BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

May 8th, 2018

May is Password Protection Month

Take our monthly quiz and test your knowledge

On this day in history (May 8th)

1880 – Founding of the Victoria and Esquimalt Telephone Company; the first in British Columbia.

1995 – The New York Times announced it would join eight other newspaper publishers in the New Century Network, with the goal of linking local online news services into a national network on the World Wide Web. The popularity of online news has grown along with the Web itself. Now, The New York Times and many other newspapers publish their entire content online every day.

This week's stories:

Unsolicited texts cost ticket reseller

Yahoo and parent Oath remove Canada-specific clause from terms of use

Privacy experts: EU changes will help consumers indirectly, push Canada to follow

Over 1 million U.S. kids had their identities stolen in 2017 – what parents need to know

Twitter: We Goofed; Change Your Password Now

Nigerian Email Scammers Are More Effective Than Ever

Data Breaches Decline in Q1 2018

Australia's Commonwealth Bank says records of nearly 20 mln accounts lost

More than 1 million kids had their identities stolen in 2017

Hide 'N Seek IoT Botnet Can Survive Device Reboots

4-Year-old Superhero is Caped Crusader of Kindness With the Sweetest Superpower

Unsolicited texts cost ticket reseller

http://digital.timescolonist.com/epaper/viewer.aspx

GATINEAU, Que. — Owners of Quebec-based ticket reseller 514-BILLETS have agreed to offer $10 rebate coupons to 7,500 clients in the first application of Canada's anti-spam law involving unsolicited messages sent to mobile phones. The Canadian Radio-television and Telecommunications Commission alleged that **514-BILLETS violated the law by sending text messages without the consent of recipients**. It also alleged the ticket reseller didn't identify the person who sent the messages or provide information so that recipients could contact the sender.

The 514-BILLETS service primarily resells tickets for sporting and cultural events. It is owned by two numbered companies — 9118-9076 QUEBEC INC. and 9310-6359 QUEBEC INC. — which have agreed to pay $75,000 in rebates and $25,000 to the federal government to settle the case.

The CRTC said the companies will also appoint an officer responsible for making sure the organization complies with Canada's anti-spam law, which lays out the conditions for sending electronic communications. "Today's announcement demonstrates our comprehensive approach to reduce unsolicited communications sent to Canadians, whether via email or text message," said Steven Harroun, CRTC chief compliance and enforcement officer.

Yahoo and parent Oath remove Canada-specific clause from terms of use

http://www.timescolonist.com/yahoo-and-parent-oath-remove-canada-specific-clause-from-terms-of-use-1.23286941

TORONTO — Yahoo's parent company has dropped a controversial new term of service that would have required its Canadian users to share data from their friends and contacts, including phone numbers, with the U.S.-based multinational group.

The Office of the Privacy Commissioner confirmed Tuesday that the company known as Oath, which owns Yahoo, Tumblr, AOL, Huffington Post and other businesses, had agreed to remove the clause following complaints. People who used the Yahoo email service provided with their Rogers accounts were among the first to complain about the clause, which was within Oath's recently revised terms of service. Terms of service, in general, outline the legal obligations of the provider and the user. In the case of Oath, which operates on a global scale, there were sections specific to different countries and regions.

Rogers Communications Inc. issued a statement Tuesday saying it knows some customers had concerns about Yahoo's clause related to personal contacts "so we are pleased it was removed." "We are working with our customers to address their questions and help them use Yahoo's opt-out settings to customize their email preferences," the Toronto-based cable, internet, wireless and media company said in a statement.

The privacy commissioner's office in Ottawa said Tuesday it has launched an investigation involving Rogers, Yahoo and Oath. A statement from Oath on Tuesday said that section of the terms of services "made clear to our users" that the consent was required "when they chose to have Yahoo Messenger invite their friends to the app." "Upon further review, we've removed this section of our terms of service as the functionality does not currently exist in our product offerings."

Oath's statement also said that it didn't use the contact information for advertising purposes.

Privacy experts: EU changes will help consumers indirectly, push Canada to follow

https://www.canadiansecuritymag.com/news/data-security/privacy-experts-eu-changes-will-help-consumers-indirectly-push-canada-to-follow

TORONTO — **The European Union's new privacy protection rules are being described as a game-changing new standard that's already being felt in Canada as companies with transatlantic operations get ready for the sweeping changes that come into effect later this month.** Through the General Data Protection Regulation (GDPR), the EU will attempt to impose fines of up to four per cent of a company's annual revenue — no matter where the business is based — if they violate the rights of EU citizens in any country where they operate. The pro-consumer GDPR's scope is sweeping — everything from giving people an opportunity to obtain, correct or remove personal data about themselves to outlining rules for disclosing security breaches.

Canada's federal privacy rules have yet to be updated to the higher standards set by the GDPR, but many of the services used by Canadians are already getting ready for its arrival. "The direct effects for Canadian consumers will arise predominantly in their dealings with multinational corporations, the companies that do business across borders," said University of Ottawa law professor Teresa Scassa.

Facebook and Yahoo are but two of the global services that have notified their users of changes to their terms of service and privacy policies by May 25, the day GDPR takes effect. But they've taken radically different approaches. Yahoo's parent company Oath, for example, has created separate policies for the different markets it serves — resulting in very different privacy provisions for Canada, or the United States than for Europe. Facebook, by contrast, has committed to applying the EU's General Data Protection Regulation to its operations worldwide.

Ann Cavoukian, a former Ontario privacy commissioner, now at Ryerson University in Toronto, says Facebook had also considered separate policies for EU and non-EU markets before the Cambridge Analytica "debacle." "But, come on, they had to do something. Right?" she said.

The data firm at the centre of Facebook's privacy scandal is declaring bankruptcy and shutting down after it was revealed the firm sought information on Facebook to build psychological profiles on a large portion of the U.S. electorate. The company was able to amass the database quickly with the help of an app that appeared to be a personality test. The app collected data on tens of millions of people and their Facebook friends, even those who did not download the app themselves.

Cavoukian believes Canada will have to do something to bring its privacy laws up to par with the new EU standards to avoid conflicts between the two jurisdictions. "And when they do, that's how Canadian consumers will benefit from the GDPR," Cavoukian said.

Federal privacy commissioner Daniel Therrien has already been pushing elected politicians to move closer to the European model and to give his office increased powers. But at this time, Therrien's biggest impact has been investigations of security breaches by Equifax, Uber, Facebook and others — which will soon be required by federal law to reveal serious breaches to the federal privacy commissioner.

Federal data breach regulations set to take effect Nov. 1 will require mandatory reporting of security breaches that pose a "real risk of significant harm," but stop short of the strict reporting requirements in the GDPR. The regulations require organizations to determine if a data breach poses a risk to any individual whose information was involved and then to notify the federal privacy commissioner and affected individuals "as soon as feasible" and give organizations flexibility to use any form of communication to individuals that a reasonable person would consider appropriate, such as phone, email or advertisement.

By contrast, the GDPR gives organizations in control of data no more than 72-hours to notify the supervisory authority unless the breach is unlikely to result in a risk to rights and freedoms and, if there's a delay, give reasons for it. If the data breach is likely to be a high risk to rights and freedoms, the individuals must be informed without undue delay. Therrien's office confirmed this week that it's investigating recent revision's to the Yahoo terms of service, part of a GDPR-related effort by its parent Oath, which also owns Huffington Post, TechCrunch, and AOL.

One clause of Oath's Canadian terms of service, in particular, outraged consumers when they discovered they were consenting to allow Yahoo to use the email addresses and phone numbers of friends and other contacts. The company has since removed the clause. In the version of Oath's revised terms of service that covers the European Union, the company prominently states that users can review or edit marketing preferences, advertising settings and other personal information or withdraw consent for the Oath group to process their information. "We believe that you should have control of your information," it said.

By contrast, there's no reference to withdrawing consent for using personal data in Oath's North American version terms of service. Instead, it says "by using the services you agree to our privacy policies .. We can only provide many of these services by using your personal data to provide personalized content and ads."

Scassa, who holds the Canada Research Chair in Information Law, says terms of service have historically provided consumers with little choice if they want the product or service. "Either you agree to all of this or you don't get the service," she said. "So it becomes one of those things that, I think, is largely considered to be a bit of a joke. Not a good joke, but a joke."

Cavoukian is encouraged that the GDPR requires companies to get consumers' clear and explicit consent. It also gives people the right to know what data about them is being collected, the right to get a copy of that data to take elsewhere and the right to demand that personal data is erased. "It's the exact opposite of what happens now," Cavoukian said. "This is such a game-changer."

Over 1 million U.S. kids had their identities stolen in 2017 – what parents need to know

https://globalnews.ca/news/4167442/child-identity-theft/

Upon hearing the words “identity fraud,” some may think it is a crime that only targets adults. That, in turns out, is far from the truth. **According to a new report by Javelin Strategy & Researching, a research-based advisory firm in digital and finance, over one million children were victims of**

identity theft in 2017 — crimes which resulted in US$2.6 billion in total losses, with families paying over US$540 million out of pocket. About two-thirds of victims were found to be under the age of eight, a statistic which shows that these crimes can happen even before children start using the internet, the report says.

While a child's stolen identity can be perpetrated by anyone, researchers did find that in about 33 per cent of incidents of child identity theft, the ID was stolen by a family friend. Researchers recommend that parents do a few things to prevent identity theft from happening to their child.

- Teach your children how to protect their identity online when they are young. These skills will also help them out in adulthood and reduce their risk of being a victim early on.
- Pay attention to bullied children. In many cases, researchers say fraud and bullying are not carried out by the same person, but come about from the same "underlying vulnerabilities." For example, oversharing personal information in an anonymous environment. They are also likely to come across people who target them emotionally or financially, and may be more vulnerable to fraud as they may be taken advantage of when they seek friendship.
- Keep physical documents secure.

Researchers based their report on information collected from an online survey of 5,000 people between August and September 2017 in the U.S. who either live with – or once lived with – a dependent minor in the past six years. So what should Canadian parents take away from this report? **Statistics on childhood identity theft in Canada are scarce, but according to an ETF Capital Management report, 32 per cent of Canadians have been victims of some form of financial fraud. In fact, more than seven in 10 people surveyed by the Chartered Professional Accounts (CPA) Canada said they were concerned about identity theft and about four in 10 believe their personal information has been compromised.**

Personal finance educator and consumer advocate Kelley Keehn, who wrote a fraud protection guide for the CPA in 2014, explains that while some kids won't have a credit file or social insurance number (SIN) until they're 18 in Canada (or unless a Registered Education Savings Plan, a.k.a. an RESP, has been opened in their name), children still make for perfect targets of identity fraud.

This is due to a few reasons. First, it would take a long time for a child or parents of a child to realize they have been the victims of identity fraud. Second, children don't have a credit file and their financial records are clean. Third, some parents don't think twice about giving up information on their children, whether it's when signing them up for sport teams or revealing sensitive information (like birth dates) on social media. "It's a heinous crime for an adult, but especially for a child," Keehn says. They might only come to the realization of what happened when they turn 18, apply for their first cellphone or credit card, and get declined, she says. "You have to clear your own name when it comes to an identity theft. A lot of people do not have the confidence and the understanding on where and how to do that. … It can be incredibly emotional devastating."

While identity theft can impact children financially in the future, not many think about other ways this can affect their child — for example, instances in which a crime is committed. A stranger may use a child's identity to commit a crime, thus creating a criminal record in that child's name, Keehn warns. Other ways a child's stolen identity can be used can be to obtain passports, receive government benefits and open new bank accounts, among other things, the RCMP details.

Should parents want to avoid this happening to their children, or need help in cleaning their child's name, Keehn suggests parents be vigilant. "Make sure you can sit down with someone like a certified financial planner who's going to help walk you through this — like help you set reminders," she says. "Who should you check with to see if your child has a credit report? That would be Equifax and TransUnion." Also, make sure all your important documents are locked away somewhere safe, she adds. "Your SIN is such a key component to your identity that Service Canada does not even issue SIN cards anymore," Keehn says. "But if you have a teenager and if they have a SIN card, do you know where that is? If you don't know where that is, then that's a red flag."

Next, don't share any of your child's personal information online, and be aware of the information some places are asking you to provide about your child. For example, your child's sport team should not be asking for their SIN. It's also not a bad idea to think about identity theft insurance, Keehn says, especially if you feel like you or your child's information might have been compromised. Should you suspect yours or your child's identity has been stolen, the RCMP advises you contact your local police office and file a

report, followed by contacting your bank and credit card companies. Next, contact both Equifax and TransUnion, then inform the Canadian Anti-Fraud Centre.

For more tips on preventing identity fraud and theft, or for fighting it, visit the RCMP website.

Twitter: We Goofed; Change Your Password Now

https://www.databreachtoday.com/twitter-we-goofed-change-your-password-now-a-10972

Just in time for World Password Day – (May 3) - **Twitter has apologized after it discovered a bug in its systems that inadvertently caused passwords to be stored in plaintext in an internal log**. **Users would be at risk if a hacker penetrated Twitter's internal systems and obtained the log.** But Twitter doesn't believe that the data has been misused or has left its systems, says Parag Agrawal, the company's CTO, in a Thursday blog post detailing the password flub. **Nonetheless, the company is recommending a password reset for its more than 300 million users.**

"We have fixed the bug, and our investigation shows no indication of breach or misuse by anyone," Agrawal writes. "We found this error ourselves, removed the passwords and are implementing plans to prevent this bug from happening again." Troy Hunt, an Australian security expert, says Twitter's disclosure is significant because of the number of accounts affected and because the passwords were stored as plaintext. But at the same time, the risk appears to be low, particularly for Twitter users that have two-factor authentication enabled, Hunt says. Even with a username and password, an attacker would need a one-time passcode sent either by SMS or generated by an authentication app to log into an account. "It's not something I'd lose any sleep over," Hunt says.

Still, the lapse brings into question Twitter's overall operational security, says Chris Pierson, CEO of Binary Sun Cyber Risk Advisors. "The engineering teams should have caught this glaring mistake, red teams and penetration testers should have taken a closer look, and it really calls into question the control environment," Pierson says. **The safest way for service providers to store passwords is to hash them, meaning to take a plaintext password and process it through a one-way hash function. In theory, it should be difficult or impossible to take a hash and discover the plaintext password**. Hashing using bcrypt (Source: Bcrypt-Generator.com).

Twitter uses the bcrypt algorithm to hash passwords. **Many services have moved to using bcrypt and away from algorithms such as MD5 and SHA1, which are widely considered to be too weak to protect plaintext passwords.**

Both MD5 and SHA1 are overly susceptible to brute-force cracking. Advances in computer hardware have made it easier to rapidly generate long lists of hashes using dictionaries of words and symbols that could potentially be someone's password. If one of the generated hashes matches a stored hash - obtained by a hacker during a data breach, for example - then the hacker can reverse-engineer the hash and obtain the original password, meaning it's been "cracked."

Bcrypt is considered to be a more secure approach because password-cracking hardware rigs can't generate bcrypt hashes nearly as quickly as they can MD5 and SHA1 hashes. So if attackers obtained a large set of bcrypt hashes from Twitter, in theory, it would take quite a bit of time for them to crack passwords, and particularly for any that might be long or complicated. Twitter's Agrawal, however, warns that the bug caused users' plaintext passwords to be written to a log before bcrypt completed the hashing process.

[Read the rest of the article online to learn more]

Nigerian Email Scammers Are More Effective Than Ever

https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/

You would think that after decades of analyzing and fighting email spam, there'd be a fix by now for the internet's oldest hustle—the Nigerian Prince scam. There's generally more awareness that a West African noble demanding $1,000 in order to send you millions is a scam, but the underlying logic of these “pay a little, get a lot” schemes, also known as 419 fraud, still ensnares a ton of people. In fact, groups of **fraudsters in Nigeria continue to make millions off of these classic cons**. And they haven't just refined the techniques and expanded their targets—they've gained minor celebrity status for doing it.

On Thursday, the security firm Crowdstrike published detailed findings on Nigerian confraternities, cultish gangs that engage in various criminal activities and have steadily evolved email fraud into a reliable cash cow. **The groups, like the notorious Black Axe syndicate, have mastered the creation of compelling and credible-looking fraud emails**. Crowdstrike notes that the groups aren't very regimented or technically sophisticated, but flexibility and camaraderie still allow them to develop powerful scams. "These guys are more like a crew from the mafia back in the day," says Adam Meyers, Crowdstrike's vice president of intelligence. "Once you're in an organization and are initiated, then you have a new name that's assigned to you. They've got their own music, their own language even. And there are pictures on social media where they're flaunting what they're doing. **The whole idea is why invest hundreds of thousands of dollars to build your own malware when you can just convince someone to do something stupid?"**

Young Nigerian scammers have often been called "Yahoo Boys," because many of their hustles used to target users on Yahoo services. And they've embraced this identity. In the rap song "Yahooze"—which has more than 3 million views on YouTube—Nigerian singer Olu Maintain glamorizes the lifestyle of email scammers. **Advanced Nigerian groups have lately increased the amounts they make off with in each attack by targeting not just individuals but small businesses. The FBI estimates that between October 2013 and December 2016 more than 40,000 "business email compromise" incidents worldwide resulted in $5.3 billion in losses.** With so many third parties, clients, languages, time zones, and web domains involved in daily business, it can be difficult for a company with limited resources to separate out suspicious activity from the expected chaos. **Nigerian scammers will send tailored phishing emails to a company to get someone to click a link and infect their computer with malware. From there, the attackers are in no hurry. They do reconnaissance for days or weeks, using key loggers and other surveillance tools to steal credentials to all sorts of accounts, figure out how a company works, and understand who handles purchasing and other transactions.**

Eventually the scammers will settle on a tactic; they may impersonate someone within the company and attempt to initiate a payment, or they might pretend to be a company the victim contracts with and send the target an innocuous-looking invoice to pay. If they've gained enough control of a system, attackers will even set up email redirects, receive a legitimate invoice, doctor it to change the banking information to their own, and then allow the email to reach its intended recipient. And the scammers rely on this sort of man-in-the-middle email attack for all sorts of manipulations.

[Read the rest of the article online to learn more]

Data Breaches Decline in Q1 2018

https://www.infosecurity-magazine.com/news/data-breaches-decline-in-q1-2018/

The Q1 2018 numbers are in, and while it might be an overly optimistic conclusion, the breach landscape could be changing. Risk Based Security recently released its *Q1 2018 Data Breach QuickView Report.* The report compares the numbers from Q1 2017 and Q1 2018, which doesn't take into account the massive Equifax breach from September 2017.

According to the report, 686 breaches were reported between 1 January and 31 March. Approximately 1.4 billion records were exposed, indicating a shifting breach landscape with the number of reported breaches down from 1,442 incidents in Q1 2017. The approximate number of total exposed records is down from 3.4 billion.

Additionally, the number of disclosed instances of phishing for employee W-2 data dropped from 214 in Q1 2017 to 31 in Q1 2018. "Over the past two years it's been very popular to target data for filing fraudulent tax returns. In 2017, we tracked over 200 such incidents. This year, the number is down significantly – to around 35 such breaches at the time the numbers were put together," said Inga Goddijn, executive vice president Risk Based Security.

Of the reported total breaches, 50.4% were in the business sector with government at a distant second, accounting for only 14.4%. Medical (10.2%) and education (7%) trailed far behind. Fraud topped the list for type of breach to compromise the most records. Accounting for 1.3 billion exposed records during the quarter, fraud was only the seventh most common breach type, representing 4.8% of reported breaches.

The leading cause of breaches for the quarter was unauthorized intrusion, accounting for 38.9% of incidents, which exposed 10.9% of the total breached records, or 159 million records. "Right now the biggest difference is the drop in the number of publicly disclosed breaches. We haven't seen a Q1 this quiet since 2012," said Goddijn. "We also think the shift toward cryptomining is possibly easing some of the attention on data theft. It's still too early to say for sure, but it does go to show [that] malicious activity will follow the best opportunities for making a profit."

Who is being impacted by the breaches has changed very little. Goddijn noted there have been no sizable changes in the type of organizations being breached, the type of data that is being exposed, the number of large events, insider vs outsider activity, breach severity scores or where breaches are taking place. "We would have expected other sizable shifts to be evident along with the drop in the number of breaches but that is not the case," Goddijn said.

Australia's Commonwealth Bank says records of nearly 20 mln accounts lost

https://www.reuters.com/article/us-australia-cba-moneylaundering/australias-commonwealth-bank-says-records-of-nearly-20-mln-accounts-lost-idUSKBN1I40II

SYDNEY (Reuters) - **Commonwealth Bank of Australia (CBA), the country's top lender, confirmed on Thursday it lost records of almost 20 million accounts and decided to not inform its clients, a breach the nation's prime minister called "an extraordinary blunder".** CBA's announcement, which was made in a YouTube video by a senior bank executive a day after BuzzFeed Australia reported the data breach, puts further pressure on Australian banks already reeling from revelations of widespread misconduct in a judicial inquiry.

It is also the latest blow to CBA, which has been accused in a federal lawsuit of breaching anti-money laundering protocols more than 50,000 times and has admitted to using outdated medical definitions to refuse sick customers health insurance payouts. Earlier this week, a regulator ordered CBA to keep an extra A$1 billion ($750 million) in cash reserves as punishment for the alleged money laundering breaches, which it is contesting.

In a YouTube video, CBA's acting head of retail banking services, Angus Sullivan, said the bank found in May 2016 it had lost two magnetic tapes containing 15 years of data on customer names, addresses and account numbers for 19.8 million accounts. The tapes were due to be disposed of, but CBA could not confirm they were securely destroyed, Sullivan said. **The tapes did not contain PINs, passwords or other data that could enable account fraud**, he said. The bank informed its regulators and launched an internal investigation which found the tapes had "most likely been disposed of", Sullivan said. It did not tell customers because "we balanced the need to alert customers without unnecessarily alarming them", he said. "This is an extraordinary blunder," Prime Minister Malcolm Turnbull told reporters. "It's hard to imagine how so much data could be lost in this way. If that had happened today, the bank would have to advise each of their customers," Turnbull added.

CBA is seen as a stable part of life in the country of 24 million where most people have had a mortgage, insurance policy or regular savings account with CBA at some point - often starting with its famed "Dollarmites" deposit account for school children. But the crises have started affecting its financial performance because of concerns it will result in heightened regulations, and CBA shares are down about 7 percent so far this year while the broader market is up. CBA shares ended up 0.6 percent on Thursday, roughly in line with the broader market.

Reputation management experts, however, said CBA's move to use YouTube to take responsibility for the incident and reassure customers no personal data was stolen was a smart one. "They've so overdrawn their goodwill cheque account that there's not much they can do to push back on this," said Steve Harris, CEO of The Brand Agency, a communications and image consultant. "They need to bypass the media and communicate directly to get their message through, because whatever they (say) via media it will be put into a whirlpool of Royal Commission, money laundering and other filters," added Harris, referring to the powerful independent inquiry into the broader finance sector.

Consumer psychologist Adam Ferrier said posting a YouTube video and "trying to put a face to the banks and admitting to errors is always a good strategy". By mid-afternoon, the video had been viewed 3,798 times, according to data published on YouTube.

More than 1 million kids had their identities stolen in 2017

https://nypost.com/2018/04/24/more-than-1-million-kids-had-their-identities-stolen-in-2017/

Your children may be less safe online than you think — even before they ever use a computer. **More than 1 million children were victims of identity fraud in 2017**, a new study from Javelin Strategy & Research found, costing a total of $2.6 billion. With limited financial history or existing account activity, children are the most likely to become victims of new-account fraud, the research showed.

These attacks can occur before children even become active internet users, with some two-thirds of victims being under the age of 8. The overall numbers are likely even higher, said Al Pascual, research director at Javelin, since the study relied on parents and guardians reporting cases of identity theft. In many cases**, the parent or another relative may be the one using a child's identity to start a new account.**

Perhaps the most unnerving detail in the report: **The most common perpetrator of childhood identity theft is a family friend, accounting for 33 percent of the incidents.** "If I am a parent and the lights have gone out, and I'm having a hard time making ends meet, using my child's identity to start a new account with the utility company may seem worth it," Pascual said. "I am doing right by them and not hurting them."

Other times, identities are compromised before they are even issued to children. **Michelle Dennedy, chief privacy officer of Cisco, became an advocate for child identity-theft prevention after her daughter was a victim of identity theft at the age of 8.** Sometimes people do not know their identity has been compromised until they enter adulthood and apply for college, a car or a home, only to realize their credit has already been wrecked. "Absolutely be as vigilant about your child's online reputation before they touch a device as you would about any other financial vehicle in your family because it can destroy families," she said. It can impact a child's ability to get a college scholarship and could lead to a long line of debt collectors, she added.

Hide 'N Seek IoT Botnet Can Survive Device Reboots

https://www.securityweek.com/hide-n-seek-iot-botnet-can-survive-device-reboots

The Internet of Things (IoT) botnet known as Hide 'N Seek that first emerged in January can now achieve persistence on infected devices, Bitdefender reports. Discovered toward the end of April, the latest version of the malware also includes code that allows it to target more vulnerabilities and new types of devices, the security firm discovered, adding that it targets 10 different architectures and a broad range of models. **The botnet has so far infected 90,000 unique devices starting in January, and could become a major threat if weaponized.**

When first observed in January, the botnet didn't have a persistence module, meaning it was not able to survive a device reboot. This, however, changed in the last version: if it manages to successfully compromise a device via Telnet, the malware copies itself to */etc/init.d/* and adds itself to startup, so it is executed when the operating system launches. The malware also abuses web based vulnerabilities to target specific devices like IPTV cameras, but persistence is only achieved if the infection took place via Telnet, because root privileges are required to copy the binary to the *init.d* directory, Bitdefender Senior E-Threat Analyst Bogdan Botezatu explains.

The malware targets a broad range of devices via the Telnet service. According to Bitdefender, the bot has 10 different binaries compiled for x86, x64, ARM (Little Endian and Big Endian), SuperH, PPC and other platforms. The latest Hide 'N Seek version can compromise more IPTV camera models by targeting vulnerabilities in Wansview NCS601W IP camera (a cloud-only device) and AVTECH IP Camera, NVR and DVR (the maker's products have been targeted by other IoT malware as well).

Responding to a *SecurityWeek* inquiry, Botezatu revealed that the Hide 'N Seek malware targets a long list of weak or default credentials frequently found in IoT devices. "The list is extremely long and features several camera models, but the hardcoded credentials also target several router models. In addition to specific models, the bot also attempts these credentials against Telnet for all sorts of devices. The fact that it has binaries compiled for 10 platforms and architectures shows that the attacker is aiming at enrolling as many devices, regardless of type, maker, and model," Botezatu said. "We've notified vendors about this," he added.

Over the past three months, Hide 'N Seek has been growing steadily although some devices left the botnet, while others joined it. Most likely, the botnet lost those devices "that could not be exploited in a way to offer persistence," Botezatu said. From February to May, however, Bitdefender's security researchers identified almost 65,000 infected devices.

Botezatu told *SecurityWeek* that five versions of the botnet have been observed thus far. However, there haven't been major changes in the list of supported commands compared to the earlier versions, and no support for distributed denial of service (DDoS), the most commonly encountered purpose of IoT botnets, has been added to Hide 'N Seek either. "Based on the evidence at hand, we presume that this botnet is in the growth phase, as operators are trying to seize as many devices as possible before adding weaponized features to the binary," Botezatu revealed.

As for the current geographic distribution of the bots, most of them are located in China, with Russia, Brazil, the United States, and Italy rounding up top five, followed by India, Poland, Bulgaria, France, and Republic of Korea.

And Now this:

4-Year-old Superhero is Caped Crusader of Kindness With the Sweetest Superpower

https://www.goodnewsnetwork.org/4-year-old-superhero-is-caped-crusader-of-kindness-with-the-sweetest-superpower/

While Austin Perine may not have the power to fly or shoot spider webs out of his hands, he does have a pretty incredible superhero identity. Austin has created an entire superhero identity out of feeding the homeless.

Every week, the 4-year-old from Birmingham, Alabama uses his allowance money to buy a bag full of sandwiches and sodas so he can hand them out to the homeless – and he does it all while wearing a little caped uniform. When asked what his superhero name is, he simply says: "President Austin". "That's his idea of what the president is supposed to do," TJ Perine, Austin's father, told CBS News. "I was like, buddy, you have no idea, but hey, I'm going along with it."

Only time will tell whether Austin actually ends up on the ballot in the future, but in the meantime, he already has a motto – and he says it to every single one of his sandwich recipients. His motto is: "Don't forget to share love".

[Watch the related CBC News video to find out more]

Click Unsubscribe to stop receiving the Digest.

****

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

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

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

****