BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

Security News Digest
February 06, 2018

New for you: 'Love Your Online Life' Security Quiz

Canadians at Higher Risk of Hacks, Thanks to Their Smart Devices: Report 🇨🇦

https://globalnews.ca/news/4000010/how-smart-home-devices-put-canadians-at-risk/

Multiple "smart" devices launched in Canada in 2017, but a new report by Norton states that **consumers affected by cyber-crime last year were largely adopters of smart home interfaces** and emerging security features. **The report revealed that 10 million Canadians spent $1.8 billion dealing with the aftermath of being hacked in 2017, and the average cost per consumer totaled $69.** Kevin Haley, the director of product management and security response at Symantec, told Global News that while consumers are tech-savvier than ever before, **having more devices - and sharing information across those several devices - inevitably means there will be more hacks**. "That attack space is larger," he said. "The more time you spend online and the more devices you have, the more likely you are to be a victim."

Smart home devices are built for usability, not for security. Both the Google Home and Amazon Echo home automation speakers made their long-awaited debuts in Canada in 2017. **Of the 10 million Canadians impacted by cyber-crime last year, over a third owned some kind of smart device they used for streaming content.** Smart speakers, including the Amazon Echo and the Google Home, offer consumers several options for streaming content through the devices. In addition, American victims of cybercrime were almost three times as likely to own a connected home device than those who didn't. Haley said that while smart devices prove incredibly convenient, "they're built to be simple to use, not to be secure." **He said consumers will often forget about simple safety practices when using connected devices because they don't think of a smart speaker as a computer."**

"We find people are doing things with these devices that they wouldn't do with a PC. They don't really think about them as computers. For example, they don't necessarily change the default password." Frank Breitinger, from the department of computer science at the University of New Haven, added that in addition to forgetting to secure our connected devices the same way we've grown accustomed to securing computers, **the way we connect with smart devices over Wi-Fi represents an additional risk**. Breitinger also attributes this trend to the public's growing trust of technology, even if people don't completely understand it. "Technology nowadays gets so complicated that the average user loses track of it. For example, why does my calendar sync with my phone as well as my laptop? How does all this technology work? We simply just use it." **According to figures from Statista, the total number of "smart" or "Internet of Things" devices in use will reach 20.4 billion in 2020, up from 8.4 billion in 2017.** "If we have billions of insecure devices online, we're going to be in a lot of trouble," Haley said. He advised consumers hoping to detect future hacks to look for unusual network activity - or to pay attention to whether the device is active when you haven't initiated it. **If it always looks like it's working when it should be idle, or if there's a significant amount of network activity when there shouldn't be, this should set off alarms.**

Don't dump good privacy habits when new features come along. In addition, the Norton report revealed that a typical Canadian impacted by cybercrime in 2017 was an early adopter of advanced security technologies, like fingerprint scanners, facial recognition technology, personal VPNs, or two-factor authentication. **The highest percentage of early adopters who said they experienced a hack in 2017 was users of fingerprint scanners at 33 per cent.** "I think that's generally people that are technically savvy, probably a large portion of millennials, and they're really willing to try the new stuff. But by the same token, they're not doing the old stuff," Haley said. He said that early adopters who fall victim to hacks do so or for similar reasons to Canadians with numerous connected devices. Even if you're using facial recognition and a thumbprint, he said, you still need to use a password.

Vancouver Woman Angry She Became Face of Russian Twitter Bot Fraud

https://globalnews.ca/news/4010584/vancouver-woman-angry-she-became-face-of-russian-twitter-bot-fraud/

Meet Cheryl Montgomery. Her Twitter profile shows her as hailing from Marlton, N.J., and she tweets a great deal about U.S. politics. Her profile picture looks a lot like Catherine Simpson, a Vancouver-based public relations professional. That's because **Cheryl Montgomery is a Twitter bot created by someone who stole Simpson's photo from an online news article and used it as a profile photo**. Simpson discovered the bot after she was contacted by Francis Carr, an investigative journalist with Columbia University, who is looking into the Twitter bot trend. "I said, 'No way,'" Simpson said. "I'm typing it in and there's my picture."

Carr told Global News he is investigating "the use of automated social media accounts in spreading political messages in the U.S." He said it's remarkably easy to create a Twitter bot. "You can go online and Google how to make a bot and have one online in two hours," Carr said. This particular bot seems to be in favour of former U.S. secretary of state Hillary Clinton and opposed to U.S. President Donald Trump.

The tweets from Cheryl Montgomery were relatively tame, but social media expert Jesse Miller said bots with more radical messaging can cause problems for the real people used in Twitter profile photos. "People have believed the individual was the one behind the keyboard and they've actively looked to find the person and unfortunately that internet vigilante justice piece kind of rears its ugly head," he said. Simpson noted that if the bot "was retweeting on Canadian politics or local politics I would've been much more concerned." She said she has contacted Twitter in the hopes of having the account suspended. **Twitter said it recently suspended 1,062 automated accounts linked to the Internet Research Agency (IRA), a Russian "troll farm" that systematically disseminated content designed to influence public opinion during the U.S. presidential election.**

A recent *New York Times* report exposed how some public figures have paid for bots to follow them on social media. But it seems that shutting down a Twitter bot is considerably more difficult than creating one. "I sent them my driver's licence," Simpson said. "I've sent them all sorts of information but I'm not really having any luck with them." Experts say it's important to flag such bots to Twitter, even if the process is frustrating. It's also important to be selective about who can see your pictures online. If not, your favourite shot might be the new face for a Twitter bot.

Uber Says Hackers Behind Data Breach were in Canada, Florida

http://www.cbc.ca/news/technology/uber-hackers-canada-florida-data-breach-1.4523466

The two people behind a 2016 data breach at Uber Technologies Inc. were found to be in Canada and Florida, an Uber cyber security executive told the U.S. Congress on Tuesday. About 25 million users affected by the breach are users located in the United States, John Flynn, chief information security officer at Uber, said in written testimony to a Senate Commerce Committee panel. **Uber announced the breach of 57 million worldwide users last November. Of those impacted in the United States, 4.1 million were drivers, according to the testimony. Uber Canada announced late last year that 815,000 Canadian riders and drivers may have been affected.**

The testimony from Flynn is the most comprehensive public account to date of the Uber hack, the handling of which prompted newly appointed Uber chief executive Dara Khosrowshahi to fire two of the company's top security officials. Reuters reported in December that a 20-year-old man was primarily behind the massive data breach, and that he was paid by Uber to destroy the data through a so-called "bug bounty" program normally used to identify small code vulnerabilities. **Flynn confirmed the man who obtained data from Uber was in Florida and that his partner, who first contacted the company on Nov. 14, 2016, to demand a six-figure payment, was located in Canada. The company's security team made contact with both people and received assurances the pilfered data had been destroyed before paying the intruders $100,000, Flynn said.**

Uber has received criticism for its handling of the breach, and lawmakers in both parties on Tuesday piled on with several admonishments. "The fact that the company took approximately a year to notify impacted users raises red flags within this committee as to what systemic issues prevented such time-sensitive information from being made available to those left vulnerable," Republican Sen. Jerry Moran said. Flynn repeatedly acknowledged Uber had made mistakes and that it should not have not used the company's bug bounty service - designed to reward security researchers who report flaws found in a company's software - to negotiate with a hacker seeking to extort money. "We made a misstep in not reporting to consumers, and we made a misstep in not reporting to law enforcement," he said. The compromised data included names, phone numbers and email addresses but not Social Security numbers or credit card information. The driver's license numbers of 600,000 drivers were also compromised.

Data Deletion Policy Key to Reducing Breach Risks, Canadian Privacy Pros Told 🇨🇦

https://www.itworldcanada.com/article/data-deletion-policy-key-to-reducing-breach-risks-canadian-privacy-pros-told/401280

[Jan31] There is a lot of technology for sale to help CISOs and privacy officers mitigate the risk of data breach. But one of the easiest and cheapest is the Delete key. In other words, **keep only the data the organization needs**. “The biggest risk for keeping information too long is simply a [data] breach,” Cameron Fraser, access to information and privacy coordinator at the office of the Auditor General of Canada, told a privacy conference Wednesday in Toronto.

“You don’t want to be in the position where four years down the road [from the creation of an email or document] where for whatever reason you’re breached - someone has their briefcase stolen or loses a USB that isn’t encrypted or you’re hacked - and you’re asked, ‘Why did you have this information? It’s useless.’ And the head of the organization says ‘Well, uh, I don’t know’ …The answer, he said is to **create a data retention and destruction policy, with a data retention officer to monitor compliance**. “Someone has to do this. Not only is it responsible but it can significantly decrease the institutional risk.” Fraser was speaking at the *Canadian Institute’s annual Privacy and Data Security Compliance Forum.*

An ideal repository for documents and email is a central database where everyone in the organization can send their data, he said – and can access everything if a person is out of town. The database could be partitioned if groups don’t want their data shared. The solution doesn’t have to be fancy, he added, although there should be a management front end with the capability to record when data was put in and signal when, according to agreed-upon corporate policy, it should be archived or deleted. There’s no rule on how the database should be organized, but it should be approved by a data retention committee.

Data has to have a lifecycle, Fraser argued: It is created /obtained, kept because it has business value for a defined period, and then destroyed.

Generally, Fraser said, **it’s accepted that most information can be destroyed after two years unless the organization has to keep it longer for legal or regulatory reasons**. If the organization doesn’t have a data retention team for creating a policy already, it needs to create one. The team should have representation from all business units because they have the expertise on what’s important. The organization should also appoint a data retention officer, which may or may not be a full-time job, who has the responsibility of ensuring the policy is carried out. …He emphasized that monitoring staff for compliance is vital. “If you leave it to individuals it will never be done.” Have regular reminders sent to staff about cleaning their email inboxes. “There’s no perfect solution,” he stressed. “It still boils down to one major factor: Each individual still has to do it. No one’s going to do it for you … It’s work, its responsible…but if this happens I guarantee it will make your job easier because finding information becomes so easy because it’s all in one spot.” However, in an interview Fraser cautioned against staff getting too enthusiastic about reducing data. “Going too far and destroying things that may have business value,” is the biggest mistake organizations make, he said.

Incident Response Plans Must Be Tested, Privacy Conference Warned 🇨🇦

https://www.itworldcanada.com/article/incident-response-plans-must-be-tested-privacy-conference-warned/401245

[Jan31] A cyber incident response plan isn’t worth the paper it’s written on if it hasn’t been tested, a Canadian lawyer has told a privacy conference. “The significance of [having] a response plan clearly can’t be overstated,” Adam Kardash, chair of the privacy and data management practice at Toronto law firm of Osler, Hoskin & Harcourt, told the *Canadian Institute’s annual Privacy and Data Security Compliance Forum* in Toronto on Tuesday. But, he warned, if the response team hasn’t practiced what it will do – either through a tabletop exercise or a real test – it isn’t worth much. Many security and privacy pros know it, he suggested.

His firm has held incident response seminars with chief privacy officers and regulators in the same room as a resource, working through potential cases. Today over 90 per cent of privacy officers say they have a plan. But when asked if they are confident the plan will work if there was a catastrophic attack, “about half say they’d be confident - but we know they’re lying because regulatory authorities are in the room, or it’s only a discussion, or they’re rationalizing to themselves,” said Kardash. “But if you talk to the top CEOs, CISOs they’re seriously going to question if it’s going to work” unless the plan has been tested.

An exercise will help the IR team find out “tiny little things,” such as managers who aren’t designated to be at the table but who should be. It will also find major things: One test with a multinational company Kardash’s law firm sat in for saw that for the first hour it couldn’t get the conference phone running – and once it was, people discovered it wasn’t a secure line.
…. **During his presentation he also talked at length about the coming final version of the federal government mandatory data breach notification regulations.** A draft version was released last September. Ottawa hasn’t set a date but Karadash is betting later this year. “We’re expecting it to have a pretty massive impact on the Canadian privacy arena,” he said. Organizations covered by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) will have to report all breaches of security safeguards to the federal privacy commissioner, and, if they involve the leak of personal information that could cause real risk of significant harm also notify persons directly affected as well as possibly third parties. Karadash noted that the definition of “significant harm” is open to interpretation. The Office of the Privacy Commissioner has promised to issue guidance. Regardless, Karadash predicted regulators will have a low threshold. “Sooner is better,” he advised.

Human Rights are at Stake in Debate around Private Security Cameras, Expert Says 🇨🇦

http://www.cbc.ca/news/canada/hamilton/cavoukian-cctv-cameras-1.4516987

Ontario's former privacy commissioner says human rights are at stake if Hamilton city council debates letting residents and businesses point their security cameras at the street. Privacy expert Ann Cavoukian says the city's current bylaw, which only lets people point cameras at their own property, is a good one. "Privacy is not just a fundamental human right," she said. "It has enormous societal value. **You cannot have fundamental liberty without privacy**."
Next week, Coun. Sam Merulla of Ward 4 will ask city council's general issues committee to consider reversing the bylaw. Letting people get security footage of public property will help police investigations, Merulla said. And people can already film on the street anyway. But the current bylaw "is such a progressive decision," said *Cavoukian, who spent three terms as Ontario's Information and Privacy Commissioner. She leads Ryerson University's Privacy by Design Centre of Excellence*. "There are creative ways of doing it where you can protect privacy and advance the needs of law enforcement." This includes encrypting camera footage, and only unencrypting it for police by court order.
Changing the so-called *fortification bylaw*, last revised in 2010, would add to an increasing trend of video surveillance in Hamilton. In November, council voted to look at expanding video surveillance in parks to combat graffiti. This came after a test at two Mountain parks, Fay and Lisgar. The city is adding cameras to HSR buses that face inward and outward with a goal of protecting drivers and passengers. It's also adding 1,100 cameras to 550 intersections to monitor traffic flow. The city also has 24 red light cameras, and will double that number by 2022. In 2016, it laid 14,167 red light charges.
The fortification bylaw can lead to charges too. Last year, Joe Moniz's home security cameras captured a city waste contractor throwing his bins in the truck along with his recycling. By-law enforcement sent Moniz a notice that his cameras were pointed the wrong way. Under the bylaw, any cameras, "night vision" systems or electronic listening devices can only go as far as the perimeter of the user's property.
Last week, Chief Eric Girt of Hamilton Police Service said Merulla's motion was "a good idea" for solving crime. "When you see (footage) from a street position and it's largely widespread, you get a much broader scope," Girt said during a budget meeting. Merulla said he was impressed by how police used surveillance cameras to catch the people who killed Ancaster resident Tim Bosma. And people can already be photographed and filmed in public places. "Privacy, to me, is someone's backyard," Merulla said. "That's off limits." Otherwise, "you're allowed to walk down the street with a video camera, but you're not allowed to have your camera facing the road."
Cavoukian said it doesn't really compare. People don't typically sit in one spot and film everyone who walks down the road. Choosing privacy or solving crime, she said, is a common false dilemma in discussions about privacy. "There's a way you can do both."

4 in 10 Young Canadians have Sent a Sext, 6 in 10 have Received One: Report 🇨🇦

https://www.ctvnews.ca/lifestyle/4-in-10-young-canadians-have-sent-a-sext-6-in-10-have-received-one-report-1.3791152

About four in 10 young Canadians have sent a sext and more than six in 10 have received one, suggests a new report, which also puts a spotlight on the unauthorized sharing of sexual photographs among teens. Still, sexting happens less commonly among youth than many people believe - including nearly all of the survey's 800 16- to 20-year-old participants, said Matthew Johnson, director of education for the non-profit organization MediaSmarts. It's also not an "intrinsically harmful" behaviour, he said, with the majority of sexts remaining private between the sender and intended recipient.

"We need to move from fear-mongering to talking about things from an ethical and moral point of view," said Johnson, **who called the report one of the first in the world to focus on the non-consensual sharing of intimate images. "We need to be talking about consent in all contexts, including digital contexts ... and to really send a loud and clear message that this is not normal, and this is not OK, and nothing gives you the right to share someone's sext except them actually telling you that you can."**

Of the survey respondents who said they had sent a sext in the past, about 40 per cent said at least one of their intimate photos had been shared without their consent. "Even though boys and girls send and receive sexts at similar rates, and even though they have their sexts shared at similar rates, the harm is very much unequal, and it falls much more heavily on girls," Johnson said. "There can be harm done to people's reputation. Obviously, there's an inherent harm just in the loss of privacy and violation of consent ... (senders) have been blackmailed, in some cases."

Researchers also found there was a significant relationship between sharing sexts and subscribing to traditional gender stereotypes that cast men as sexual aggressors and women as "gatekeepers."

According to the study, roughly one-third of participants either said they believed that a girl who sexts outside of a relationship "shouldn't be surprised if it gets around," or felt "nobody should be surprised if boys share sexts with each other." Young people's attitudes about sexting were highly influenced by those of their peers, Johnson added, and if their friends engaged in sharing sexts, many participants said there was an expectation that they would reciprocate. "The sharing behaviours are being done by almost exclusively the same people," he said. "All of these things point to essentially a subculture among youth that normalizes sharing, and even to a certain extent valorizes it." **While nearly two-thirds of participants said they were aware of a relatively recent law against the non-consensual sharing of intimate images, Johnson said the threat of criminal consequences does not appear to be much of a deterrent among teens.**

The MediaSmarts study was based on an anonymous, internet-based survey of young people around the country that was conducted in August and September 2017. The polling industry's professional body, the Marketing Research and Intelligence Association, says online surveys cannot be assigned a margin of error because they do not randomly sample the population.

Russian Hackers Came Close to Stealing Secret U.S. Defence Technology

http://www.cbc.ca/news/technology/russian-hackers-defence-tech-1.4524179

Russian hackers exploited a key vulnerability in U.S. cyber defences to come within reach of stealing some of the nation's most secret and advanced defence technology, an Associated Press investigation has found. **What may have been stolen is uncertain, but the cyberspies clearly took advantage of poorly protected email and scant direct notification of victims.**

The hackers known as Fancy Bear, who also intruded in the U.S. election, went after at least 87 people working on military drones, missiles, rockets, stealth fighter jets, cloud-computing platforms, or other sensitive activities, the AP found. Thirty-one agreed to interviews.

Employees at both small companies and defence giants like Lockheed Martin Corp., Raytheon Co., Boeing Co., Airbus Group and General Atomics were targeted. Contacted by the AP, those companies offered no comment. "The programs that they appear to target and the people who work on those programs are some of the most forward-leaning, advanced technologies," said Charles Sowell, a former senior adviser in the Office of the U.S. Director of National Intelligence, who reviewed the list of names for the AP. **"And if those programs are compromised in any way, then our competitive advantage and our defence is compromised." "That's what's really scary,"** added Sowell, who was himself one of the hacking targets.

The AP identified Fancy Bear's prey from about 19,000 lines of the hackers' email phishing data collected by the U.S.-based cybersecurity company Secureworks, which calls the hackers Iron Twilight. The data is partial and extends from March 2015 to May 2016. **Most of the people on the target list worked on classified projects. Yet as many as 40 per cent clicked on the hackers' phishing links**, the AP analysis indicates. That's the first step in potentially opening their accounts or computer files to digital theft. **Hackers predominantly targeted personal Gmail, with a few corporate accounts mixed in**. Personal accounts can convey classified information - whether through carelessness or expediency -

and lead to more valuable targets or carry embarrassing personal details that can be used for blackmail or to recruit spies.

Among their interests, the Russians seemed to be eyeing the X-37B, an American unmanned space plane that looks like a miniature shuttle. Referring to an X-37B flight in May 2015, Russian Deputy Prime Minister Dmitry Rogozin invoked it as evidence that his country's space program was faltering. "The United States is pushing ahead," he warned Russian lawmakers. Less than two weeks later, Fancy Bear tried to penetrate the Gmail account of a senior engineer on the X-37B project at Boeing.

The hackers also chased people who work on cloud-based services, the off-site computer networks that enable collaborators to work with data that is sometimes classified. For example, the cyberspies tried to get into the Gmail of an employee at Mellanox Federal Systems, which helps the government with high-speed storage networks, data analysis and cloud computing. Its clients include the FBI and other intelligence agencies.

Few warnings from officials. Yet of the 31 targets reached by AP, just one got any warning from U.S. officials. The FBI declined to give on-the-record details of its response to this Russian operation. Agency spokeswoman Jillian Stickels said the FBI does sometimes notify individual targets. "The FBI takes ... all potential threats to public and private sector systems very seriously," she said in an email. However, three people familiar with the matter - including a current and a former government official - previously told the AP **the FBI knew the details of Fancy Bear's phishing campaign for more than a year**. Pressed about notification in that case, a senior FBI official, who was not authorized to publicly discuss the hacking operation because of its sensitivity, said **the bureau was overwhelmed by the sheer number of attempted hacks**. "It's a matter of triaging to the best of our ability the volume of the targets who are out there," he said.

A Pentagon spokeswoman, Heather Babb, said the department recognizes the evolving cyber threat and continues to update training and technology for military, civilian and contract personnel. But she declined to comment on this hacking operation. The Defence Security Service, which protects classified U.S. technology, focuses on safeguarding corporate computer networks. "We simply have no insight into or oversight of anyone's personal email accounts or how they are protected or notified when something is amiss," spokeswoman Cynthia McGovern said in an email.

Former Facebook and Google Workers Launch Campaign to Fight Tech Addiction

https://www.theguardian.com/technology/2018/feb/05/tech-addiction-former-facebook-google-employees-campaign

Reformed techies have united to launch a campaign to put pressure on technology companies to make their products less addictive and manipulative. **“Truth About Tech” is the brainchild of the Center for Humane Technology, a group of former Facebook and Google employees dedicated to “reversing the digital attention crisis and realigning technology with humanity’s best interests” and is funded by Common Sense, a not-for-profit that promotes safe technology and media for children.** The campaign will include educational material aimed at families highlighting the potential harm caused by digital platforms and outlining techniques for mitigating the addictive properties of tech, for example turning off notifications and changing the screen to greyscale. There will also be a lobbying push around the issue calling for policymakers to regulate tech companies using manipulative practices and the two organisations will develop standards of ethical design to help the industry discourage digital addiction.

The Center for Humane Technology is led by former Google design ethicist Tristan Harris and former Facebook investor and adviser Roger McNamee.

“Tech companies are conducting a massive, real-time experiment on our kids, and, at present, no one is really holding them accountable,” said Common Sense’s CEO, James Steyer, warning that tech companies’ attention-grabbing business models may hurt “the social, emotional and cognitive development of kids”. “When parents learn how these companies can take advantage of our kids, they will join us in demanding the industry change its ways and improve certain practices.”

According to research by Common Sense, teenagers consume an average of nine hours of media per day, while tweens consume six hours. A separate study by psychologist Jean Twenge found that heavy users of digital media are 56% more likely to say they are unhappy and 27% more likely to be depressed.

This is the latest chapter in a rising backlash against big tech. Many former employees of large Silicon Valley firms have offered sharp critiques of the industry. **In November, Facebook’s founding president, Sean Parker, said the social network knew from the outset it was creating something that exploited a “vulnerability in human psychology”.** “God only knows what it’s doing to our children's brains," he said. In January, the Salesforce CEO, Marc Benioff, said that Facebook should be regulated like the cigarette industry.

Authorities Shut Down Luminosity RAT Used by Buyers in 78 Countries

https://www.hackread.com/authorities-shut-down-luminosity-rat-used-by-buyers-in-78-countries/
[Note: this does not refer to the Lumosity brain-training app] **The popular Luminosity RAT has been shut down by authorities and its users have no access to it anymore.** In a joint operation, the law enforcement authorities from Australia, Europe, and North America have shut down a "hacking tool" called Luminosity Link RAT (Remote Access Trojan) also known as LuminosityLink. In the operation over a dozen agencies including Europol, UK's South West Regional Organised Crime Unit and National Crime Agency (NCA) took part leading to the successful shut down of the sophisticated trojan.
Luminosity RAT allowed attackers to secretly infect a targeted device by disabling its anti-virus or anti-malware program, spy on the victim by monitoring their online activities, record every keystroke, watch them by enabling their webcam and steal data including login credentials. In a press release, Europol said that Luminosity had over 8,600 users in more than 78 countries and its victims are also believed to be in thousands. Originally, the RAT started targeting victims in May 2015 while the authorities identified its presence in September 2016 on a computer system of a suspect arrested by investigators in Bristol, United Kingdom. NCA has also seized over 100 devices and Internet accounts during the operation which are being analyzed by forensic experts.
According to IT security researchers at Kaspersky, Luminosity was also used by Nigerian hackers in their phishing campaign in which their prime targets were industrial companies. It should not come as a surprise since Luminosity's developers sold it on a website for just £30 ($42 – €33). Here, it is noteworthy that authorities shut down Luminosity in September 2017 but only shared the details of the operation now due to "operational reasons." However, the good news is that the RAT is not functional and those who bought it cannot access it anymore.
According to Detective Inspector Ed Heath, head of the South West Regional Cyber Crime Unit "The sale and deployment of this hacking tool were uncovered following a single arrest and the subsequent forensic examination of the computer. "More than a year's complex work with international policing partners led us to identify a large number of offenders." **Luminosity might be history but there are thousands of RATs and malware targeting unsuspecting users around the world. Therefore, readers are advised to keep their system up to date, do not download files from an anonymous third-party store, avoid clicking the link and downloading attachment files sent by unknown senders**.

Child Abuse Images Behind Apple's Telegram Ban

http://www.bbc.com/news/technology-42959845
Apple removed messaging app Telegram from its app store because some users were sharing images of child abuse. The explanation was revealed in an email from Phil Schiller, manager of the App Store, which was published by Apple news site 9to5Mac. The secure messaging app returned to the app store within hours with fixes to prevent the illegal content being served to users, it said. Mr Shiller said users "who posted this horrible content" had been banned. The email, which 9to5Mac said it had verified with Apple read: The Telegram apps were taken down off the App Store because the App Store team was alerted to illegal content, specifically child pornography, in the apps. "After verifying the existence of the illegal content the team took the apps down from the store, alerted the developer, and notified the proper authorities, including the NCMEC (National Center for Missing and Exploited Children)."
Apple said it had put in place more controls to "keep this illegal activity from happening again". Telegram has been accused of harbouring violent and extremist content on its platform in the past and its use was restricted in Iran in December after claims it was used to organise four days of anti-establishment protests. And in November, Afghanistan moved to ban the app in an effort to prevent the Taliban and other insurgent groups from using it. **The messaging app has a high level of encryption and allows for large chats of up to 50,000 users. Its secret chat function allows messages to self-destruct after they are sent.** Prime Minister Theresa May recently singled out the app as a place where criminals can hide their activities. "No-one wants to be known as the terrorists' platform or the first-choice app for paedophiles," she said.

YouTube Kids App Still Showing Disturbing Videos

http://www.bbc.co.uk/newsround/42958126

[YouTube and YouTube kids are owned by Google.] YouTube says it is "very sorry" after more disturbing videos were found on the YouTube Kids app. Newsround found several videos not suitable for children, including one showing how to sharpen knives. Another had characters from children's cartoon Paw Patrol on a burning plane. YouTube has been criticised for using algorithms rather than human curators to decide what appears on YouTube Kids. In 2015, two child safety groups complained after disturbing videos were found on the YouTube Kids app.

YouTube said it needed to "do more" to tackle inappropriate videos being seen by children. Newsround had arranged for five children to meet Google's Katie O'Donovan. They spoke about distressing videos they had seen on the main YouTube website and app. The videos included images of clowns with blood on them, scary advertisements and messages telling them someone was at their door. Ms O'Donovan said she was "very, very sorry for any hurt or discomfort" caused by the videos. "We've actually built a whole new platform for kids, called YouTube Kids, where we take the best content, stuff that children are most interested in and put it on there in a packaged up place just for kids," she said. But Newsround revealed that it had discovered inappropriate videos there too. They included Mickey Mouse characters with guns and children's characters being injured. YouTube said it had a variety of processes in place to try and prevent inappropriate material appearing on its platforms.

It told Newsround: "We have seen significant investment in building the right tools so people can flag that [content], and those flags are reviewed very, very quickly. We're also beginning to use machine learning to identify the most harmful content, which is then automatically reviewed." Newsround asked whether there was too much content for the platform to check. Google said that ensuring YouTube remained an open platform "comes with real challenges because the content is uploaded and it is live". "It is a difficult balance to get right," YouTube told Newsround, adding: "It is a difficult environment because things are moving so, so quickly." According to YouTube's own statistics, almost a third of internet users use YouTube, and a billion hours of video is watched by those users every day. Newsround asked YouTube whether it had a responsibility to check videos before they go on YouTube Kids. The company said: "We have a responsibility to make sure the platform can survive and can thrive so that we have a collection that comes from around the world on there."

In Just 24 hours, 5,000 Android Devices are Conscripted into Mining Botnet

https://arstechnica.com/information-technology/2018/02/out-of-nowhere-currency-mining-botnet-infects-5000-android-devices/

A fast-moving botnet that appeared over the weekend has already infected thousands of Android devices with potentially destructive malware that mines digital coins on behalf of the unknown attackers, researchers said. The previously unseen malware driving the botnet has worm-like capabilities that allow it to spread with little or no user interaction required, researchers with Chinese security firm Netlab wrote in a blog post published Sunday. **Once infected, Android phones and TV boxes scan networks for other devices that have Internet port 5555 open.** Port 5555 is normally closed, but a developer tool known as the Android Debug Bridge opens the port to perform a series of diagnostic tests. Netlab's laboratory was scanned by infected devices from 2,750 unique IPs in the first 24 hours the botnet became active, a figure that led researchers to conclude that the malware is extremely fast moving. "Overall, we think there is a new and active worm targeting Android systems' ADB debug interface spreading, and this worm has probably infected more than 5,000 devices in just 24 hours," Netlab researchers wrote. "Those infected devices are actively trying to spread malicious code." The researchers said they were withholding some information about the devices that are getting infected, presumably to make it harder for copycat attackers to exploit the same underlying weakness or vulnerability. Once infected, devices are saddled with an app that causes them to mine the digital coin known as Monero. It's not clear what precise effect this mining has on the devices. In past cases, however, Monero mining apps are so aggressive they physically damage the Android devices running them.

Information returned by Monero Hash Vault—the mining pool the malicious apps use to generate the digital coin—showed the attackers have a 24-hour average rate of 7,880 hashes per second. That's a relatively small amount. So far, the attackers have generated 0.0171757089 XMR, which at current prices is worth about $3.

It's not yet clear precisely how devices are getting infected. As noted earlier, Netlab researchers are withholding some details, but they did provide one potential clue when they said some of the infection code relies on Mirai, the malware that compromises routers and other Internet-of-Things devices by guessing default administrator passwords.

Cryptocurrency Botnets are Rendering Some Companies Unable to Operate

https://arstechnica.com/information-technology/2018/02/cryptocurrency-botnets-generate-millions-but-exact-huge-cost-on-victims/

A massive cryptocurrency mining botnet has generated as much as $3.6 million dollars' worth of the digital coin known as Monero since last May, a researcher said Wednesday. The windfall isn't the only noteworthy thing about the botnet. Dubbed Smominru, it's also significant for the 526,000 computers it has infected and for the ability of its operators to withstand takedown attempts by whitehats. "As Bitcoin has become prohibitively resource-intensive to mine outside of dedicated mining farms, interest in Monero has increased dramatically," a researcher, who uses the pseudonym Kafeine, wrote in a blog post published by security firm Proofpoint. "While Monero can no longer be mined effectively on desktop computers, a distributed botnet like that described here can prove quite lucrative for its operators." Like cryptocurrency mining botnets known as Adylkuzz and Zealot, Smominru appropriates potent exploit code developed by the National Security Agency and later published online by a group calling itself the Shadow Brokers.

Like Zealot, Smominru uses other exploit techniques to infect targeted computers, but it can fall back on the NSA-developed EternalBlue in certain cases, presumably for spreading from machine to machine inside infected networks or when other infection techniques fail on a machine that hasn't been patched. Smominru also makes use of the Windows Management Interface. Proofpoint said that the botnet is also likely exacting a punishing performance impact on the business networks it infects by slowing down servers and driving up electricity costs. [see article for more details]

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

****

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

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

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

****