Security News Digest
October 24, 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”.

Sunday, October 29 is Internet Day which celebrates the origin of the very first internet transmission ever sent, and from it the utterly world-changing series of events that followed.

How to Celebrate Internet Day Why don’t you start your celebration of Internet Day by visiting the **original website**, which just so happens to still be online! Take a moment to gander at its high-quality graphics, it’s utterly sleek and streamlined design, and the sheer high-tech embodied by the first website ever. Absolutely stunning? No? Realize that at its time, this was the internet, this was how things were designed and put together. So low was the rate at which data could be transferred that images were to be a dream of a distant future, one that would come along swiftly, and with advances and innovations that couldn’t be imagined at that point.

TD Insider Says Bank Doesn't Want You to Know It's Outsourcing Work Overseas

http://www.cbc.ca/news/business/td-bank-outsourcing-fraud-india-1.4362324

Alyson Mosher knows a lot of private information about the TD Bank customers whose fraud claims she handles - and now, she says, that information is going to offshore workers without most people's knowledge. "They see your birth date, your social insurance number, whether you have a chequing account, a savings account, a line of credit, a mortgage, investments, Visa cards, anything," Mosher says. "They have access to your entire identity."

Mosher and her colleagues used to investigate fraud claims - cases where customers' Visa or debit cards were compromised, or used without the owner's knowledge. She contacted Go Public after becoming increasingly concerned about the amount of work TD has started sending overseas, instead of having it done by employees in the bank's Markham, Ont., fraud claims department. Over the past two years, Mosher says work has been transferred to people working in Hyderabad and Chennai, India. Go Public has confirmed those contract workers are employed by the outsourcing giant Tata Consultancy Services. "TD advertises a lot about 'trust'," says Mosher. "Customers are giving the bank a lot of personal information, trusting that it is in the right hands."

Complaint filed with privacy commissioner. Mosher is so concerned about the amount of customer information being shared offshore, she's filed a formal complaint with the Office of the Privacy Commissioner of Canada, alleging that TD is not being upfront with its customers. In her complaint, she describes how fraud investigations are processed in India, but if a call to a customer is required, the claim goes back to Canada for a representative to handle. "I believe this is being done to hide from the customer what processes and information is being sent offshore to India." "The customer is led to believe that I am the person working the claim and that I am the person receiving all of their documents and information," writes Mosher. "Not an agent in India. "I think if they were being upfront and honest, then they would have these agents from offshore on the phone. To try and hide that seems like they're trying to camouflage that they're sending your information to India." Mosher has no idea how many jobs have been created in India, but says a colleague sent to India to set up operations told her there were about 120 people doing fraud claims for TD.

TD's response. A spokesperson for TD Bank declined Go Public's request for an interview, but responded to questions in several emails. Spokesperson Mohammed Nakhooda denies that TD is trying to keep customers from learning their information is being handled offshore. He says Canadian workers do the customer contact because they are "trained customer service representatives" adding that TD makes "limited use of (offshore) vendors to complement work done by TD employees" and that none of the offshore jobs is permanent. He would not say how many fraud claims jobs have been created offshore, or why the bank didn't hire Canadians for those jobs, but said no one in Canada has lost their job because of the outsourcing.

But Mosher says that people who have left the department have either not been replaced, or been replaced by temporary contract workers. TD employs almost 60,000 people in Canada, but Nakhooda did not explain why the bank has moved work to India. **As for telling customers their information can been accessed by offshore workers, Nakhooda said that is spelled out in a clause on the bank's cardholder terms of agreement and on its website, noting that information may be shared with other parties worldwide.**

'Nobody reads cardholder agreement'. A leading privacy expert says it's "not acceptable" to expect customers of a bank - or any company - to read the fine print in the lengthy terms and conditions that often accompany products. "Nobody reads the cardholder agreement," says Ann Cavoukian, who served three terms as the information and privacy commissioner of Ontario, and now heads up Ryerson University's Privacy by Design Centre of Excellence. "I think transparency is very important in this day and age," says Cavoukian. "People want to know who can see their private information. That needs to be spelled out loud and clear, especially when there seems to be cyberattacks on a daily basis." Last month saw one of the largest data breaches in history. Equifax, one of the world's largest credit reporting agencies, got hacked, exposing the personal information of 143 million Americans and 100,000 Canadians.

In Canada, there's no way to know how many breaches there are, because unlike most U.S. states and European countries, no mandatory requirement exists for companies to report them - it's voluntary. According to the Office of the Privacy Commissioner of Canada, there were 100 voluntary breach reports between April 1, 2016, and March 31 of this year. One-quarter of those breaches occurred in the financial sector.

Personal data 'exposed'. Data security expert Marc-Roger Gagné says any time a company moves work offshore, it creates an opportunity for cyberattackers. "It gives them another point of entry, aside from the server in Toronto," says Gagné. "Your data is exposed at another end, instead of just one centralized area - Toronto. That is an exposure that wouldn't be there if the information was controlled and processed within Canada." TD Bank says its security teams "work diligently to protect data against unauthorized access and have implemented comprehensive measures to protect ... customers' information."

CLC president outraged. The president of the Canadian Labour Congress says he's outraged that TD Bank is creating jobs in India instead of Canada. "I think most Canadians would find this simply unacceptable," says Hassan Yussuff, pointing out that TD recently posted record profits. "There's no justification for this behaviour, other than to increase those profits." While TD's Nakhooda told Go Public that no one in Canada has lost their job, Yussuff says that's "disingenuous." If you're taking work from Canadian workers and moving it to another jurisdiction outside the country, there is job loss," he says. "I think it's fair for the federal government to say, 'We're going to bring in tighter regulations to ensure the banks are not going to offshore services that should be performed by Canadians in this country."

Many banks hiring offshore. TD Bank is not alone in its move to hire contract workers offshore. Go Public contacted Canada's other four big banks - **Scotiabank and RBC confirmed they use offshore workers**. BMO and CIBC would not answer questions about outsourcing. The Canadian Bankers Association told Go Public that banks outsource work to other countries to enable them to provide service efficiency for the best value and that the cost savings allow banks "to invest in areas that deliver greater value for the bank and its customers."

Reluctant whistleblower. Mosher says she wrote to TD's Whistleblower Hotline and only went public after her concerns weren't addressed. "We teach children that they should always stand up for what they believe in, but as adults we don't always follow that," she says. "If we all sit there ... nothing will ever change in this world."

Canada's 'Super Secret Spy Agency' is Releasing a Malware-Fighting Tool to the Public

http://www.cbc.ca/news/technology/cse-canada-cyber-spy-malware-assemblyline-open-source-1.4361728

Canada's electronic spy agency says it is taking the "unprecedented step" of releasing one of its own cyber defence tools to the public, in a bid to help companies and organizations better defend their computers and networks against malicious threats. The Communications Security Establishment (CSE) rarely goes into detail about its activities - both offensive and defensive - and much of what is known about the agency's activities have come from leaked documents obtained by U.S. National Security Agency whistleblower Edward Snowden and published in recent years.

But as of late, CSE has acknowledged it needs to do a better job of explaining to Canadians exactly what it does. Today, it is pulling back the curtain on an open-source malware analysis tool called Assemblyline that CSE says is used to protect the Canadian government's sprawling infrastructure each day. "It's a tool that helps our analysts know what to look at, because it's overwhelming for the number of people we have to be able to protect things," Scott Jones, who heads the agency's IT security efforts, said in an interview with CBC News.

'Super secret spy' reputation. On the one hand, open sourcing Assemblyline's code is a savvy act of public relations, and Jones readily admits the agency is trying to shed its "super secret spy agency" reputation in the interest of greater transparency. But on the other, the agency is acknowledging that, given the widening range of digital threats affecting Canadians and Canadian businesses, it believes it has a more public role to play in cyber defence than it has in the past. "This is something new for CSE," he says. It's a fact not lost on longtime agency observers.

"They're pushing the envelope in a way they haven't quite before," said Bill Robinson, an independent researcher who has studied CSE's activities for more than two decades, and recently joined the University of Toronto's Citizen Lab as a fellow. "It's a big a change, a sea change for them in that way."

The step may be unprecedented for CSE, but not for its partners in the Five Eyes - an intelligence-sharing alliance involving Australia, Canada, New Zealand, the United Kingdom and the United States. Both the NSA and the U.K.'s Government Communications Headquarters (GCHQ) have maintained active projects on the code sharing repository GitHub in recent years.

'A gift' for companies. Assemblyline is described by CSE as akin to a conveyor belt: files go in, and a handful of small helper applications automatically comb through each one in search of malicious clues. On the way out, every file is given a score, which lets analysts sort old, familiar threats from the new and novel attacks that typically require a closer, more manual approach to analysis. "There's only so many ways you can hide malware within a Word document," said John O'Brien, who leads the development of the tool, which first started in 2010. "So by looking for the hallmark of that type of an attack, that can give us an indication that there's something in here that's just off."

Cybersecurity researcher Olivier Bilodeau says although there is overlap between Assemblyline and existing tools, CSE's contribution is that it has cobbled together many of the tools that malware researchers already use into one platform, like a Swiss Army Knife for malware analysis that anyone can modify and improve. And it has demonstrated that Assemblyline can scale to handle networks as large as the government's. Bilodeau - who leads cybersecurity research at the Montreal security company GoSecure, and has developed a malware research toolbox of his own - says those attributes could make it easier for large organizations such as banks to do more of the kind of specialized work that his company does. "They usually spend a lot of time fighting the malware, but not a lot of time investing in malware fighting infrastructure," he said. "So this is definitely a gift for them."

Spying on spies. The possibility that CSE's own tool could be used to detect spy software of its own design, or that of its partners, is not lost upon the agency. "Whatever it detects, whether it be cybercrime or [nation] states, or anybody else that are doing things - well that's a good thing, because it's made the community smarter in terms of defence," said Jones. Nor does he believe that releasing Assemblyline to the public will make it easier for adversaries to harm the government, or understand how CSE hunts for threats - quite the opposite, in fact. "We believe that the benefits far outweigh any risks and that we can still use this to be ahead of the threat that's out there."

Facebook Canada Unveils Plan to Fight Fake News, Hacking in Lead-Up to 2019 Election

https://globalnews.ca/news/3814648/facebook-canadian-election-integrity-initiative/

Facebook has launched an “election integrity initiative” to help promote authentic dialogue and civic engagement in the lead-up to the 2019 Canadian federal election. The social media giant has come under heavy scrutiny over the use of its platform to display fake news stories and advertisements designed to influence the 2016 U.S. presidential election.
The Facebook news feed was infiltrated by several false and hoax stories during the hotly contested final stretch of the election, with its algorithms blamed for not rooting out intentionally misleading content. Facebook also admitted recently that tens of thousands of dollars were spent by Russian-linked operatives on advertising designed to stoke racial tensions among U.S. voters. To thwart similar problems besetting the Canadian democratic process, Facebook on Thursday unveiled its Canadian Election Integrity Initiative. The program will include a digital news literacy campaign targeting regular Canadians, “cyber hygiene” training for Canadian politicians, and the creation of a crisis hotline for politicians and political parties whose digital accounts have been hacked. **The initiative was designed to address specific challenges identified by the Communications Security Establishment’s (CSE) cyber-threat assessment report, said Facebook Canada’s head of public policy Kevin Chan.**
“We know that Facebook plays an important role in facilitating public dialogue,” Chan said in a press release. “That’s why we take the threats identified by the CSE very seriously and why we’re starting now to proactively address them.” Chan added that the Canadian initiative marked “the next step in Facebook’s global efforts with respect to election integrity.” The digital news literacy component of the initiative will run in partnership with MediaSmarts, an Ottawa-based non-profit organization focusing on media literacy. **Dubbed “Reality Check,” the program will look to promote research, foster education and release public service announcements to teach Canadians how to spot misinformation and false news online, something Chan labelled an “essential life and citizenship skill.”**
At a panel discussion to mark the launch of the initiative, Matthew Johnson, MediaSmarts’ director of education, said the modern digital environment behooves people to take responsibility when it comes to scrutinizing the content they come across. “We really, in many ways, can’t rely on other people to act as gatekeepers anymore,” Johnson said. “In the end, we today are responsible for filtering our own information, and we are responsible as a society for empowering everyone to be active citizens online, taking active steps to improve their online communities.”
Anatoliy Gruzd, research director of the Ryerson University Social Media Lab, said the Russian-led misinformation campaign underscored the importance of better social media education. “As Canada is one of the most connected countries in the world… I think it’s becoming very critical for us to understand how communication platforms such as social media influence what we see online and what we do offline.”
While ordinary Canadians learn to be more discerning when reading and sharing news articles, politicians will be taught to better protect their social media accounts.
To this end, **a cyber hygiene guide will be sent to all Canadian federal politicians and their teams, in an effort to empower them with best practice guidelines to deal with phishing and other cyber threats, while also arming them with strategies to secure their social media presence**. Politicians and political parties will also get access to a special cyber threats email line, effectively a “direct pipeline” to the Facebook security team, to help them get fast and streamlined responses to hacked pages and accounts. …In addition to empowering regular Canadians and lawmakers with new tools, Facebook says it’s also working towards greater advertiser transparency, faster reviews of inauthentic content and more effective identification of fake accounts.

Tech Firms to Remove Extremist Posts Within Hours 

http://www.bbc.com/news/technology-41693777

Tech giants Microsoft, Facebook, Twitter and Google have agreed to do more to remove extremist content within hours of it being posted. The accord was decided at a two-day meeting between the G7 nations and the tech firms, hosted on the Italian island of Ischia. The aim, according to officials, is to remove jihadist content from the internet within two hours. …Italy's interior minister Marco Minniti said they were "important first steps".
In a statement issued after the meeting, the G7 said: "We underscore the challenge to industry and we urge it... to develop solutions to identify and remove terrorist content within one to two hours of upload, to the extent it is technically feasible, without compromising human rights and fundamental freedoms." **It also urged the companies to develop better detection tools and to ensure all removed material is reported to authorities.** In September, UK prime minister Theresa May said technology companies

must go "further and faster" in removing extremist content. She said then that she wanted such content removed within two hours. MI5 head Andrew Parker said that allowing extremists "safe spaces online" made threats harder to detect. It is the first time that representatives from Google, Microsoft, Facebook and Twitter have taken part in G7 talks. The G7 consists of Canada, France, Germany, Italy, Japan, the UK and the US.

Digital Fingerprints: The Data You Leave Behind

https://www.forbes.com/sites/riskmap/2017/10/20/digital-fingerprints-the-data-you-leave-behind/#79ae583b7bce

In an age where electronic devices rule and data is easily accessible, staying connected to the world has never been easier. With thousands of public Wi-Fi hotspots across the globe, whether in a restaurant, on a plane or in your car, public Wi-Fi has become too convenient to ignore. But at what costs should you connect?

Understanding the risks of public Wi-Fi and the different ways in which your information, privacy and security are being compromised will have you think twice before joining an unsecure network. Connecting to public Wi-Fi is the equivalent of leaving your front door open when you leave your home. If no precautions are implemented you are welcoming hackers to ransack your device. When connected to public Wi-Fi your device sends information over the network in clear text, allowing hackers to view sensitive information with minimal effort applied.

Fake Wi-Fi Connections. Hackers will create a fake access point using any device with internet capabilities **to mimic the same name as a genuine Wi-Fi connection**. When the user connects to the fake Wi-Fi connection any data transmitted will go directly to the hacker.

How to protect yourself: Be cognizant of the Wi-Fi names populated on your list of available Wi-Fi connections. Review the list and be suspicious if two similarly named Wi-Fi connections are available. If you are trying to connect while at a well-known establishment (restaurant, café, place of business, etc.) speak with the staff onsite, have them provide you with the correct information. Additional precautionary measures are to always connect using a virtual private network (VPN). Utilizing a VPN establishes a level of encryption between the end-user and a website, intercepted data is unreadable without the correct decryption key.

Man in the Middle Attacks (MITM). Using public Wi-Fi makes the user vulnerable to MITM attacks. **Hackers will intercept information by breaking the direct connection between the client and the server, rerouting unencrypted data.**

How to protect yourself: Do not access websites that require you to login with your personal information; this information is vulnerable to data theft. When connecting to a website, review the URL to ensure an HTTPS (S- means secure) connection is being utilized.

Krack Attack

A newly discovered vulnerability known as the Krack Attack can be executed by an attacker who is within range of a Wi-Fi network. The attacker could sniff (view) the collection of information over an unencrypted network via the use of data packets. The gathered information can then be viewed using free software, to look for passwords, login credentials and additional private information captured during the users' public Wi-Fi session.

How to protect yourself: Be cognizant of the websites and information you enter over public Wi-Fi. Rely on the use of encryption such as HTTPS, VPN (Virtual Private Network) and SSL (secure connection) certificates (creates a secure and private connection).

Being Aware of your Surroundings. When using public Wi-Fi, be cautious of your surroundings, avoid visiting private websites, filling out applications which contain personal information and remain alert of individuals in your vicinity. It is very easy for someone to snoop over your shoulder and review the data you are entering or what you are typing.

Now that you are aware of a number of public Wi-Fi attacks, **here are some tips to help stay protected**:

(1) Use a VPN when connecting to a public network. A VPN creates a private and secure connection, encrypting your information providing the security necessary to keep your data protected. VPN services can be purchased and installed on all of your devices from laptops to mobile devices.

(2) Before connecting a computer (Windows or Mac) to a public network, make sure to disable sharing (network discovery, file and printer sharing). If kept enabled, you are allowing people the ability to access your device.

(3) Ensure that your firewall is enabled when on a public network. The firewall will protect you from unwanted and potentially harmful incoming connections.

(4) Purchase a subscription to a known hotspot service whether through your cellular provider (AT&T, Verizon, etc.) or a third party company such as Optimum or Verizon Jetpack.
(5) Keep your operating system and mobile applications up to date. Often the updates created for your operating system or applications pertain to security fixes needed to keep your device protected. When the updates are made available, the security hole becomes public knowledge; making your device vulnerable to attacks the longer it stays unpatched. By ensuring that you are running the "latest and greatest" versions of an operating system or application, limits your exposure to compromise.
With attackers looming in the shadows and technology driving the world, take the extra steps to protect your device/information. Always use best practices and ensure security when using public Wi-Fi.

Ransomware On The Rise: Dark Web Market Demand Up 2,500%

http://www.ibtimes.com/ransomware-rise-dark-web-market-demand-2500-2601378

The demand for ransomware attacks on dark web skyrocketed in the last year, with the marketplace showing a growth of more than 2,500 percent, according to a new report. United States-based cybersecurity company Carbon Black published a study titled "the Ransomware Economy" earlier this week that shows ransomware attacks are becoming increasingly more accessible across the dark web and will likely continue to present a threat to users around the world. To conduct the study, Carbon Black's researchers scoured the dark web for websites, hacking forums and marketplaces where users can buy and sell cyber attacks, including ransomware and other related services.
The experts at the cybersecurity firm found more than 6,300 destinations online where sellers were offering ransomware services and more than 45,000 advertisements marketing the products to potential buyers looking to launch an attack. The market for ransomware attacks featured a massive volatility in pricing, with attacks being made available for as little as just $0.50 and as expensive as $3,000. In many cases, the pricing for attacks were flexible, with some charging per target while others use fees charged a monthly or yearly rental fee. Also involved in the varied pricing model is just what type of service the buyer is purchasing. Ransomware-as-a-Service (RaaS) attacks, in which every aspect of the attack is managed through a single platform - from distribution channels to payment portals and decryptor tools to unlock files - often cost more.
Buyers can also buy more limited services that may provide just one aspect of an attack. Users can purchase individual ransomware strains to build an attack around, for example, and pay significantly less for the payload alone with no surrounding service. Flexible pricing models may make attacks seem cheap for users but are generating a significant amount of income for attackers. **Carbon Black reported some ransomware authors make more than $100,000 per year - well above the average salary for the average software developer, who make about $69,000 per year according to figures from PayScale.com**.
Those tempting revenue figures for ransomware authors are driven primarily by the newfound demand for the malicious software. Carbon Black reported ransomware marketplace sales on the dark web. The year-to-date figures for ransomware sales in 2017 shows total revenue at $6,237,248.90. By comparison, the sales figures from 2016 for ransomware didn't even crack a quarter of a million, totaling $249,287.05. That marks a total growth in sales of 2,502 percent. **Also on the rise as a result of the marketplace are ransoms extracted from victims who have their machine infected by the attacks. According to the FBI, ransom payments in 2016 totaled about $1 billion, up from just $24 million the year prior. One would expect the figures for 2017 to continue that trend of growth.**
2017 has included several of the highest profile ransomware attacks on record, including the WannaCry ransomware that infected more than one million machines in more than 160 countries and the Petya attack that spread to more than 65,000 computers - both of which relied on a stolen exploit from the United States National Security Agency to spread.

'IOTroop' Botnet Could Dwarf Mirai in Size and Devastation, Says Researcher

https://threatpost.com/iotroop-botnet-could-dwarf-mirai-in-size-and-devastation-says-researcher/128560/

A botnet, which is adding new bots every day, has already infected one million businesses during the past month and could easily eclipse the size and devastation caused by Mirai. The malware and botnet, dubbed IOTroop, was spotted in September by researchers at Check Point who warn that **60 percent of corporate networks have at least one vulnerable device**. **Similar to Mirai, the malware targets poorly protected network-connected devices such as routers and wireless IP cameras**

manufactured by D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys, Synology and GoAhead. **"So far we estimate over a million organizations have already been affected worldwide, including the U.S., Australia and everywhere in between, and the number is only increasing,"** according to Check Point's preliminary research published Thursday.

While this malware appears to share some of Mirai's code, it is new malware and campaign, said Maya Horowitz, group manager of threat intelligence at Check Point, in an interview with Threatpost. "This has the potential to be more damaging than Mirai," Horowitz said. "This is malware that has a much broader range of vulnerabilities to target across a much larger spectrum of products," she said.

In October 2016, Mirai malware spread itself to IoT devices gaining access via default password and usernames. The malware then roped affected devices into a botnet and carried out distributed denial of service (DDoS) attacks. The largest of such attacks flooded DNS provider Dyn causing several well-known websites to go dark for hours. Horowitz said the IOTroop malware Check Point is examining has similarities to Mirai, such as the recruiting of a global army of network devices capable of launching crippling DDoS attacks. "The most interesting difference between this malware and Mirai is that it is far more sophisticated. **Attackers are not just exploiting default credentials to compromise devices, but also using a dozen or more vulnerabilities to get on these devices**," she said.

In the case of the GoAhead wireless IP camera, attackers exploited a well-known bypass authentication vulnerability (CVE-2017-8225) identified in March and affecting more than 1,250 camera models. For other devices such as Linksys RangePlus WRT110 Wireless Router, adversaries are exploiting a remote command execution vulnerability known since 2014. This vulnerability exists because the router's web interface fails to sanitize ping targets and lacks the use of cross-site request forgery tokens for protection. Researchers said they have also identified several command-and-control servers used by adversaries behind the malware that update it with ranges of IP addresses to attack.

"Every infected device gets a range of IP addresses that are used to scan for these dozen or so vulnerabilities," Horowitz said. "The malware is mostly self-propagating, with minimal C2 intervention. But we are still studying the malware and reverse engineering it to better understand how it works."

"While we don't have the completed answers, we do know that the infected devices get a range of IP addresses that the malware is instructed to check for vulnerabilities. And then the IPs of the vulnerable devices are sent back to the C2," she said.

Researchers believe that the botnet is quickly amassing and may be on the cusp of a massive DDoS attack. "Our research suggests we are now experiencing the calm before an even more powerful storm," wrote researchers. Still unknown is who are the threat actors behind the malware/botnet, any targets hackers might have and what the timeline of any attack might be. "It is too early to assess the intentions of the threat actors behind it, but it is vital to have the proper preparations and defense mechanisms in place before an attack strikes," said researchers.

Android Apps Infected with Sockbot Malware Turn Devices into Botnet

https://www.hackread.com/android-apps-infected-with-sockbot-malware-turn-devices-into-botnet/

Cybercriminals apparently are well aware of the fact that Minecraft is a truly profitable game perhaps that's why they are eager on identifying new ways of exploiting it. **Reportedly, there are a number of Minecraft oriented Android apps available on Google Play Store that are infecting devices and turning them into botnets.** According to research conducted by Symantec's cybersecurity researchers, **eight apps on Google Play Store are infected with an embedded malicious Trojan called Sockbot**. The installation scope of this particular malware campaign is quite wide-ranged with approx. 600,000 to 2.6 million devices targeted so far. The apps initially posed as add-ons for Minecraft: Pocket Edition game to get posted at Google Play Android app store.

However, these are not official Minecraft game apps but only providing skins for changing the appearance of characters in the game. The apps have been designed to generate ad revenue through illegal ways. One of these eight apps was found to be communicating with a command and control server (C&C) for instructions to open a socket using SOCKS before creating a link with the targeted server. The C&C server provided a list of metadata and ads to promote ad requests. But in reality, the app is not meant to display ads but to compromise mobile devices for nefarious purposes. **After being installed on a device, the app asks for a range of permissions** including displaying of alerts, accessing GPS data, open network connections, access Wi-Fi service and acquire read and write privilege on external storage devices.

According to Symantec, the proxy topology is “highly flexible” as it can easily be extended to benefit from vulnerabilities of networks and also effectively span security parameters. Apart from executing “arbitrary network attacks,” the wide-ranging scope of this infection can be utilized to launch a DDoS (distributed denial of service) attack.
A developer using the alias FunBaster is identified to be linked with the malicious apps. It is noted that the developer signs every app with a unique developer key and has ensured that the coding of the app is obfuscated while the key string is also encrypted. If the code could be decrypted, it would be clear how the apps have managed to thwart security processes of Google to get posted on the Play Store. Google was notified of the presence of malicious apps on its Store by Symantec on October 6th after which the company removed them. However, there are tons of other malware-infected apps on Google Play Store that might trick Android users, therefore, avoid downloading unnecessary apps and use anti-virus software.

Credit Card Fraud Scheme Hit 5 States, Including Ohio

https://patch.com/ohio/cleveland/credit-card-fraud-scheme-hit-5-states-including-ohio

In a massive, 26-count indictment 12 people were charged for their role in a massive credit card skimmers fraud. **The group placed skimmers on gas pumps in at least five states**, including many locations throughout Northeast Ohio. “This group stole credit card information from thousands of people all over Northeast Ohio just looking to fill up their gas tanks and continue on their way,” U.S. Attorney Justin E. Herdman said. **“Instead, these victims had their personal information taken and used to make fraudulent credit cards, which this group in turn used to steal merchandise.”**
The skimming scheme took place between Aug. 2014 and July 2017. …**Herdman's office said the group would work together to distract gas station employees and install the skimmers**. Skimmers from the group were found on gas pumps in Rocky River, Solon, Stow, Hudson, Fairview Park, Medina, Cleveland, Canton, Cuyahoga Falls, Norton, Austintown and elsewhere, according to a release from Herdman's office. Skimmers were also located in Colorado, Maryland, Utah and in other places.
Once the information was captured, the suspects then reportedly re-encoded the stolen credit card info, including the actual account holders' names, onto counterfeit cards. They then purchased gift cards, merchandise, goods and services in places throughout Ohio and the nation, the indictment says. “This sophisticated, multistate criminal enterprise stole credit card numbers from innocent folks putting gas in their cars,” said FBI Special Agent in Charge Stephen D. Anthony. “These individuals, now in custody, caused financial difficulties for numerous everyday citizens, and for this, they will be held accountable.”
“This case is a complex investigation that involves suspects from multiple states that targeted innocent people from Northern Ohio and around the country stealing their personal and financial information,” said Secret Service Special Agent in Charge Jonathan Schuck. “The success of today’s arrests are due to the great collaboration of multiple law enforcement agencies working together.”

[U.S.] Government Drops Its Demand For Data On 6,000 Facebook Users

https://www.techdirt.com/articles/20171019/07133838437/government-drops-demand-data-6000-facebook-users.shtml

It's amazing what effect a little public scrutiny has on government overreach. In the wake of inauguration day protests, the Department of Justice (DOJ) started fishing for information from internet service providers. **First, it wanted info on all *1.2 million* visitors of a protest website** hosted by DreamHost. After a few months of bad publicity and legal wrangling, the DOJ was finally forced to **severely restrict** its demands for site visitor data.
Things went no better with the warrants served to Facebook. **These demanded a long list of personal information and communications from three targeted accounts, along with the names of 6,000 Facebook users who had interacted with the protest site's Facebook page.** Shortly before oral arguments were to be heard in the Washington DC court, the DOJ **dropped its gag order**.
The last minute removal of the gag order appears to have been done to avoid the establishment of unfavorable precedent. It looks like the government perhaps has further concerns about precedential limitations on warrants served to service providers. As Kate Conger reports for Engadget, **the DOJ has decided to walk away from this particular warrant challenge**.
*“In a court hearing today, **the Department of Justice dropped its request for the names of an estimated 6,000 people who “liked” a Facebook page about an Inauguration Day protest**, the*

American Civil Liberties Union said. The ACLU challenged several warrants related to protests against President Trump's inauguration on Friday, one of which included the search, claiming they were over-broad." The ACLU notes the judge seemed sympathetic to allegations of overreach. In response, the government has apparently reduced its demands to info from two arrested protestors' accounts and further limited the date range from which data is sought.

This isn't a good look for the government. Dropping demands before an order has been issued indicates the DOJ had some idea its demands were too broad. It also shows the government will make concessions, rather than risk adverse rulings. **Then there's the whole issue of seeking personal information on protesters.** This sort of thing creates a very real chilling effect by threatening to turn over personal information to the same entity the protesters were protesting. Fortunately, the government has walked back most of its demands in both cases.

Hackers Take Over Funeral Home's Email Account and Run Online Scams

https://www.bleepingcomputer.com/news/security/hackers-take-over-funeral-homes-email-account-and-run-online-scams/

Hackers have taken over the email account of a Louisiana funeral home and are sending email scams to the company's customers, asking for money. The hack took place on late Wednesday when employees of Griffin Funeral Home in West Monroe, Louisiana lost access to the company's Yahoo account, used as the main communications point with customers and business partners.

Hackers asked customers for money transfers. The hackers sent out emails posing as the funeral home's owner - Glenda Griffin - asking customers and suppliers for a favor. If the other party replied, hackers would ask for $2,450 to be paid in a Ukrainian bank account. They justified the request by saying that Glenda was on vacation in Europe and her cousin suffered an accident and needed urgent medical care. The scam was well put together as hackers had apparently studied the company and its owners before launching the campaign. As usual, they didn't pay too much attention to detail, as they forgot to copy Glenda's full email signature.

Employees said they detected something wrong after customers and partners called in to inquire about Glenda's supposed predicament. They realized they got hacked when they inspected emails in the Sent folder and saw the emails without the full signature, which was also supposed to contain a standard disclaimer.

Hackers wrestle control over the email inbox away from staffers. Funeral home staff changed the account's password, but hackers kept accessing the system. Employees changed the password four times before being locked out for good. The company reached out to Yahoo for help, but they have not heard back. They also filed a complaint with local police.

In the meantime, the company also changed its official email address and is now informing customers to ignore the recent emails and update their contact details. Speaking to local media a funeral home employee **recommended that companies change all passwords as soon as former employees leave, hinting at a possible source of the initial password leak**.

Domino's Blames Data Breach on Former Supplier's Systems

https://www.theguardian.com/technology/2017/oct/18/dominos-blames-data-breach-on-former-suppliers-systems

Domino's Australia has blamed a system "issue" of a former supplier for a leak of customer personal information to spam email lists. The pizza seller has called in the Australian information commissioner to investigate the breach but insists its systems haven't been compromised. Instead, it blames a "former supplier's systems" for leaking customer email addresses, names and store suburb.

"Domino's acted quickly to contain the information when it became aware of the issue and has commenced a detailed review process," an undated statement posted on the company's website reads. The company did not say when it first became aware of the issue and insists no financial information has been accessed.

Customers complained on social media about the "eerie" personalised emails and the lack of communication from Domino's Australia. "It was a bit eery [sic] getting all these spam emails that somehow knew my name and suburb and initially were making it past the spam filter," Mitchell Dale posted on Domino's Facebook page. "The decision to try to keep me in the dark and not announce what had happened is why I will not be ordering Dominos again." "Nothing better than waking up finding out your data has been breached," Dylan James posted on Facebook. "Why haven't you informed anyone

yet?" "I won't be ordering from you again, not because of the breach but because of how you chose to handle it," Lara Douglas posted.
Mandatory data breach notification laws will come into effect in February 2018, meaning organisations like Domino's will have to notify customers of any data breaches. The assistant minister for cybersecurity, Dan Tehan, advised people to watch for suspicious messages, links and attachments. "You should always be suspicious of unsolicited emails requesting personal or financial information," he said.
Domino's Australia says it ceased working with the former supplier in July.

Australia Warns Businesses about Sophisticated Cyberattacks

https://www.theguardian.com/australia-news/2017/oct/10/australia-warns-businesses-about-sophisticated-cyberattacks

An Australian company with contracting links to national security projects was caught up in one of **47,000 cybercrime incidents across the nation in the past year**. The unnamed business serves as Dan Tehan's warning to all companies that cybercrime is on the rise in Australia – and could affect anyone, as he launches the Australian Cyber Security Centre's (ACSC) 2017 threat report. In a speech to the National Press Club on Tuesday, the minister assisting the prime minister for cybersecurity will warn that in the past year, ACSC recorded a 15% increase in cyber incidents from the year before. Scams and frauds continue to rise despite the warnings, jumping by more than 20% in the past year, and accounting for more than half of all cybercrimes.
Tehan reports **7,238 cybersecurity incidents hit Australian businesses in the last financial year, while 734 were attacks on "private sector systems of national interest and critical infrastructure providers**". Among those was a business Tehan cited as an example that no one was immune – a company with links to national security projects hit by a "malicious cyber actor" in November 2016 through an unsecured network. "ACSC analysis confirmed that the adversary had sustained access to the network for an extended period of time and had stolen a significant amount of data," Tehan's speech says. "The adversary remained active on the network at the time of the ACSC investigation. "Analysis showed that the malicious actor gained access to the victim's network by exploiting an internet or public-facing server, which they accessed using administrative credentials. "Once in the door, the adversary was able to establish access to other private servers on the network."
But of greatest concern to Tehan was **the growing sophistication of the attacks**, which he described as "more elaborate than the attacks we have seen in previous years". "It is clear that the malicious actors looking to target major systems and critical infrastructure are increasing the sophistication of their vectors," his speech notes say. "But they are not alone. Like nation states, cybercriminals are using more complex methods to target businesses, large and small. **In particular they are using increasingly personalised techniques to trick their victims**."

Russian Agents Used Pokemon Go to Stoke Racial Tensions During U.S. Election: Report

https://globalnews.ca/news/3804067/russia-pokemon-go-election-meddling/

Even Pikachu aren't safe from Russian election meddling. That's the conclusion of a CNN investigation which found that Russian-linked operatives used the Pokemon Go gaming app - as well as other digital platforms - to stoke racial tensions in the U.S., as part of a campaign to meddle in the 2016 presidential election. Pokemon Go, which became a global sensation following its release in 2016, lets players collect virtual creatures, called Pokemon, from real-world locations. **Addictive gameplay aside, the app has also been harnessed for all kinds of marketing and awareness campaigns.**
One of them was "Don't Shoot Us," a contest that challenged players to find Pokemon in places where acts of alleged police brutality took place. Purportedly set up by the Black Lives Matter movement, the campaign encouraged players to name Pokemon characters collected in these areas after victims of police brutality, in order to spread awareness about the issue. It promised winners of the contest Amazon gift cards. **Only "Don't Shoot Us" wasn't run by Black Lives Matter activists, but a Kremlin-linked troll farm called the Internet Research Agency.** According to CNN, Russian operatives sought to use "Don't Shoot Us" to provoke protest among African Americans, with the aim of unsettling white Americans and making them perceive black activism as a threat.
Niantic, the makers of Pokemon Go, said it would look into the matter. "It's clear from the images shared with us by CNN that our game assets were appropriated and misused in promotions by third parties without our permission," the company said in a statement. "Niantic will consider our response as we learn

more." In addition to Pokemon Go, the Don't Shoot Us campaign also set up Facebook, Instagram and Twitter accounts, which have since been suspended. But a YouTube channel called "Don't Shoot" - which compiles hundreds of videos of alleged police brutality and racial profiling - was still active as of Saturday. On Friday, the Associated Press reported that Twitter presented U.S. Senate investigators with information about 201 "handles" or accounts linked to Russian attempts at influencing the election. Earlier in the week, Google, which owns YouTube, was reported to have uncovered tens of thousands of dollars in advertising spending traced to Russian operatives.

And Now, This:

Trump Campaign Staffers Pushed Russian Propaganda Days Before the Election

https://www.thedailybeast.com/trump-campaign-staffers-pushed-russian-propaganda-days-before-the-election

Some of the Trump campaign's most prominent names and supporters, including Trump's campaign manager, digital director, and son, pushed tweets from professional trolls paid by the Russian government in the heat of the 2016 election campaign. The Twitter account @Ten_GOP, which called itself the "Unofficial Twitter account of Tennessee Republicans," was operated from the Kremlin-backed "Russian troll farm," or Internet Research Agency, a source familiar with the account confirmed with The Daily Beast. The account's origins in the Internet Research Agency were originally reported by the independent Russian news outlet RBC. @Ten_GOP was created on Nov. 19, 2015, and accumulated over 100 thousand followers before Twitter shut it down. The Daily Beast independently confirmed the reasons for @Ten_GOP's account termination.

The discovery of the now-unavailable tweets presents the first evidence that several members of the Trump campaign pushed covert Russian propaganda on social media in the run-up to the 2016 election. A Twitter spokesperson declined to comment, "for privacy and security reasons." Two days before election day, Trump campaign manager Kellyanne Conway tweeted a post by @Ten_GOP regarding Hillary Clinton's email. "Mother of jailed sailor: 'Hold Hillary to same standards as my son on Classified info' #hillarysemail #WeinerGate" the tweet reads.

Three weeks before the election, Brad Parscale, the Trump campaign's digital director, retweeted a separate post from @Ten_GOP. "Thousands of deplorables chanting to the media: 'Tell The Truth!' RT if you are also done w/ biased Media!" the tweet read. President Trump's son Donald Trump Jr. followed the account until its closure on Aug. 23 of this year. Trump Jr. retweeted the account three times, including an allegation of voter fraud in Florida one week before the election. "BREAKING: #VoterFraud by counting tens of thousands of ineligible mail in Hillary votes being reported in Broward County, Florida Please, RT," the tweet read. Trump Jr. also retweeted the account on Election Day. "This vet passed away last month before he could vote for Trump.. Here he is in his #MAGA hat.. #voted #ElectionDay," the account wrote.

Former Trump national security adviser Michael Flynn retweeted the Russian-backed troll account at least once. His son, Michael Flynn Jr., retweeted the account 34 times before it was removed from Twitter in August for its ties to Russian propaganda. The account notably pushed for Flynn's reappointment as Trump's national security adviser, a job Flynn lost after press revelations that he'd lied about his telephone discussions with the Russian ambassador after the election hacks. It also repeatedly pushed Breitbart-backed talking points, including a fake news story about a gang rape in Twin Falls, Idaho, that merited dozens of articles from Breitbart News. Flynn Jr. will likely receive a Senate subpoena after he refused to be interviewed for the Senate Intelligence Committee's Russia investigation, ABC News reported on Tuesday.

Former Trump campaign advisor and longtime confidante of the president Roger Stone retweeted the account three times in 2017, twice to rail against commentators on CNN. On the same day as the account's permanent ban, @Ten_GOP was caught passing a photo of the 2016 Cleveland Cavaliers NBA Championship parade in Cleveland as a picture of the crowd gathered outside a Trump rally in Phoenix. Last March the account was one of the most active in promoting WikiLeaks' first big release of CIA documents, **using the occasion to float the false claim that the so-called Vault 7 documents acquitted Russia in the hack of the Democratic National Committee**. "BREAKING: Obama's CIA posed as RUSSIAN HACKERS to disguise their dirty work," read one of the tweets. "The 'Russian hacking' was a false flag by the CIA. It was done to give Obama a reason to spy on Trump!" read another. Overt Russian propaganda outlets Sputnik and RT frequently used @Ten_GOP's tweets in their

news stories, including a story titled “Russia has no compromising info on Trump or Clinton, report is ‘total bluff’ - Kremlin.”
Far right news sites The Gateway Pundit and InfoWars quoted the account in articles several times. Fox News cited @Ten_GOP as its sole example of a “Trump fan” in an article titled “Trump fans call for Kellogg’s boycott after brand pulls Breitbart ads” last December. Former FBI counterterrorism agent Clint Watts, who testified to the Senate Intelligence Committee on Russian cyberattacks, told The Daily Beast that this is “exactly what I was talking about” in his testimony in March. “If what you said is true, I’d say, ‘My job is done,’” said Watts. “If this account is definitely an (Internet Research Agency) account, it proved Russian Active Measures (like the 2016 propaganda campaign) works, because Americans will use it against other Americans.” Watts said the content of these pages is “made to look organic” so that “Americans will use it against their political enemies.” **“If you take rumors, false information, plants, and just repeat them, you’re doing the job of a foreign country. They are seeding out information or narratives they know candidates or partisans will use. They were so effective, they had the very top people in the campaign using it,”** said Watts. “Basically, Russia loaded the gun. The Trump team fired.”
Mike Hasson, chief strategist of the Republican data analytics firm Red Metrics, said he remembered seeing the account as far back as the primaries, but became skeptical of the account due to a “couple odd things that stood out.” “I remember seeing it in late primary season, showing up in my timeline, retweeted by ordinary grassroots people. Some of the stuff was conspiracy theorist and inflammatory, but other times the content was intended to be inspiring and heartwarming,” said Hasson. Hasson said he became more confident of Ten_GOP’s origins after the account stopped tweeting about Tennessee and started tweeting about nationalist French presidential candidate Marine Le Pen, then tweeted several links from Russian propaganda network RT.
“For it to jump from Tennessee-related stuff and national stuff to Le Pen, that was probably the trigger point - like, ‘OK, maybe there is something here that’s a lot worse,’” said Hasson. “At that point, it was much more than just suspicion. That was more of a confirmation,” he said, of Russia Today’s frequent citation of the account. “By that point, it had accumulated enough red flags that I felt pretty sure that this was one of the bad guys.” The account was retweeted 15 times by far-right agitator Ann Coulter, who also posted one of its tweets to her Twitter account.
Last month, after the account’s closure, someone launched a petition on the White House’s “We The People” site complaining about “a war on conservatives on Twitter.” The petition demanded the reinstatement of several alt-right Twitter accounts that had been suspended from the service, adding “My own account, @Tennessee_GOP, was banned on August the 23th.” The petition misstates the name of the @Ten_GOP account, but came at around the same time as two more White House petitions protesting Facebook’s deletion of fake African American and progressive political accounts linked to the Russian active measures campaign. None of the petitions received enough signatures to qualify for a White House response.
Others in Trump’s inner circle, including former deputy national security advisor Sebastian Gorka, also retweeted Russian-tied Twitter accounts. Despite posing as Tennessee Republicans, the account never hesitated to push the Kremlin’s talking points on issues like Syria and the French election. In May, the anonymous operator of a Twitter account called AltCyberCommand used Twitter’s password reset process to try and prove Russia’s involvement. **A video of the hack appeared to show that TEN_GOP’s Twitter account was set up with a phone number in country code 7, indicating the Russian Federation, not Tennessee.**

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

****