BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
January 23, 2018

Be a Security Star in 2018 by taking the ‘Security New Year’ Quiz

Tax Scams on Increase in Victoria, Police Say

http://www.timescolonist.com/news/local/tax-scams-on-increase-in-victoria-police-say-1.23147658

Canada Revenue Agency scams are increasing in Victoria, say Victoria police. “So far in 2018 alone, losses reported to VicPD as a result of the scam have totalled $25,000,” police said in a statement on Wednesday. “**Investigators are also seeing more spoofing [impersonating/ falsifying] of phone numbers** where, in one investigation, the victim divulged his accountant’s information then moments later got a call from his ‘accountant,’ which really was one of the fraudsters.”

These scams come in the form of unsolicited calls. Fraudsters are often aggressive, police said. Potential victims are told that they committed fraud on their tax returns and are facing legal action. “Often, the fraudster claims police are on their way to arrest the potential victim unless he or she pays an immediate reduced fine,” police said. “With the scammers often calling from overseas locations, once paid, victims are often left with little recourse to recover their lost funds.”

The Canada Revenue Agency never contacts people over the phone to discuss fraud concerns, and never threatens arrest over the phone, say Victoria police fraud investigators. It also does not accept payment in Bitcoin, a digital currency. If you have concerns after being contacted by someone claiming to be from the CRA, you can call the CRA yourself at 1-800-959-8281. With fraudsters targeting older individuals, investigators recommend speaking to relatives and friends about the scam.

Police Probing Bell Canada Data Breach; Up to 100,000 Customers Affected

https://www.theglobeandmail.com/report-on-business/police-probing-bell-canada-data-breach-up-to-100000-customers-affected/article37701579/

Police are investigating a new data breach at Bell Canada, which says **hackers have illegally obtained customer information, primarily subscriber names and e-mail addresses**. BCE Inc.-owned Bell confirmed Tuesday that up to 100,000 customers were affected by the hack, which comes **about eight months after hackers accessed nearly 1.9 million Bell customer e-mail addresses as well as 1,700 names and phone numbers**. "We apologize to our customers and are contacting all those affected," said BCE spokesman Mark Langton. "There is an active RCMP investigation of the incident and Bell has notified appropriate government agencies including the Office of the Privacy Commissioner."

Mr. Langton said that, in this case, hackers accessed names and e-mail addresses and "in some cases phone number, user name and/or account number." He added **there was "no indication that any credit card or other banking information was accessed**." Several customers on Tuesday reported receiving an e-mail from John Watson, executive vice-president of customer experience at Bell, informing them that some of their customer information was illegally accessed. Mr. Watson apologized for the breach and advised affected subscribers: **"It is good practice to change your passwords and security questions frequently and to regularly review all your service and financial accounts for any suspicious activity." Even non-financial information such as user names can be used by hackers** to attempt to break into other accounts owned by the same person, and e-mail addresses can provide a potential list of targets for social engineering scams known as phishing, in which hackers try to convince people to click on malicious links or attachments.

Mr. Langton said Bell - which is Canada's largest communications company and has almost 22 million combined wireless, television, internet and home telephone customers - works closely with police and other government agencies to address cyber crime, adding, "we have successfully supported law enforcement in past prosecutions of hackers."

Payment Scam Using Administration Cards Costing Calgary Businesses Thousands

https://globalnews.ca/news/3969385/payment-scam-using-administration-cards-costing-calgary-businesses-thousands/
[Jan16] A Calgary restaurant is trying to warn other businesses about a scam it says is making the rounds in the city. Around 8:30 p.m. Saturday night, Chianti Cafe & Restaurant's surveillance video captured a man entering their establishment to pick up a takeout order. He paid his bill for $88.11 cents using a MasterCard, adding a $20 tip. But when the payment went through, it was for a total of $902.11. "I thought I made a mistake entering the money. So I refunded the money," general manager Todd Duly said, adding he thought he had somehow charged the customer $881.11 instead of the $88.11 owing. **The total was refunded back to the client, without staff realizing he had swapped the original MasterCard used for payment with a debit card for the refund.**
"Everything looked like it was above board until I looked at the small print and I was like, 'Wait a minute. Something's up here.'" It was only when Chianti reported the problem to payment processing company Moneris that they realized what had happened: **Moneris told them the customer had used an administration card to change the amount owed, and the original MasterCard that was billed in the sale had been stolen**. "We phoned Moneris and they said they couldn't do anything about it," owner Barbara Masterson said. "They knew that we were scammed. **They said that he did use an admin card to change the settings** and there was nothing they could do."
After posting the surveillance video to Facebook, Masterson said she soon realized her business wasn't alone. Reports of similar scams came pouring in from several businesses all over the city. "They had somehow manipulated the machine with an administrative card and had manually put something in and then had it refunded to a different card. So we ended up being out a couple thousand dollars," Dennis Madden, general manager of the Calgary Rose and Crown said. Various Mr. Sub locations have also been hit by a similar scam, costing the company over $1,600. Surveillance tapes appeared to show the same man that Chianti captured Saturday. It's not just restaurants that are being targeted by this type of scam. Great Clips hair salon said over the past year they've seen a similar scam attempted, hitting at least five of their locations in Okotoks and Calgary. "They would proceed to put through a tip amount of about $900. It seemed to be the same on just about every single transaction. They realized that it's a mistake and then say, 'That's a mistake, I need a refund,'" regional manager Rita Alberto said.
Moneris said in a statement to Global News on Tuesday that while it can't discuss the details of merchant accounts, it is "currently investigating the events with our fraud and risk team." "Moneris takes issues of fraud seriously," the statement reads. "We actively provide merchants with tips and guidance to avoid fraud. When a merchant starts working with Moneris, we provide documentation on proper card acceptance and device management procedures as part of the merchant agreement and operating manual." The company went on to say it also provides clients with resources to help identify potential fraud situations. A Calgary police investigation into the matter is ongoing, but businesses aren't wasting time warning others about the scam. **"These machines should be safe. Nobody should be able to change these machines,"** Masterson said. "It's not the restaurant's fault. It's not the waiter's fault. People need to be aware. **They need to put passwords on their machines** and these companies need to make us aware of that."

How To Keep Personal Data Safe When Companies Can't (Or Won't) 🇨🇦

http://www.huffingtonpost.ca/ale-brown/how-to-keep-personal-data-safe-when-companies-cant-or-wont_a_23331062/
Organizations came under fire in 2017, a year of reckoning for businesses on how they managed corporate and personal data. The increase in cyberattacks, and in particular the use of ransomware, has become so pervasive that an underground ransomware market has developed in strength. **According to Carbon Black, the number of ransomware applications available for purchase, which currently accounts for approximately 45,000 different ransomware products, has grown from US$250,000 in 2016 to US$6.25 million in 2017. A staggering 2,500 per cent increase.**
The stats continue with ransomware payments from affected individuals and organizations totaling close to $1 billion dollars in 2016, up from $24 million in 2015. Ransomware is becoming sophisticated, easy to access and, most important of all, the best way to make a profit out of malware. One thing is clear: cyberattacks, in their many forms, are here to stay. But the question remains are organizations incentivized to prioritize our safety, or are they more driven by self-preservation?
A tale of two cyber gaffes - Equifax and Uber were two high-profile cases last year that rocked consumer confidence and suggested the latter - self-preservation. The lack of privacy management processes shown by the two companies before, during and after the breaches have resulted in them

facing serious financial and legal consequences that have significantly hindered both their profits and their credibility. These are lessons worth learning for other businesses. Thinking of other long-lasting implications, such as loss of customer trust and reputational damage, some companies may be forced to close their doors completely. [go to this lengthy article for comments on Equifax and Uber]

Consumer impact: another important consequence of a data breach:

Data breaches can have very hefty financial implications for a consumer. **A consumer will spend on average about 20 hours and $770 on lawyers and time lost to resolve the case when they find themselves on the receiving end of a data breach.** …The most dangerous misconception consumers can have when it comes to data privacy is eschewing their share of the responsibility. Consumers have a stake in how they control their personal data and they need to act on it.

Lessons to learn: [Important Advice on Protecting Your Information]

These are some of the takeaways on what to do if you find out your personal data has been compromised by a cyberattack or a privacy breach incident:

Stay alert and be proactive- First and foremost, make sure you know what businesses have your data and how they use it. If you receive letters or emails from companies you don't recognize, call them and ask them how they obtained your information. If a company informs you of a breach, change your account passwords, be mindful of phishing emails and if you believe your credit or debit card numbers have been compromised, reach out to the credit card company or banking institution and request a new card. Keeping an eye on your credit score for a period of time doesn't hurt, either. Protecting personal data is paramount in moving forward to continue fostering this trust and loyalty.

Make a complaint to the appropriate regulators- In Canada, there are different regulators responsible to ensure that personal data is managed appropriately. If you feel a company is not using your personal data as per your expectations or if you believe your data has been compromised, you have the right to reach out to the Office of the Privacy Commissioner of Canada or to the local privacy authorities in your province. In the case of complaints around email communications, the Canadian Anti-Spam legislation (CASL) is enforced by the Canadian Radio-television and Telecommunications Commission (CRTC) and they take these complaints very seriously.

Ask the organization for identity theft monitoring services- When there is a data breach and an organization gives you notification, in most cases they offer identity theft monitoring services. If they don't, demand that they provide such services since you are certainly at a higher risk of identity fraud and the implications that this conveys. Identity theft monitoring usually includes insurance that will cover any costs related to an identity theft incident so it is very important to ensure you are protected.

Request the organization to erase your data- If you experience a breach and you don't feel you will do business with this company due to lack of trust or simply because you are not interested anymore, ask them to erase whatever personal data they have that belongs to you to ensure that if an incident occurs in the future, you are not impacted by it again.

Moving forward in the cyber world- .. The world of cyberattacks is here to stay, and my advice to consumers is to stay vigilant - and remember that you have options. Ultimately, protection of your personal data is in your hands.

Infant Social Security Numbers are For Sale on the Dark Web

http://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html

The personal details of children - including dates of birth and mother's maiden names - have been sought after for years. Now, researchers have found an ad on a forum for the sale of data claiming to be from infants. The cost: $300 worth of bitcoin for each baby's data set. **An infant's personal information can provide cybercriminals access to a clean credit history.** This can be used to take out mortgages, apply for credit cards or receive government benefits. Because child identity theft schemes can go undetected for years, often until they're old enough to open up a credit card account, their data is considered especially valuable.

The ad read "get em befor tax seson [sic]" - a nod to the busiest time of year for identity theft. It was posted on a dark web marketplace only accessible through software called Tor. The dark web refers to a networks of websites that require specific software to access. Some dark web sites are known for criminal activity. On some dark web forums, cybercriminals can take classes on how to steal credit card data. Members of these forums also sell "fullz," a slang term for full sets of people's personal information. The listing for infant data was discovered by researchers at Terbium Labs, a dark web intelligence firm. The cost and age of the alleged victims came as a surprise to Emily Wilson, the company's director of analysis. **Although the firm has seen child data for sale before, this was the first time it has seen infants' data for sale.** "It's unusual to have information specifically marked as belonging to children or to infants on these markets," Wilson said. The interest is not surprising. According to a 2011 report from Carnegie Mellon University's CyLab, **the rate of child identity theft is 51 times higher than for adults** (whose data sets cost about $10 - $25 on dark web markets).

Identity theft can have a lingering effect on a child's financial history. Christina Warren - a former reporter who now works for a large tech company - was about 12-years-old when she started receiving credit card bills. After collection notices piled up, her parents had to convince creditors her identity had been stolen. Credit reporting agencies said they fixed the issue, but she later had trouble getting her first credit card. "It was a massive headache," Warren told CNN Tech. "I didn't realize until six years later that it was still ongoing." Even now, Warren, 35, doesn't know how her identity was stolen. Before the internet became a playground for hackers, low-tech methods included mail theft, burglary, phone scams or taking advantage of lost or stolen wallets, said Eva Velasquez, president and CEO of the Identity Theft Resource Center.

Now, it's easier than ever for criminals to steal personal data, thanks largely to the growth of sophisticated phishing attempts, major data breaches and more credit card applications and taxes filed online. In 2017, the Equifax breach alone exposed Social Security numbers and other personal information of more than 145 million people. Lisa Schifferle, an attorney with the FTC's Division of Consumer and Business Education, said Social Security numbers are the main component of child identity theft. "It [doesn't always have to be in] the child's name," Schifferle said. "Sometimes thieves use Social Security numbers in connection with a made-up name or their own name." **When personal data is dumped online, it takes only a few minutes before people try to exploit it, according to a FTC report conducted last year.**

The FTC currently provides resources for parents who think a child's identity may have been stolen, and tips for keeping their information safe, starting from the time he or she is a baby. Velasquez said **parents should keep an eye out for signs that their child's information has been stolen.** This may include receiving an alert when a Social Security number has credit history when you file your taxes or if a child is receiving a jury summons. After numerous phone calls and verifying documentation, Warren and her parents eventually straightened out the issue. "[One thing I learned is to] **keep documentation and paperwork for everything," said Warren, noting identity theft victims may be asked to prove the situation was sorted**.

Top 500 Legal Firms have Over a Million of Their Credentials Leaked on the Dark Web

https://wccftech.com/top-500-legal-firms-data-breach/

UK - Hackers have dumped files in the Dark Web containing nearly 1.2 million email addresses and credentials from the UK's top 500 law firms. Security researchers from RepKnight cybersecurity firm revealed earlier today that over **1,159,687 email addresses were found in the dump and over 80 percent of these were linked to leaked passwords**. The firm, however, adds that most of this data doesn't come from any direct attacks and is a result of several third party breaches. But that doesn't mean it isn't damaging for the law firms who are now at risk of attacks since many of these passwords in plaintext are expected to work despite the security breach notifications.

"Legal firms have access to some of the most sensitive data imaginable about their clients – whether corporate or private," the researchers wrote. "And just like any other company, they hold personal information about their employees, such as home address, contact details, bank account numbers and pension information."

But just how secure is the average law firm? The researchers analyzed the "dark web footprints of domains belonging to the top 500 law firms in the UK, and discovered details of more than 1 million hacked, leaked or stolen credentials being circulated online – that's an average of 2,000 email addresses per firm." Every single of these top 500 law firms had at least 1 credential exposed, with the largest one accounting for 30,000 leaked email addresses. **Most of this data made it to the dark web because legal professionals used their work emails to sign up for websites and services (like LinkedIn, MySpace, Tumblr, etc) that were later breached.**

While email addresses alone put users at risk of phishing attacks, passwords make things worse. **Leaked passwords not only puts that person but an entire network at risk of credential stuffing attacks**, the researchers wrote. **In these attacks, bots are used to repeatedly try the same username and password on multiple sites.** [Note: This is exactly why security best practices repeatedly tell users to use different passwords for their separate accounts.] Then, there are spear phishing attacks or identity fraud, where leaked credentials are used as part of a targeted cyberattack on that individual. "The data we found represents the easiest data to find as we just searched on the corporate email domain," Patrick Martin of RepKnight said. "A far bigger issue for law firms is data breaches of highly sensitive information about client cases, customer contact information, or employee personal info such as home addresses, medical record and HR files," he added. "That's why, in addition to securing their networks, every firm should be deploying a Dark Web monitoring solution, so they can get alerted to leaks and breaches immediately."

Go Ahead and Put Your Password on a Post-It Note

https://motherboard.vice.com/en_us/article/7xeqe9/hawaii-emergency-password-post-it

Many are shaming the Hawaii Emergency Management Agency for keeping passwords on post-its, but the practice isn't always a terrible idea. On Saturday, people in Hawaii and across the world panicked after the local government alerted of an incoming missile. Luckily, the alert was just a false alarm caused by an employee clicking the wrong button on his computer. After the panic came the reckoning. How could the Hawaii Emergency Management Agency make such a mistake? The Federal Communications Commission announced that it would investigate the "absolutely unacceptable" mistake, as FCC commissioner Ajit Pai put it. Then, someone found a photo from July showing a HEMA officer posing in front of computer screens adorned by a couple of post-its. One of them, as it turns out when you zoom in carefully, spells out: "Password: warningpoint2." The internet caught on and began making fun of HEMA and its terrible [security operations]. "These people are just as incompetent as you'd expect from a gov't employee," said someone on Twitter. Another joked: "The deep state apparently uses Password Post-it Keeper™." "You have to write your password on the back of the post-it note to be secure," wrote a Redditor.

In reality, however, it's usually OK to have a password printed on a sticky note. Of course, that depends on what password we're talking about (please don't use 123456 as a password EVER), what screen it's attached to, and whether photographers or TV crews are coming to film your office. In other words: it depends on your threat model.

If you have a faulty memory and want to make sure you can unlock your home computer with your new multi-word passphrase, then by all means put the password on a piece of paper until you memorize it. You could even use a physical, offline password manager for your passwords [also referred to as a paper notebook]. **That's much more secure than writing down all your passwords in an unencrypted text file on your computer. Or reusing the same passwords for all your accounts. Generally speaking, the risk of someone breaking into your home to read that sticky note or notebook is much lower than someone infecting your computer with malware and then accessing all your passwords**, or than someone getting your old password from a hacked video game forum and then using it to steal money from your PayPal account that has the same password.

In general, we still recommend software password managers. But don't listen to the security absolutist and tweet-shamers who are gloating over what is admittedly a mistake on behalf of HEMA. Think about what your threats are, and how to protect against them. That's how you, and everyone else, will be more secure. Of course, if you're working at a sensitive government post, you need to worry about a lot of things - especially if you broadcast your office to the world.

Russia-Linked Attacks on Political Organizations Continue

http://www.securityweek.com/russia-linked-attacks-political-organizations-continue

The cyber-espionage group known as Fancy Bear was highly active in the second half of 2017, hitting political organizations worldwide, Trend Micro said this week. Also known as *APT28, Pawn Storm, Sofacy, Group 74, Sednit, Tsar Team,* and *Strontium*, the group is said to have ties with the Russian government. Since 2015, the group has been associated with attacks on political organizations in France, Germany, Montenegro, Turkey, Ukraine, and the United States. During the second half of 2017, such attacks continued, without revealing much technical innovation over time. However, the attacks are well prepared, persistent, and often hard to defend against, the security researchers say.

"Pawn Storm has a large toolset full of social engineering tricks, malware and exploits, and therefore doesn't need much innovation apart from occasionally using their own zero-days and quickly abusing software vulnerabilities shortly after a security patch is released," Trend Micro points out. During the second half of 2017, the group was observed targeting organizations with credential phishing and spear phishing attacks. In August and September, **the hackers used *tabnabbing* against Yahoo! users, a method that involves changing a browser tab to point to a phishing site after distracting the target**.

In attacks observed in October and November 2017, the group used credential phishing emails to target specific organizations. One incident employed an email claiming to inform the target of an expired password, while the other claimed a new file was present on the company's OneDrive system. **During the past six months, Pawn Storm also targeted several International Olympic Wintersport Federations**, including the European Ice Hockey Federation, the International Ski Federation, the International Biathlon Union, the International Bobsleigh and Skeleton Federation, and the International Luge Federation. The attacks appear to be related to several Russian Olympic players being banned for life in fall 2017. A recent incident involving the leak of emails exchanged between officials of the International Olympic Committee (IOC) and other individuals involved with the Olympics also appears to be related to the state-sponsored actor.

Some of the group's political targets included *chmail.ir* webmail users, who received credential phishing emails on May 18, 2017, one day before the presidential elections in Iran. Similar incidents were observed targeting political organizations globally, Trend Micro says. In June 2017, the actor set up phishing sites mimicking the ADFS (Active Directory Federation Services) of the U.S. Senate. In attacks observed during fall 2017, the group was abusing Google's Blogspot service to target Bellingcat, a group of investigative journalists that uses open source information to report on various events taking place around the world.

Individuals interested in the CyCon U.S. conference organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in collaboration with the Army Cyber Institute at West Point were also targeted by Pawn Storm last year. Moving forth, the group is expected to continue targeting political organizations, while also likely focusing on influencing public opinion via social media, given that social media algorithms are "susceptible to abuse by various actors with bad intentions."

"Publishing stolen data together with spreading fake news and rumors on social media gives malicious actors powerful tools. While a successful influence campaign might seem relatively easy to do, it needs a lot of planning, persistence, and resources to be successful. **Some of the basic tools and services, like ones used to spread fake news on social media, are already being offered as a service in the underground economy**," Trend Micro notes. Other actors too might start campaigns attempting to influence politics and issues of interest domestically and abroad, the researchers say. Pawn Storm, however, is expected to continue to be highly active, especially with the Olympics and several significant global elections taking place in 2018.

Four Ways to Avoid Being a Victim of Russian cyberwarfare

https://www.theguardian.com/technology/shortcuts/2018/jan/22/four-ways-avoid-being-victim-russian-cyberwarfare

Russian cyberwarfare is the new threat to the nation, according to Nick Carter, the head of the British army, **which means that the new frontline is, well, you**. So it's now more than just simple self-care to be smart about your online security – it's your patriotic duty.

(1) Update your devices – and upgrade the ones you can't

Some of the most damaging cyber-attacks in recent years haven't come through elite hackers crafting one-of-a-kind viruses to break into secure government devices, but from exploiting the old and out-of-date hardware that normal people use every day. Take the Mirai botnet: a swarm of millions of hacked devices, it was used to overload servers by bombarding them with traffic requests. But the basic elements of the botnet were simple, cheap, "internet of things" devices such as security cameras or smart lightbulbs, which had glaring security flaws that no one ever bothered to fix.

(2) Don't be a John Podesta

"Fancy Bear" is the organisation behind the hacking of Hillary Clinton's campaign chairman, John Podesta. He fell prey to a phishing campaign, well-executed but simplistic, that allowed the attackers to download – and leak – every email he had sent or received. At its heart, the hack used a fake warning from Google, asking Podesta to click a link and log in to respond to a security alert. After an aide mistakenly told him the link looked legitimate (he meant to type "illegitimate"), he did – but the link didn't go to Google, and so he ended up sharing his username and password with the attackers. The easy-to-say, hard-to-do advice is "always make sure links are from who they say they are". A more useful recommendation may be to join the 10% who have "two-factor authentication" turned on for their email.

(3) Avoid paying the ransom

The WannaCry ransomware attack has been credibly linked to North Korea, which has apparently been stepping up its use of cybercrime as a method of fundraising – a technological improvement from recent history, when the nation was one of the largest forgers of US currency. Keeping a backup of your critical data is a good idea anyway (who knows when a stray cup of coffee will fry your treasured photos?), but it is twice as useful if you can avoid paying a bitcoin ransom to a pariah state.

(4) Think twice before retweeting and sharing

According to new figures from Twitter, more than 50,000 accounts on the site were created for the express purpose of spreading Russian misinformation during the US election. Of course, the point of the misinformation accounts was to blend in with conventional US political activists, so … maybe just log off altogether?

Cybercrime: £130bn Stolen from Consumers in 2017, Report Says

https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking

UK - Hackers stole a total of £130bn from consumers in 2017, including £4.6bn from British internet users, according to a new report from cybersecurity firm Norton. More than 17 million Brits were hit by cybercrime in the past year, meaning the nation, which accounts for less than 1% of the global population, makes up almost 2% of the 978 million global victims of cybercrime and almost 4% of the global losses.

The most common crimes were generally low-tech, such as attempts to trick individuals into revealing their personal information through bogus emails with generally low costs to victims. Other forms of cybercrime were more expensive: **the typical victim found that a technical support scam cost them £44, a ransomware attack £111, and a fraudulent purchase online costing as much as £166**. But **Norton warns that cybercrime victims are not doing enough to protect themselves online.** The report found that they are more than twice as likely as those who haven't fallen prey to cybercrime to share passwords to online accounts with other people, and almost twice as likely to use the same password for all online accounts. What's more, a surprising number of cybercrime victims – more than a quarter – believe they are safe from future attacks.

"Consumers' actions revealed a dangerous disconnect: despite a steady stream of cybercrime sprees reported by media, too many people appear to feel invincible and skip taking even basic precautions to protect themselves," said Nick Shaw, Norton's general manager for EMEA. "This disconnect highlights the need for consumer digital safety and the urgency for consumers to get back to basics when it comes to doing their part to prevent cybercrime."

The head of the UK's National Cybersecurity Centre warned on Tuesday that it was a matter of "when, not if" Britain would be hit by a major cyber-attack, capable of disrupting critical infrastructure or the democratic process. "Some attacks will get through. What you need to do [at that point] is cauterise the damage," Ciaran Martin said.

Facebook Hacking Android Malware GhostTeam Found in 53 Play Store Apps

https://www.hackread.com/facebook-hacking-android-malware-ghostteam-in-play-store-apps/

Another day, another Android malware targeting those who download apps from Play Store. This time, however, malware aims at hijacking Facebook and Google Play accounts. Trend Micro researchers have identified new Android malware dubbed as GhostTeam. It is capable of stealing Facebook credentials after infecting devices. The malware tricks unsuspecting users into installing it and it is spread through malicious, infected apps. Research suggests that it is present in 53 different applications. One of these infected apps has over 100,000 downloads.

The prominent targets of GhostTeam include users in Brazil, India, and Indonesia but researchers are of the opinion that this campaign will spread to other regions most probably to the US considering that Google Play Store has been unknowingly harboring malicious apps since April 2017. Just like other Android malware, GhostTeam also is capable of performing a variety of tasks. **It basically steals Facebook credentials, which Trend Micro researchers believe could be an attempt to build what they refer to as a "zombie social media army." Their objective, speculate researchers, is to spread unauthentic news articles and cryptocurrency mining malware along with launching full-screen ads on targeted devices to generate click revenue**.

The apps in which this malware is hidden are harmless looking regular apps such as social media video downloaders, flashlights, and QR scanners, etc. It must be noted that the malware is not downloaded by the installation of these apps, just like other malware does, but instead, it involves a multi-stage attack process so as to keep its payload hidden. … To stay protected, you need to install a reliable anti-virus app and before downloading an app do check out its reviews, comments, and ratings. If you suspect anything fishy, do not download it at all. Furthermore, you need to keep Android devices updated with latest security patches.

If you somehow fall prey to GhostTeam infection, you can disable device administrator permissions from accessing Settings menu to mitigate the threat. Finally, it is really important to enable 2FA (two-factor-authentication) for Facebook and all other social media accounts wherever it is available. Trend Micro has already informed Google about the presence of infected apps and these have been removed as well. The company has updated Google Play Protect to detect GhostTeam.

500 Hacks From Beirut Show Any Government Can Spy On Google's Androids

https://www.forbes.com/sites/thomasbrewster/2018/01/18/lebanon-surveillance-hits-google-android-lookout-eff/#173ad45c7971

So much focus is placed on sexy, novel ways that government intelligence agencies break into modern-day smartphones, it's easy to forget that cheap and simple often works just as well. Research from cybersecurity firm Lookout and digital rights NGO the Electronic Frontier Foundation published Thursday proves just that, detailing a successful surveillance campaign on around 500 phones running Google's Android operating system, tracing the infections back to a Beirut building owned by a Lebanese intelligence agency.

The hackers have been dubbed Dark Caracal and, after mistakenly leaking digital clues, were traced back to a building belonging to the Lebanese General Security Directorate in Beirut, where the country's chief communications intelligence agency operates. The researchers claimed **the group had stolen hundreds of gigabytes of data across more than 20 countries in North America, Europe, the Middle East and Asia, with at least 2,000 victims in total**. Michael Flossman, security researcher at Lookout, told *Forbes* there are likely many thousands more infected with the group's various spywares for PCs and cellphones, noting he and his colleagues didn't have complete visibility of the Dark Caracal attacks.

What struck Flossman, as well as fellow researchers Mike Murray from Lookout and Cooper Quintin from the EFF, was **the lack of sophistication and the success of the smartphone attacks**. Looking through the surveillance efforts dating back to 2012, no "zero-day exploits" (hacks of previously-unknown, unpatched vulnerabilities) were used, nor did the attackers have to get their malware onto the Google Play store. **Instead, they relied on basic social engineering and the permissions granted to its malicious apps once downloaded.**

They started by phishing over WhatsApp where messages were sent encouraging users to visit a website the hackers controlled. From there, the targets were promised updates to secure messenger apps, including WhatsApp, Signal, Threema and Telegram, as well as Orbot, an app to access the dark web over the anonymizing Tor network on Androids. Those apps contained the Dark Caracal surveillance malware, dubbed Pallas, which was capable of doing what any surveillance app would want: take photos, steal data, spy on communications apps, record video and audio, and acquire location. With Google's help, the researchers also found Pallas code in several apps claiming to be Adobe Flash Player and Google Play Push. **Fake Facebook personas and groups were also set up to find targets and coerce them into downloading malicious apps, whilst news-themed lures were also deployed to draw people into the hackers' web.**

OnePlus Was Hacked and Up to 40,000 Customers Had Credit Card Info Stolen

https://www.forbes.com/sites/thomasbrewster/2018/01/19/oneplus-hacked-40000-credit-card-data-theft/#37185d0277ad

Bought a OnePlus smartphone in recent months? You might want to check your bank account. The Chinese manufacturer admitted Friday it had been breached back in November and that as many as 40,000 of its customers could've had their credit card information stolen. [the phone sells in some 42 countries outside of Mainland China]

The news came after a week in which hundreds of customers reported fraud on their accounts after paying over the OnePlus website. U.K.-based cybersecurity company Fidus Information Security then detailed some security failings on the site. After an investigation and a temporary block enforced on credit card payments, **OnePlus determined hackers had broken into its website server and installed**

malicious JavaScript code that would grab credit card data once it was entered. Customers were informed Friday morning via email, which explained credit card numbers, expiry dates and security codes were all pilfered from customers who were entering their data into the oneplus.net website from mid-November through to January 11. That's all the information anyone needs to start raiding bank accounts. **Anyone who had saved credit card information or used PayPal shouldn't have been affected, the company said**.

OnePlus is offering free credit monitoring to affected customers. It's also informing law enforcement and data protection authorities across its operating regions. It's also promised to improve its security. Fidus hacker and founder Andrew Mabbitt told *Forbes* **OnePlus were "100% at fault here."** "The only way the loss of credit cards could have occurred was through a breach of the OnePlus website and the use of malicious JavaScript. **They should have been redirecting to the payment processors own payment page as that environment will be fully PCI [Payment Card Industry] compliant**," he said. The PCI Security Standards Council sets minimum bars to reach for payment processors in protecting data.

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

****

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

****