she told the audience in Davos.

This time May moved the specific target of her attacks on encrypted messaging from the Facebook-owned WhatsApp to a smaller firm, Telegram, created by the Russian entrepreneur Pavel Durov. "Just as these big companies need to step up, so we also need cross-industry responses because smaller platforms can quickly become home to criminals and terrorists. We have seen that happen with Telegram. And we need to see more cooperation from smaller platforms like this," she said.

Despite the years of strong words, however, actions from the UK government have been rare. The Investigatory Powers Act of 2016, strongly backed by May while she was home secretary, gave the government the power to demand the removal of encryption applied to messages, but the government has yet to apply that power to any major technology firm. Instead, May has repeatedly insisted the technology companies should voluntarily act.

And Now, This:

Child Development Experts Urge Facebook to Pull Messenger Kids App

https://www.theguardian.com/technology/2018/jan/30/messenger-kids-facebook-mark-zuckerberg-app-child-development-experts-

More than 110 child-health advocates have called on Facebook chief executive Mark Zuckerberg to pull the firm's Messenger Kids app aimed at under 13s, warning of the dangers of social media for children.

In an open letter led by the Boston-based Campaign for Commercial-Free Childhood, signed by doctors, educators and child health experts including baroness Susan Greenfield, **warn that "younger children are simply not ready to have social media accounts"**.

The authors write: "At a time when there is mounting concern about how social media use affects adolescents' wellbeing, it is particularly irresponsible to encourage children as young as preschoolers to start using a Facebook product." The standalone Messenger Kids app was launched in December targeting children under 13 with strict parent controls that include contact approvals, screened content and safety filters to prevent children sharing inappropriate material. It contains no ads and Facebook says data collected from it will not be used for advertising purposes.

But the launch of the app was attacked by commentators and British health secretary Jeremy Hunt, who said the firm should "stay away from my kids". The open letter authors said Messenger Kids was likely to increase the amount of time pre-school and elementary age children spend with their devices. "In a landscape of ubiquitous technology that undermines children's emotional growth, the last thing the youngest among them need is a powerful enticement to move their friendships online" said Dr Sherry Turkle, Abby Rockefeller Mauzé professor of the social studies of science and technology at MIT, and author of the book Reclaiming Conversation. "It's galling to see Facebook target young children at a time when **evidence is mounting that excessive social media use negatively impacts kids and teens' wellbeing**," said Josh Golin, executive director of the Campaign for Commercial-Free Childhood.

Facebook said it developed Messenger Kids with the help of online safety experts including the National PTA and Blue Star Families. It is designed to connect children to relatives and friends through text, photos and video chat while making parents the gatekeepers. It is fully compliant with the US Children's Online Privacy and Protection Act, the social network said. "As children spend more and more time on digital devices, they lose the healthy capacities to cultivate moments of quiet and solitude that are so crucial for developing empathy and healthy relationships," said Turkle. Jenny Radesky, MD, a developmental behaviour pediatrician and media researcher at the University of Michigan, said **those under 13 years old find it hard to grasp concepts such as privacy and personal data**. "They're just starting to build awareness about their identity, their role in relationships, and morality," she said. "Combine that immaturity with the problematic interactions that often happen on social media, and it could be really messy."

US federal law prohibits companies from collecting personal information on those under 13 without parental consent. However, millions of children are already on Facebook, with or without their parents' permission, said Stephen Balkam, chief executive of the nonprofit Family Online Safety Institute, who saw the launch of Messenger Kids as a pragmatic approach to the situation. The open letter joins a chorus of discontent directed towards the impact of social media, and in particular Facebook, on society and the young. Industry insiders including former Facebook president Sean Parker, SalesForce CEO Marc Benioff and Apple chief executive Tim Cook have all recently expressed concerns over the use of social media by children.

“Parents, health professionals, and even investors are standing up to tell tech giants that they’ve gone too far,” said Golin. “This is a pivotal moment, and Silicon Valley executives must decide if they care about the welfare of children, families and society, or only about hooking users and pursuing profits.” A Facebook spokesperson said: “We worked to create Messenger Kids with an advisory committee of parenting and developmental experts, as well as with families themselves and in partnership with the PTA. We continue to be focused on making Messenger Kids be the best experience it can be for families. We have been very clear that there is no advertising in Messenger Kids.”

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

****

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

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest
To learn more about information security issues and best practices, visit us at:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens’ Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

****