Security News Digest
June 20, 2017

Celebrate the Summer Solstice at 9:24 pm Pacific Time! Be outdoors and enjoy the experience☺

The Internet of Things? What things?
Take the Internet of Things Quiz and find out!

How a Single Criminal Hacking Group Held Canadian Casinos and Mining Companies Ransom

http://www.cbc.ca/news/technology/canada-mines-casinos-hacked-ransom-extortion-fireeye-fin10-1.4162940

A "financially motivated" and digitally-savvy criminal hacking group has spent at least three years infiltrating computers at several unnamed Canadian mining companies and casinos, stealing sensitive data and holding it for ransom. The group, dubbed FIN10 by the cybersecurity company FireEye, began operating as early as 2013, continued until at least 2016, and has not been identified before, investigators said.

Charles Prevost, one of the investigators and a senior manager at FireEye's security consulting practice Mandiant, said they "have no idea why" FIN10 had seemingly chosen to target only Canadian mines and casinos. He could not attribute FIN10 to a particular country or location - a notoriously difficult problem in cybersecurity investigations - but noted that its members appeared to be native English speakers, despite attempts to appear otherwise. *According to FireEye's report, released today, the attacks targeted sensitive files such as corporate records, private communications and customer information. After stealing the data from the victims' computers, the investigators say the hackers demanded ransoms of between 100 and 500 bitcoin - about $35,000 to $170,000 Cdn*.

The group then threatened to release some of the stolen data to the public if no payment was received within 10 days, and to release more data if there was still no payment three days later. *FIN10 also wreaked havoc on targets who did not meet their demands "by essentially shutting off production systems so that the mine or casino couldn't operate for a period of time,"* according to Charles Carmakal, another investigator and Mandiant vice president, resulting in "real" but unspecified revenue loss.

Common criminal playbook. The attacks follow a common playbook among criminals operating in the digital realm. In at least two cases, *the hackers used carefully crafted emails, tailoring messages, links and attachments to entice their targets to click - a technique known as **spearphishing***, which was also used by Russian-backed hackers to break into the U.S. Democratic National Committee in the summer of 2015. *In one case, the attackers hid their code in a **malicious webpage** claiming to be an updated holiday schedule for staff. In another, they disguised a malicious Microsoft Word document as an employee questionnaire*.

However, unlike the Russian-backed groups that frequently dominate headlines, Prevost said FIN10's tools and techniques were "very far from the state-sponsored type of activity that we investigate" - meaning the group used easily available **"**penetration testing tools" with names like Metasploit, PowerShell Empire and SplinterRAT. Those tools allowed FIN10 to gain a foothold into its targets' networks, remove data and run basic commands that deleted important operating system files - effectively knocking out casino money handling computers, critical mining databases and systems that were required to let employees log into their workstations. The attackers "scheduled them just like a timebomb," Prevost said - in one client's case, taking 60 critical systems offline overnight.

Who were the victims? Carmakal said FireEye's report involved "less than 10" companies, but would not specify how many. *FireEye also declined to name any of the companies that were targeted, citing confidentiality agreements with the victims*. But previous breaches offer some possible clues. In the mining industry, both Goldcorp and Detour Gold Corporation have suffered data breaches in recent years, and seen gigabytes of personal information published online - including employee's personal contact and financial information.

Among Canadian casinos, the River Cree Resort and Casino just outside of Edmonton, Alberta said in March 2016 that criminals had stolen customer and employee information from its systems. Then in June, Cowboy's Casino in Calgary was also breached, and similar information was stolen. And in November, the Casino Rama Resort in Rama, Ont. also admitted that it had been breached, saying that customer, employee and vendor information had been stolen, too. Earlier this week, some of the information from the Cowboy's Casino breach - specifically, customer's personal information and information on gambling habits and payouts - was posted online. *It's not clear if the casinos or mines mentioned in previous reports are also part of FireEye's report, and the company wouldn't say*. It was reported by the Financial Times that FireEye was investigating the River Cree Resort incident, but the company also would not confirm whether the incident was part of the company's report.

Canadian Security Agency Will Soon Be Able to Launch Cyber Attacks Against Terrorists

http://globalnews.ca/news/3542168/canada-launch-cyber-attack-terrorism/

Security officials in Canada will soon have the ability to launch cyber attacks against foreign actors, including terror groups and even other governments. The move is part of a much broader series of updates to national security legislation announced Tuesday, and shifts Canada's Communications Security Establishment (CSE) to a much more offensive posture when it comes to dealing with threats in cyberspace. At the moment, CSE does not have the authority to take action online outside of Government of Canada networks to deter cyber threats against the country. *But once this new legislation passes, CSE employees will be allowed to conduct both "defensive cyber operations" and "active cyber operations," including operations that "advance national objectives."* "Currently we only have a defensive shield," said Defence Minister Harjit Sajjan on Tuesday. "We have to wait to be hit."

The targets of the "active cyber operations" (in other words, attacks) could include foreign groups, organizations, states and individuals who are involved in terrorist activity, are attempting to compromise national security, trying to disable key infrastructure, or spying on Canadians. CSE could, for example, move to disable a foreign server that was attempting to steal private information from a Government of Canada network. The agency could also hack into, and disable, networks being used by terrorist groups to recruit fighters within our borders. "The proposed CSE Act will eliminate the ambiguities about what we are permitted and authorized to do in cyber space," CSE noted.

Before any of these new powers are exercised, however, the legislation states that CSE would need to get the green light from the highest levels of government. Canadian-led cyber attacks would require the direct approval of both the defence minister and the minister of foreign affairs. Defensive cyber operations, meanwhile, will require the approval of the defence minister and "consultation" with the foreign affairs minister. CSE would also be required to report the outcomes of all these activities to both ministers.

Strict no-go zones are also built into the legislation. CSE would be prohibited from directing cyber operations activities at "Canadians, any person in Canada, or the global information infrastructure in Canada," for example. None of the activities would be permitted to cause death or bodily harm, and CSE could not attempt to "obstruct, pervert or defeat the course of justice or democracy." The idea that Canada should become more actively engaged in cyber warfare is not new. The government's recent defence policy review made it explicitly clear that Canada's military feels that "a purely defensive cyber posture is no longer sufficient" given the explosive growth in online threats.

Canada's Spy Agency Expects Cyberattacks During 2019 Federal Election

http://www.cbc.ca/news/politics/cse-report-elections-cyber-threats-1.4163868

Canada's electronic spy agency issued a stark warning Friday that online attempts to influence or undermine the country's electoral process are on the increase - and steps must be taken to counter the efforts. The assessment is contained in a new report released by the Communications Security Establishment (CSE) that comes amid questions about Russia's role in the last U.S. presidential election. While foreign states did not use cyberattacks to try to influence the last federal election in 2015, there are no guarantees they won't try in 2019, the next time Canadians are scheduled to go to the federal polls. In response, the Liberal government is promising to set aside political bickering and work with other federal parties to protect the electoral system from foreign adversaries and other nefarious actors. "We will approach our shared challenge ahead in a very Canadian way: working together, co-operating, and with a

steely resolve," said Democratic Institutions Minister Karina Gould. "We will continue to put the security of Canadians and Canadian democracy first."
Among the steps being taken is to have the CSE, whose mandate includes protecting the country from cyberthreats, brief all federal parties for the first time on the dangers - and how to protect themselves. The electronic spy agency will also work with Elections Canada and its provincial counterparts to shore up their own defences.
The CSE report, the first of its kind, looked at the threat posed by cyberactivity not only in Canada, but around the world in recent years. *It found that there has been an upward trend in such activity over the past five years, and that 13 per cent of elections held around the world this year had been targeted*. The nature of the activity runs the gamut, the report says, including efforts to suppress voter turnout, attempts to discredit or blackmail parties and candidates and an overall campaign of disinformation. Canada has not been immune, said CSE chief Greta Bossenmaier*, noting that the last federal election saw low-level cyberattacks that were most likely perpetrated by what she called "hacktivists" and cybercriminals.*
While Bossenmaier said the attacks did not have any impact on the actual electoral process, she expected to see more sophisticated methods employed by such actors the next time around. "Looking to 2019, we do anticipate to see cyber attempts to influence the election," Bossenmaier told a news conference.
"We believe multiple hacktivist groups will make such attempts. While much of it will likely be low-sophistication, groups will likely study past operations and adopt more sophisticated means." The bigger question is whether another country will try to influence Canada's next federal election, as Russia is alleged to have done in the U.S., France and Germany.
Protecting Canadians
The CSE report doesn't name any countries, but it does warn such foreign interference could happen depending on Canada's foreign and domestic policies, and the positions taken by different federal parties. What matters isn't who is behind a specific attack, said Gould, but rather that Canada take steps to protect itself and ensure nobody - state-sponsored or otherwise - is successful in their attempts to interfere. "Ultimately this is about protecting ourselves as Canadians," she said. Part of the reason for emphasizing the need to protect the electoral process - or build resilience, as Bossenmaier described it - is that catching perpetrators is extremely difficult. "There is rarely any timely punishment," the CSE chief said, "and it's worth the risk." *That is particularly true when it comes to the spread of disinformation, which has taken on epic proportions with the spread of social media.*
The government will be working to educate voters and increase awareness of the problem, Gould said, which includes CSE's report and working with other parties to identify other possible actions. "Today is the first step," she said. *"For the first time in the world, a democracy is informing the public about cyberthreats."*

Alberta Passes Bill to Protect Cyberbullying Victims

http://www.cbc.ca/news/canada/edmonton/alberta-passes-bill-to-protect-cyberbullying-victims-1.4094647
[May01- missed this when it came out] The Alberta legislature has passed a bill that makes it easier for people to sue for damages if their intimate images are shared on the internet without their permission. *Bill 202, the Protecting Victims of Non-Consensual Distribution of Intimate Images Act*, also makes it illegal for anyone to profit from such images. The bill, introduced by Scott Cyr, the Wildrose MLA for Bonnyville-Cold Lake, unanimously passed third reading Monday afternoon with support from Wildrose, NDP, Progressive Conservative and Alberta Party MLAs.
Cyr said he looked to a similar bill in Manitoba while drafting the legislation. But his act goes further, as it allows school boards to suspend or expel students caught sharing intimate images of other students. The bill will create consistency across Alberta schools that currently doesn't exist, Cyr said. "My concern is, by not having some uniform system, or a law that is being broken, that we don't identify the real true source of the problem here, which is sharing of pictures that should never have actually been put on the internet," he said.
When he introduced the bill in March, Cyr said lawsuits launched by victims were rarely successful. The bill creates the tort law necessary to make it easier for people to sue. *Cyr said he was inspired to introduce the bill after having a discussion with his 11-year-old daughter about the dangers of taking intimate images and sharing them with others. He said during the discussion, his daughter asked why people were allowed to post such images. That inspired the MLA to see what he could do legislatively.*

Hundreds of Calgary Women Secretly Photographed, Posted to 'CanadaCreep' Twitter Account 

http://www.cbc.ca/news/canada/calgary/canadacreep-twitter-account-calgary-voyeurism-1.4158523?

A Twitter account that amassed 17,000 followers by posting surreptitiously recorded images of Calgary women's clothed breasts, buttocks and genital areas - including videos filmed up women's skirts while they walked - *has been suspended by the social media service*. The "CanadaCreep" account was active for almost a full year and had posted hundreds of photos and videos before Twitter shut it down on Tuesday morning, following numerous complaints.

Alexandra Constantinidis, 22, learned on Monday evening she was among the women whose images were posted to the site. She said numerous friends alerted her to a nearly minute-long video that appeared to be of her walking in downtown Calgary, filmed from behind and focused on her backside. When she watched it for herself, she recognized it as being recorded on Friday, as she was going to get lunch. She then looked through the previous "CanadaCreep" posts, which date back to June 2016, and said *she was shocked the account had been so active for so long*.

Creepy or criminal? Many of the images were captured on the streets of downtown Calgary, others in and around Prince's Island Park. Some were clearly recorded at a C-Train station or in the city's Plus-15 network of elevated walkways. Several photographs appear to have been taken during the Calgary Comic and Entertainment Expo in the spring. Others of a woman in a bathing suit look to have been taken at an indoor pool. There were also numerous videos in which the camera operator follows women wearing dresses or skirts from behind until the women walk up stairs or there is another opportunity to put the camera low to the ground and point it upward, capturing images of their underwear. *That can qualify as a criminal act in Canada, where surreptitiously recording images up women's skirts where the victims have a "reasonable expectation of privacy" is punishable under the voyeurism section of the Criminal Code*. *"The charges may also be more serious if there is intent to distribute the pictures, and depending on who is photographed there also may be a risk of being charged with child pornography,"* University of Calgary criminologist Michael Adorjan told CBC News….

Police actively investigating. Calgary police said Tuesday they are actively investigating the "CanadaCreep" account for voyeurism. Staff Sgt. Cory Dayley said some of the videos posted to the account appear to clearly cross the line into criminal territory. "Anything that's going to be underneath a layer of clothing would be considered an expectation of privacy in our minds," he said. Police have already saved copies of content that was recorded in Calgary, he added, and they may seek more material saved on Twitter's computer servers as evidence. Dayley said police were alerted to the existence of the account on Monday evening and were in contact with numerous victims on Tuesday.

Hospital Records Breach Costs Health Authority $1M 

http://thechronicleherald.ca/novascotia/1478315-hospital-records-breach-costs-health-authority-1m

Hundreds of Nova Scotian hospital patients may get to share a $1-million settlement in a case involving breaches of their privacy. *Halifax's Wagners Law Firm has reached a proposed settlement with a former provincial health authority and if it's approved will offer $1,000 each to nearly 700 plaintiffs they represent in a class-action lawsuit*. In 2012, the South West Nova District Health Authority sent letters to 700 people, telling them an employee had "inappropriately" accessed their health information, according to a Wagners news release.

…said Ray Wagner in a phone interview with The Chronicle Herald: "We were happy to come to a resolution before trial, given the uncertainty of a courtroom environment." A two-week trial was to begin this month but it has been replaced with a settlement approval hearing. *The original lawsuit included 717 people, but over the years some opted out, and the access to others' records by the staffer was found to be for legitimate reasons. The Roseway Hospital in Shelburne had previously disclosed that the employee had accessed the files through a work computer. The employee was fired*. "The actual number is 686, and we are committed to giving $1,000 to each of those people," said Wagner. The number includes legal fees and the costs of administering the settlement. "The privacy breaches in the advent of electronic info has become a recent issue. But we would be the first to get a resolution," he said. "This could set an important precedent and give credibility to the responsibility of information holders to make sure privacy is respected." ..The hearing will be June 22 at the Law Courts Building at 1815 Upper Water St. in Halifax.

Trudeau Shuts Down Internet Tax On Streaming Services 

http://www.huffingtonpost.ca/2017/06/15/canada-streaming-tax_n_17120780.html

[Not security news, just news that affects most Canadians] Prime Minister Justin Trudeau is swiftly shooting down a parliamentary committee's recommendation that Ottawa impose a five per cent tax on broadband Internet services as a way to "level the playing field" in Canada's rapidly changing news industry. Liberal members of the Commons heritage committee have released a long-awaited report with 20 recommendations aimed at helping the slumping media industry adapt to significant business challenges brought on by technological changes and evolving consumer habits. *The majority report calls on Ottawa to apply the tax, levied on broadband Internet providers, to high-speed Internet services that allow for the streaming of music, movies and TV shows, but not to slower and cheaper services*.

An Internet tax would add hundreds of millions of dollars in revenues to the Canadian Media Fund, which already receives a levy on cable bills to finance the production of Canadian content. Speaking to reporters in Montreal after the report's release, Trudeau said he respects the independence of the committee, but rejects the idea of raising taxes on the middle class through an Internet broadband tax.

The committee report also recommends requiring the publicly funded CBC to eliminate advertising on its digital platforms; letting media companies deduct taxes on digital advertising on Canadian-owned platforms; and a tax credit for print outlets for a portion of their digital investments. [article provides debate on these issues]

Cellphone Unlocking Fees Banned By The CRTC 

http://www.huffingtonpost.ca/2017/06/15/crtc-bans-cellphone-unlocking-fees_n_17123254.html

[Not security news, just news that affects most Canadians] Cellphone companies will soon no longer be allowed to charge customers to unlock their devices, Canada's telecom regulator said Thursday as it unveiled sweeping changes to the wireless code of conduct. *The new code from the Canadian Radio-television and Telecommunications Commission also says as of Dec. 1, all newly purchased devices must be sold unlocked - one of several other changes aimed at giving people more control over their wireless services*.

The updated code, which originally came into effect in 2013, now stipulates: (a) Unsatisfied customers will be able to cancel contracts within 15 days, as long as returned devices are in near-new condition and customers haven't used more than half of their monthly usage, (b) Only the wireless account holder on family or shared plans can consent to overage and roaming charges, unless others on the plan are expressly authorized to approve the costs, (c) Data caps be tied to single accounts, no matter how many devices are listed on a shared plan, and (d) Wireless service providers cannot unilaterally change the key terms of a contract with a customer for voice, text or data services. The changes come six months after the regulator heard from consumer groups who accused some cellphone companies of violating the code, either passively or actively, and called for the rules to be tightened and enforced.

"The changes and clarifications we are announcing today will give Canadians additional tools to make informed choices about their wireless services and take advantage of competitive offers in the marketplace," CRTC chairman Jean-Pierre Blais said in a statement. "While they appreciate the code, (Canadians) told us loudly and clearly that it could be more effective. We have listened to them," said Blais, whose term at the helm of the regulatory body ends this week. *Banning unlocking fees could cost the big wireless providers a cumulative $37.7 million, which is what they collected in fees for unlocking roughly 943,000 devices in 2016, according to disclosure documents provided to the CRTC*. Carriers typically charge $50 to unlock a device, using the fees to discourage customers from switching service providers.

Consumer rights advocates applauded the changes, predicting they will provide Canadians with greater clarity about what to expect when they sign up for wireless services. ..The original code effectively killed three-year phone contracts, limiting them to 24 months. *But that led, in many cases, to higher monthly bills as the service providers were forced to recoup the cost of subsidized smartphones over a shorter period*.

198 Million Americans Hit by 'Largest Ever' Voter Records Leak

http://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/

A huge trove of voter data, including personal information and voter profiling data on what's thought to be every registered US voter dating back more than a decade, has been found on an exposed and unsecured server, ZDNet has learned. It's believed to be the largest ever known exposure of voter

information to date. The various databases containing 198 million records on American voters from all political parties were found stored on an open Amazon S3 storage server owned by a Republican data analytics firm, Deep Root Analytics.
UpGuard cyber risk analyst Chris Vickery, who found the exposed server, verified the data. Through his responsible disclosure, the server was secured late last week, and prior to publication. *This leak shines a spotlight on the Republicans' multi-million dollar effort to better target potential voters by utilizing big data*. The move was largely a response to the successes of the Barack Obama campaign in 2008, thought to have been the first data-driven campaign. Through a handful of companies, including data firms, market researchers, and analytics providers, the GOP replicated that Obama campaign strategy by helping its political candidates make data-based decisions about their campaigns. The exposed records include files provided by Data Trust, a data warehouse created by the GOP to serve as its exclusive data provider of voter records. The company sells and supplies voter data to political candidates, who rely on access to the data in order to shape their campaigns.
According to UpGuard, the folder includes dozens of spreadsheets containing a unique GOP identifier for each voter for the 2008 and 2012 presidential campaigns, which link to "dozens of sensitive and personally identifying data points, making it possible to piece together a striking amount of detail on individual Americans specified by name." A folder containing 2016 data only included files for Ohio and Florida, two crucial battleground states. Each record lists a voter's name, date of birth, home address, phone number, and voter registration details, such as which political party a person is registered with. *The data also includes "profiling" information, voter ethnicities and religions, and various other kinds of information pertinent to a voter's political persuasions and preferences, as modeled by the firms' data scientists, in order to better target political advertising*.
Senior executives at Data Trust would not speak on the record prior to publication. … Alex Lundry, co-founder of Deep Root, confirmed the company owned the Amazon S3 storage server, and said in an email that company has taken "full responsibility for this situation." ..We accept full responsibility, will continue with our investigation, and based on the information we have gathered thus far, we do not believe that our systems have been hacked," he said.
This isn't the first batch of voter data found by Vickery. Vickery, who we profiled on *ZDNet* earlier this year, found 87 million Mexican voter records in an exposed database in 2016. He was also responsible for discovering several US voter databases online totaling 18 million voters, and the state of Louisiana's entire database of 2.9 million voters. Deep Root's exposure also appears to be larger than the 191 million voter records exposed in late 2015, and another massive leak of 154 million voter records a year later.

Hackers Can Exploit E-Cigarettes to Hack Computers

https://www.hackread.com/hackers-can-use-e-cigarettes-to-hack-computers/

The manufacturers of Electronic cigarettes highlight the benefits to letting you lead a stress-free and healthy life, *what they certainly do not highlight was that the device could be used for malware distribution as well*. It's amazing what hackers can do these days. When it comes to malware, they prefer sending malicious attachments in an email but times have changed and these threat actors are coming up with new ways to target their victims. One of the new ways requires an e-cigarette or a vape pen and some modification to convert it into a hacking tool and infect a targeted computer.
Security researcher Ross Bevington (@FourOctets on Twitter) had *a presentation at BSides London that showcased an e-cigarette attacking a computer by tricking it to believe that it was a keyboard. It was also able to hack the computer by interfering with its network traffic. It is done because most of the e-cigs come with a rechargeable lithium-ion battery, which can be plugged into a cable or directly connects to the USB port of a computer*.
In a conversation with Sky News, Bevington said that: *"He had modified the vape pen by simply adding a hardware chip which allowed the device to communicate with the laptop as if it were a keyboard or mouse – A pre-written script that was saved on the vape made Windows open up the Notepad application and typed "Do you even vape bro!!!!"* It is unclear what kind of malware infection can be done through the e-cigarettes, however, based on WannaCry malware attack one can expect the worst, therefore, [should] be careful while using e-cigarettes or vape devices on their computer.
This is not the first time when news regarding e-cigarettes infecting computers has come out. In 2014, a company executive had their computer infected with a malware and no amount of cleaning, robust security or anti-malware protection was able to thwart the data compromise. The IT security experts failed to nail the problem and decided to investigate if executive routine had any changes. *It was then*

that they found out that the executive had switched to e-cigarettes in an attempt to quit smoking and lead a healthy life. The IT experts discovered that the charger of the e-cigarette was compromised and the moment it was connected to the computer, the malware would connect it to a remote server and download the malicious software.
To avoid such risks, it is advised to disable data pins on the USB and keep only the cable charge to prevent any information exchange between the devices it connects. Alternatively, use a USB Condom, a gadget that connects to USB and makes data pins ineffective.

PayPal Phishing Site Asks Victims to Submit a Selfie Holding Their ID Card

https://www.bleepingcomputer.com/news/security/paypal-phishing-site-asks-victims-to-submit-a-selfie-holding-their-id-card/

*A **PayPal phishing campaign** is luring victims to a hacked site where **a clone of the PayPal login page** is trying to trick users into giving away their PayPal credentials, payment card details, and ... a selfie of the user holding his ID card*. Brought to Bleeping Computer's attention by security researchers from PhishMe, the crook behind this operation relies on spam emails to drive users toward a PayPal phishing page hosted on a compromised WordPress site from New Zealand. At the time of writing, the phishing page had been removed, but following a classic pattern for phishing sites, users arriving on this page were asked to log in with their PayPal credentials. *There was no attempt to spoof the browser URL, so if users had any kind of experience with phishing pages, they would have immediately noticed they were on a page with the wrong address*.

Greedy crook wants more data. Once users entered their logins, the crook wasn't satisfied. At this point, it was obvious he's dealing with an inattentive or untrained user, so this phisher decides to go all-in and ask for more data. During a four-step process, the attack asks for the user's address, payment card data, and a picture of the user holding his ID card. It is unclear why the crook would ask for this information. *PhishMe expert Chris Sims believes it is "to create cryptocurrency accounts to launder money stolen from victims."*

A similar tactic was seen last year. *This tactic of asking a user for a selfie while holding his ID card has been seen before*. In October 2016, McAfee discovered a variant of the Acecard Android banking trojan that was also asking users to take a selfie holding their ID card when logging into their mobile banking accounts. The tactic was quite innovative at the time, and it got a lot of press coverage…

Hundreds of Malicious Android Apps Masked as Anti-Virus Software

https://www.hackread.com/malicious-android-apps-masked-as-anti-virus-software/

With the recent surge in ransomware attacks, it is no surprise to see that attackers have capitalized on the opportunity and played on people's fears by offering them *Android anti-virus apps that are, in reality, another malware*. It goes without saying then, that given the dangers and prevalence of ransomware, users have resorted to downloading various anti-virus apps in an attempt to avoid potential accidents. However, as RiskIQ, found, users need to be more careful as the anti-malware solutions might just be another prank disguised as authentic software. RiskIQ researched a number of apps that appeared to be anti-virus software and scanned them using its own mobile database. It was revealed that *most of them were simply another form of adware.*

A total of 6,295 Android apps popped up when the word "Antivirus" was searched and of the total, over 700 apps were shown in the blacklisted category, implying that in reality, the apps were not what they claimed to be. Moreover, the test was run to see how many apps have been listed on Google Play Store and the results showed that out of the 655 apps on Google play, 131 were blacklisted. It was also found that over 4,290 apps were active and 525 were blacklisted. Overall, it was revealed that Google Play had blacklisted 20% of anti-virus apps which was higher than the usual 11%. However, RiskIQ states that not all of the apps that are blacklisted may contain malware. Nevertheless, if an app is shown as risky by a trusted anti-virus vendor or by a group of them, then it is safe to say that a particular app is far from safe. Some of the apps scanned by RickIQ were: *"MP Security Antivirus App Lock, "Antivirus Malware Trojan," "Mobile Antivirus Security Info" and "Androids Antivirus" etc. ..As you can see, the best way to protect yourself is only to use legitimate and official websites and platforms to download anti-virus apps. Avoid downloading apps from third-party stores and always go through permissions an app is asking for. Stay safe online.*

US Blames North Korea Group Dubbed 'Hidden Cobra' for Domestic and Global Hacks

https://hotforsecurity.bitdefender.com/blog/us-blames-north-korea-group-dubbed-hidden-cobra-for-domestic-and-global-hacks-18222.html

A recent US Government Technical Alert (TA) issued by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), singles out a hacking group believed to be associated with the North Korean government and allegedly responsible for hacks of media, aerospace, financial, and critical infrastructure sectors. *Dubbed "Hidden Cobra," the alert includes details involving tools actively employed by the hackers, targets and* ***indicators of compromise (IoC)*** *that can help organizations defend themselves against them. While the analysis also includes a list of vulnerabilities allegedly used by the hacker group - ranging from Adobe Flash Player to Microsoft Silverlight and Hangul Word Processor - most have already been patched by newer distributions*. The alert also attributes the WannaCry incident, which involved a vulnerability in the SMB v1 Windows protocol, to the Hidden Cobra group, while urging independent security researchers to join the investigation to uncover the full extent of the group's full cyber capabilities.

"Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature," reads the alert. ..Cyber analysts are encouraged to review the information provided in this alert to detect signs of malicious network activity."

A distributed denial-of-service (DDoS) botnet infrastructure codenamed "DeltaCharlie" is also believed to be used by Hidden Cobra. The tool's capabilities range from downloading additional components to self-removal from infected machines. Proposed mitigation solutions include updating and patching operating systems and applications to their latest version, application whitelisting, restrictive administrative privileges, network segregation, firewalls, logging and access control lists. "We recommend that organizations *upgrade these applications to the latest version and patch level*. *If Adobe Flash or Microsoft Silverlight is no longer required, we recommend that those applications be removed from systems*," reads the alert.

4 School Districts in Florida Attacked By Moroccan Hackers

https://www.hackread.com/florida-school-districts-hacked-by-moroccan-hackers/

A group of hackers from Morocco allegedly tried to hack the US voting systems. In an attempt, they hacked four school districts from Florida. According to reports, several hacking attempts were said to be made on the US voting system and culprits were mostly believed to be from Russia. However, it seems that another group also wanted to try and interfere with the election. MoRo, a hacking group from Morocco, managed to breach defenses of four different school district networks. *Their main goal was to try and find their way into the sensitive government systems from there. The UDT (United Data Technologies), which is a company that investigates such attacks, has stated that* ***hackers managed to get into these networks via phishing attacks***.

Miami Herald reports that they managed to infect school networks through malware by sending infected images via email. Unsuspecting workers clicked on images, which was enough for malware to infect the devices. *A similar attack has also targeted one of the Florida city networks. Upon entering school systems, hackers remembered to turn off logs that recorded who entered the systems. This has made it very difficult to discover what exactly they did once inside*. Still, UDT analysts managed to find that hackers spent around three months in the system. They used this time to test defenses and map out the systems, and they even posted a photo of a man dressed as an ISIS fighter. The only named one of these four districts which were Miami-Dade, which is also the largest one in Florida. It is believed that attackers that hacked this and other three districts initially intended to steal personal data from thousands of students. Then they realized that they could access much more than that.

Apart from personal information, the school also handles Social Security numbers for former and current students, and also their parents. Not to mention all of the school employees. Still, they seem to have failed in obtaining any of this data, despite the three months of access. *Analysts even claim that hackers didn't manage to access voting systems at all*. *"They weren't just looking for the names of kids and valuable Social Security numbers, UDT found. The hackers were also searching for some way to slip into other sensitive government systems, including state voting systems."*

How An Office Printer May Have Led to Arrest of Alleged NSA Leaker Reality Winner

http://globalnews.ca/news/3515812/officer-printer-code-reality-winner/

[June9] The National Security Agency may have used a signature left by one of their office printers to track down Reality Winner, the U.S. woman accused of leaking top secret government information to an online news outlet. The NSA is accusing Winner, a U.S. intelligence contractor, of leaking a top secret National Security Agency report on Russia's interference with the U.S. elections to The Intercept in May. *According to a probable-cause affidavit from the FBI, Winner admitted to printing a copy of the intelligence report in her office and mailing it to the news outlet. The FBI says in the affidavit, the NSA saw The Intercept documents and determined they could have been printed*. "The pages of the intelligence reporting appeared to be folded and/or creased, suggesting they had been printed and hand-carried out of a secured space," the affidavit read.

Several security experts have pointed out that Winner may have revealed herself as the leaker, thanks to a hidden printer security measure. A pattern of tiny yellow dots on the leaked documents would have offered the government a way to track down the alleged leaker, security blogger Errata noted late this week. *The U.S. government requested in 2005 that the new model colour printers leave a unique stamp on documents. Errata points out the hidden dots are nearly impossible to see. But, if someone wanted to, they could take a screenshot and "invert the colours," to make the dots visible*.

According to San Francisco-based Electronic Frontier Foundation (EFF), a digital rights group, *the printed code is known as DocuColor and is printed in a rectangular grid of 15 by eight yellow dots on every colour page. The printer reproduces the same grid of dots over the entire page. The EFF designed a computer program to decode the series of dots. By manually entering the same pattern from a printed colour document into EFF`s decoder tool, the results will reveal a number of things including printer serial number, time and date the document was printed*.

Though the FBI said "an internal audit" revealed Winner had email communication with the news outlet, it's possible the printer Winner allegedly used may have led to her arrest. Winner was charged on Wednesday [June7] with a single count of willful retention and transmission of national defense information, a felony offense under the Espionage and Censorship Act. The charges carry a maximum sentence of 10 years in prison.

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

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