BRITISH COLUMBIA **OCIO** | Office of the Chief Information Officer

Security News Digest
June 13, 2017

There is so much to know about the Internet of Things!
Start by taking the Internet of Things Quiz!

Bank of Canada Warns Financial Sector Vulnerable to Cyberattacks 🇨🇦

http://www.cbc.ca/news/politics/bank-canada-cyberattacks-banks-1.4158068

Canada's interconnected banks are vulnerable to a cascading series of cyberattacks that could undermine broad confidence in the financial system, the Bank of Canada warns. *The structural vulnerability could allow for the easy spread of an initial attack that ripples into other sectors such as energy or water systems, says the bank's June financial review*. The report urges banks to co-operate on countering the threats that are not going away any time soon.

The former head of the U.S. National Security Agency made the same recommendation earlier this month, saying private-sector companies - including banks - have to do a better job of sharing data on attempted hacks in real time to counter the ongoing challenge. Retired Gen. Keith Alexander told a defence industry trade show that *banks have valuable metadata on attempted hacks embedded in the logs of their firewalls and sharing that information can allow them to more successfully fend them off*. *Alexander suggested the 2014 cyberattack on the American bank JPMorgan Chase that affected an estimated 80 million accounts could have been prevented if banks had shared information*.

Canada's central bank expressed a similar concern in its most recent update. "The interconnectedness of the financial system could lead to rapid transmission of stress from a cyberattack," the report said. "This is a structural vulnerability that is unlikely to go away. And because of the interconnections in the system, the public sector has a role in coordinating cyber defences." .."Contagion could occur through financial interconnections or common critical infrastructures in non-financial sectors, such as telecommunications, energy and utilities," it said. "A prolonged interruption in financial services, compromised data integrity or a loss of confidence could harm the financial system with knock-on effects to the real economy." There were eight high-profile cyberattacks on banks in 2016, the report said, including an $81-million heist at the Bangladesh Bank. The report urges private-sector players to work together because protecting against an attack "has benefits beyond an individual institution and can be considered a public good."

The note also underscored the importance of identifying threats and improving the sharing of incident information. ..In that vein, the independent, not-for-profit Canadian Cyber Threat Exchange aims to promptly share threat information between Canadian businesses and government agencies, as well as provide cyber threat analysis and advice for reducing risk.

RCMP Working With Moroccan Police to Lay Charges in U of Moncton Cyberattack 🇨🇦

http://www.cbc.ca/news/canada/new-brunswick/rcmp-police-morocco-moncton-cyberattack-1.4135677

More than three months since a vicious online attack on a female University of Moncton student that authorities have described as "cyberterrorism," the RCMP is reporting progress in its investigation. Starting in late February, a series of ten emails were sent to students and staff, many containing a video or photo of the student that were sexually graphic in nature. The emails also included offensive messages, and links to the student's Facebook page, in an apparent attempt by the sender to shame her. Sgt. Mario Fortin of the Codiac RCMP confirmed to CBC the man behind the attacks lives in Morocco, and that the RCMP is working with Moroccan police, as well as Crown prosecutors, to try to lay charges against the individual. In one of his emails, the attacker had threatened police by saying, "I'm living in Morocco. So just catch me if you can," but authorities had previously disclosed little information on his whereabouts, and would only reveal the emails originated from a server outside the country. Fortin is also confirming the victim and the author of the emails knew each other, but would not disclose the nature of their relationship, or reveal his name.

He said the RCMP is looking at a number of possibilities, including having Moroccan police lay charges, or issuing an arrest warrant here in Canada against the attacker. Meanwhile the University of Moncton confirms there have been no new emails since the tenth one on March 4, but would not provide details on strategies used to intercept the messages - or whether the attacker had simply given up.

Case could pave the way. David Shipley, a cybersecurity expert and CEO of Beauceron Security, said *most cybercrimes remain unresolved forever, and considers the RCMP to be far along in its investigation*. "That is encouraging that they are actually working with authorities in Morocco," said Shipley. "That is not the norm." *Shipley said most cases of online sexual exploitation never get investigated. In fact he estimates only one in 15 cybercrimes get reported to police in Canada. Police only identify a suspect in about 6 per cent of all cases, he said.* "Hopefully this case paves the way for further action. Particularly when these crimes involve borders," said Shipley.

Need for global treaty. Shipley called Canada's laws against these types of activities "groundbreaking" but said Morocco may not be as far along. Since 2015, a new charge was added to the Canadian Criminal Code, allowing police to arrest someone for distributing intimate images of a person without their consent. "Not all jurisdictions have criminalized this kind of behaviour - as reprehensible as it is," he said. Shipley said the University of Moncton incident *highlights the need for a global treaty to legislate cybercrimes, that would either allow for individuals to be extradited to the country where they committed the crime to face justice, or tried in their home country for a crime committed somewhere else*. "Most cybercrimes actually cross borders quite frequently," he said.

CRA Launches Raids in Canada, U.K. to Crack Down on ‘Carousel’ Tax-Fraud Scheme 🇨🇦

https://www.theglobeandmail.com/news/politics/cra-launches-raids-in-canada-uk-to-crack-down-on-carousel-tax-fraud-scheme/article35296779/

The Canadian government fears that it has lost millions of dollars in an elaborate swindle known as a “carousel scheme” that is based on fraudulent sales tax refunds, a government source says. The use of this scheme is prevalent in Europe, but is thought to be relatively new to Canada. At this stage of a continuing investigation, *the Canada Revenue Agency has identified more than $50-million in allegedly fraudulent requests for sales tax refunds*, a government official said. It remains unknown exactly how much money was lost as part of this alleged fraud. The federal tax-collection agency launched a crackdown on the scheme on Tuesday [today], conducting a series of raids in three locations in Canada and six others in the United Kingdom. Canadian and British officials have been collaborating for five years on this investigation, the official said. The Canada Revenue Agency is expected to make public more details on its investigation after the raids are completed.

To make money off of a carousel scheme, fraudsters create shell companies, false commercial transactions and a lengthy paper trail in a bid to convince government agencies that they are eligible for large sales tax refunds. The complex web of companies in this case were set up in Canada and the U.K., *with the fraudsters allegedly creating false transactions to obtain GST or HST refunds for fake transfers of goods and services*.

Canada’s Code Guru James Gosling is an International Star in Computing 🇨🇦

https://www.theglobeandmail.com/news/national/canada-150/canadas-code-guru-an-international-star/article35280585/

Most Canadians have never heard of James Gosling. But *the Alberta-born principal creator of Java – one of the most widely used and longest-lived programming languages in modern computing – is a hero in Silicon Valley. Java is the foundational software behind Android, the operating system found on most mobile devices. By some measures, Java can be found on 97 per cent of enterprise computer systems*, and the virtual-machine systems Mr. Gosling designed for Java are critical to the world of cloud computing. For those who remember the Y2K computing crisis, Java was the main tool used to repair and replace the broken systems. There are millions of Java programmers the world over, and some of those people still stop Mr. Gosling on the street for selfies – as if he were a movie star – and then thank him for their careers. … On May 22, Mr. Gosling returned to the world of big-time software development when he announced he was joining Amazon Web Services (one of the world’s leading cloud-computing providers) as a distinguished engineer. [this lengthy article provides a fascinating look at the evolution of computing and James’ contributions]

Israeli Intelligence Discovered IS Plans for Laptop Bomb: Report

http://www.securityweek.com/israeli-intelligence-discovered-plans-laptop-ban-report

Israeli government spies hacked into the operations of Islamic State bombmakers to discover they were developing a laptop computer bomb to blow up a commercial aircraft, the New York Times reported Monday. *The Times said the work by Israeli cyber operators was a rare success of western intelligence against the constantly evolving, encryption-protected and social-media-driven cyber operations of the extremist group*. It said the Israeli hackers penetrated the small Syria-based cell of bombmakers months ago, an effort that led to the March 21 ban on carry-on laptops and other electronics larger than cellphones on direct flights to the United States from 10 airports in Turkey, the Middle East and North Africa.

The Israeli cyber-penetration "was how the United States learned that *the terrorist group was working to make explosives that fooled airport X-ray machines and other screening by looking exactly like batteries for laptop computers*," the Times said. The intelligence was so good that the detonation method for the bombs was understood, the Times said, citing two US officials familiar with the operation. Following the US laptop ban, Britain announced a similar prohibition for flights originating from six countries. Israel's contribution to the intelligence on the laptop bombs became public after President Donald Trump revealed details on it to Russian Foreign Minister Sergei Lavrov in a May 10 White House meeting. Trump's disclosure "infuriated" Israeli officials, according to the Times.

Watch Out! Scammers Are Making a Fortune in the iOS App Store

https://hotforsecurity.bitdefender.com/blog/watch-out-scammers-are-making-a-fortune-in-the-ios-app-store-18188.html

Just how much money can a scammy iPhone app make in the iOS App Store? You may be surprised. After all, how does $80,000 per month sound to you? *The “Mobile protection :Clean & Security VPN” app is estimated to be have earnt its developer $80,000 per month, after tricking users into signing up for an eye-watering $99.99 per week subscription through a careless thumb press*. The app, promoted through Apple’s new app store search ads, was spotted by developer Johnny Lin who documented his concerns in a blog post. *When first run, the app asks for permission to scan your list of contacts* (what possible reason could it want to do that?) *before informing you that your iOS device is at risk*. Quite why it believes that your iOS device is in peril is a mystery, as the app hasn’t done anything yet. Even more bizarrely, reports Lin, clicking on the “Secure Internet” button pops up a prompt to play a bubble-shooting game! Perhaps wisely Lin declined that offer, but his curiousity was piqued by the subsequent screen that appeared – offering a “free trial” to “instantly use full of smart anti-virus”.

How free? Well, you should read the small print before you offer your fingerprint to Touch ID…“You will pay $99.99 for a 7-day subscription” Yes, the “free trial to Full Virus, Malware scanner” is really a *shocking 7-day auto-renewing subscription costing $99.99*. In short, you could be paying $99.99 per week in order to have all of your internet traffic routed through a complete stranger’s dodgy VPN. And don’t think that no-one would ever be so dumb as to fall for a scam like this. *It’s all too easy to offer your fingerprint without reading the small print. In this case, the deal has been promoted as a free trial and you may not notice – until it’s too late – that you could be spending $400 a month for the privilege*. Sadly it seems that enough people have been falling for the scam to earn the app’s developer a staggering amount of money. Indeed, Lin reports that “Mobile protection :Clean & Security VPN” *managed to make it to the US App Store’s list of top ten grossing productivity apps*. Since Lin’s blog post the apps appear to have been removed from the App Store – but one wonders how many other apps have managed to slip through Apple’s vetting process, and have been promoted through the store’s new ads.

Apple Mac Computers Targeted by Ransomware and Spyware

http://www.bbc.com/news/technology-40261693

Mac users are being warned about new variants of malware that have been created specifically to target Apple computers. One is ransomware that encrypts data and demands payment before files are released. The other is spyware that watches what users do and scoops up valuable information. *Experts said they represented a threat because their creators were letting anyone use them for free. The two programs were uncovered by the security firms Fortinet and AlienVault, which found a portal on the Tor "dark web" network that acted as a shopfront for both*.

In a blog, Fortinet said the site claimed that the creators behind it were professional software engineers with "extensive experience" of creating working code. Those wishing to use either of the programs had been urged to get in touch and provide details of how they wanted the malware to be set up. The malware's creators had said that payments made by ransomware victims would be split between themselves and their customers. Researchers at Fortinet contacted the ransomware writers pretending they were interested in using the product and, soon afterwards, were sent a sample of the malware. Analysis revealed that it used much less sophisticated encryption than the many variants seen targeting Windows machines, said the firm. However, they added, any files scrambled with the ransomware would be completely lost because it did a very poor job of handling the decryption keys needed to restore data. "Even if it is far inferior to most current ransomware targeting Windows, it doesn't fail to encrypt victim's files or prevent access to important files, thereby causing real damage," wrote the researchers.

The free Macspy spyware, offered via the same site, can log which keys are pressed, take screenshots and tap into a machine's microphone. In its analysis, AlienVault researcher Peter Ewane said *the malicious code in the spyware tried hard to evade many of the standard ways security programs spot and stop such programs*. Mr Ewane said Mac users needed to start being more vigilant as malware creators targeted them. "As OS X continues to grow in market share we can expect malware authors to invest greater amounts of time in producing malware for this platform."

Statistics gathered by McAfee suggest that there are now about 450,000 malicious programs aimed at Macs - far fewer than the 23 million targeting Windows users. Aamir Lakhani from Fortinet said Mac users should make sure their machines were kept up to date with the latest software patches and be wary of messages they receive via email. "Mac ransomware is definitely becoming bigger," he told EWeek. "Although market share is still small, hackers know that there is valuable data on the Mac." Apple declined to comment on the developments.

Cybersecurity Firms Uncover Malware that Could Cause Power Outages Around the Globe

http://www.huffingtonpost.com/entry/malware-power-grid_us_593fa144e4b0b13f2c6d9285

Two cyber security firms have uncovered malicious software that they believe caused a December 2016 Ukraine power outage, they said on Monday, warning the malware could be easily modified to harm critical infrastructure operations around the globe. *ESET, a Slovakian anti-virus software maker, and Dragos Inc, a U.S. critical-infrastructure security firm, released detailed analyzes of the malware, known as Industroyer or Crash Override, and issued private alerts to governments and infrastructure operators to help them defend against the threat*. The U.S. Department of Homeland Security said it was investigating the malware, though it had seen no evidence to suggest it has infected U.S. critical infrastructure.

The two firms said they did not know who was behind the cyber-attack. Ukraine has blamed Russia, though officials in Moscow have repeatedly denied blame. *Still, the firms warned that there could be more attacks using the same approach, either by the group that built the malware or copycats who modify the malicious software*. “The malware is really easy to re-purpose and use against other targets. That is definitely alarming,” said ESET malware researcher Robert Lipovsky said in a telephone interview. “This could cause wide-scale damage to infrastructure systems that are vital.” The Department of Homeland Security corroborated that warning, saying it was working to better understand the threat posed by Crash Override. *“The tactics, techniques and procedures described as part of the Crash Override malware could be modified to target U.S. critical information networks and systems,” the agency said in an alert posted on its website*. *The alert posted some three dozen technical indicators that a system had been compromised by Crash Override* and asked firms to contact the agency if they suspected their systems were compromised by the malware.

…Power firms are concerned there will be more attacks, Alan Brill, a leader of Kroll’s cyber security practice, said in a telephone interview. “You are dealing with very smart people who came up with something and deployed it,” Brill said. “It represents a risk to power distribution organizations everywhere.” Industroyer is only the second piece of malware uncovered to date that is capable of disrupting industrial processes without the need for hackers to manually intervene. The first, Stuxnet, was discovered in 2010 and is widely believed by security researchers to have been used by the United States and Israel to attack Iran’s nuclear program.

Raspberry PI Attack Compromises Networks, Steals Admin Credentials

https://www.scmagazine.com/raspberry-pi-attack-compromises-locked-devices-steal-admin-creds/article/666772/

Kaspersky Lab researchers developed a proof of concept attack that *encourages IT pros to think twice about how insider threats can compromise networks*. While other attacks can be carried out which exploit physical access to devices, researchers noted this attack is special because it can be carried out by anyone who has physical access to any USB port on the victim's network and could allow an attacker to retrieve user authentication data even when the targeted system is locked, according to a June 6 blog post. It's also possible to obtain administrator credentials or cookies from a PC and *can be implemented using a device that costs no more than $20 without any special skills*, all that is needed is physical access to corporate computers.

Researchers conducted a series of two experiments to intercept user credentials within the corporate network and to retrieve cookies in a bid to restore the user session on a popular website. *The attacks are carried out by briefly connecting a Raspberry Pi Zero via USB port to the computer within the corporate perimeter*. The device was configured to enumerate itself as an Ethernet adapter on the system it was being plugged into. The attacks were tested against three scenarios which were against a corporate computer logged into a domain, against a corporate computer on a public network, and against a home computer. An intruder could also steal cookies from a PC when a Raspberry Pi Zero is connected to it via USB, however, so far the attack only works when the system is unlocked, which reduces the chances of success, the post said. *Researchers recommend users never leave their systems unlocked, check if there are extra USB devices connected to their computers, regular change passwords, and remain cautious when asked to use unfamiliar flash drives*. *Administrators are encouraged to monitor for suspicious USB's drives and devices connected via USB ports as well*.

“If the network topology allows it, we suggest using solely Kerberos protocol for authenticating domain users,” the report said. “If, however, there is a demand for supporting legacy systems with LLNMR and NTLM authentication, we recommend breaking down the network into segments, so that even if one segment is compromised, attackers cannot access the whole network.” Admins should also restrict privileged domain users from logging in to the legacy systems, especially domain administrators, change domain user passwords regularly, and ensure all of the computers within a corporate network have to be protected with security solutions.

Internet Cameras Have Hard-Coded Password That Can’t Be Changed

https://arstechnica.com/security/2017/06/internet-cameras-expose-private-video-feeds-and-remote-controls/

Security cameras manufactured by China-based Foscam are vulnerable to remote take-over hacks that allow attackers to view video feeds, download stored files, and possibly compromise other devices connected to a local network. That's according to a 12-page report released Wednesday by security firm F-Secure. Researchers at F-Secure documented 18 vulnerabilities that the manufacturer has yet to fix despite being alerted to them several months ago. All of the flaws were confirmed in a camera marketed under the Opticam i5 HD brand. A smaller number of the vulnerabilities were also found in the Foscam C2. *The report said the weaknesses are likely to exist in many other camera models Foscam manufactures and sells under other brand names*.

F-Secure researchers wrote: “The sheer number of vulnerabilities offers an attacker multiple alternatives in compromising the device. Among the discovered vulnerabilities are insecure default credentials and hard-coded credentials, both of which make it trivial for an attacker to gain unauthorized access. Other vulnerabilities allow for remote command injection by an attacker. World-writeable files and directories allow an attacker to modify the code and to gain root privileges. Hidden Telnet functionality allows an attacker to use Telnet to discover additional vulnerabilities in the device and within the surrounding network. *In addition, the device’s “firewall” doesn’t behave as a firewall, and it also discloses information about the validity of credentials*.”

The flaws allow for a wide range of hacks, including using the Internet-connected cameras to participate with other infected devices in distributed denial-of-service attacks, accessing private videos, and compromising other devices connected to the same local network. The vulnerabilities are compounded by the ability to permanently replace the normal firmware controlling the camera with malicious firmware that can survive restarts without being detected.

…. The researchers went on to say that they notified Foscam representatives of the vulnerabilities several months ago and that, to date, the manufacturer hasn't fixed any of them. With no security updates, F-Secure declined to release proof-of-concept exploits. Besides the Foscam and Opticom brands, F-Secure said it was aware of 14 other brands used to market Foscam-made devices. They include: Chacon, Thomson, 7links, Opticam, Netis, Turbox, Novodio, Ambientcam, Nexxt, Technaxx, ,Qcam, Ivue, Ebode, and Sab. People who running one of these devices should strongly consider running them inside a dedicated local network that doesn't have access to other connected devices and can't be reached from the outside Internet.

Mouse Hovering Malware Delivery Scheme Spotted, Called Potentially Very Dangerous

https://www.scmagazine.com/mouse-hovering-malware-delivery-scheme-spotted-called-potentially-very-dangerous/article/667379/

Cybercriminals have started using a new technique to infect computers that only requires a victim place their cursor over a malicious hyperlink for the malware to be injected. The new technique was noticed by several cybersecurity researchers – with dodgethissecurity doing an extensive analysis. The information security blog reported that an attack begins with the target receiving an email containing an attached PowerPoint document.

“This PowerPoint document was interesting to analyze,” the researcher said. "First of all, this document was interesting as it did not rely on macros, JavaScript or VBA for the execution method. Which means this document does not conform to the normal exploitation methods." When the presentation is opened, the target sees a “Loading….Please Wait” message. As with many hyperlinks this appears blue. *When the victim follows their natural inclination to hover their cursor over the “hyperlink” to check where it links, the document executes a PowerShell command*. “When that PowerShell is executed it reaches out to the domain “cccn.nl” for a c.php file and downloads it to disk as a file named “ii.jse” in the temp folder,” Dodgethissecurity wrote. But, the report added, even after waiting eight hours no cybercriminal connected to the system.

Jérôme Segura, lead malware intelligence analyst at Malwarebytes, told SC Media on Thursday that the mouse- over technique is “novel and interesting.” The fact that this attack vector does not rely on a macro could make it less suspicious-looking to users and system administrators. *Luckily, he said, it does not automatically run malicious code but instead requires the user to accept a prompt, before finally infecting them*.

“Like most distribution tactics, the proof of their efficiency is in how widespread their adoption is. For now, we are still seeing malicious spam that contains macros or various scripts. However, we know threat actors keep a tab on infection statistics and can easily adjust their campaigns to pick the one with the best ROI [return on investment],” Segura said.

Limor Kessem, IBM's executive security adviser, noted to SC Media that *since this type of attack is hard to spot everyone has to revert to using their email security scheme*. *"Indeed, this is a new technique and is quite malicious because the user is not taking much action, other than opening the file. This makes it harder to warn users about this method, but at the very least, all email users should be wary when opening files from unsolicited email. If the matter is not clear, it's best to call the sender and verify that the file was indeed sent by them. If the email comes from an unknown source, don't even open email, nor the files it contains,” she said*.

Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known

https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

Russia’s cyberattack on the U.S. electoral system before Donald Trump’s election was far more widespread than has been publicly revealed, *including incursions into voter databases and software systems in almost twice as many states as previously reported*. In Illinois, investigators found evidence that cyber intruders tried to delete or alter voter data. The hackers accessed software designed to be used by poll workers on Election Day, and in at least one state accessed a campaign finance database. Details of the wave of attacks, in the summer and fall of 2016, were provided by three people with direct knowledge of the U.S. investigation into the matter. In all, the Russian hackers hit systems in a total of 39 states, one of them said.

The scope and sophistication so concerned Obama administration officials that they took an unprecedented step - complaining directly to Moscow over a modern-day “red phone.” In October, two of the people said, the White House contacted the Kremlin on the back channel to offer detailed documents of what it said was Russia’s role in election meddling and to warn that the attacks risked setting off a broader conflict. The new details, buttressed by a classified National Security Agency document recently disclosed by the Intercept, show the scope of alleged hacking that federal investigators are scrutinizing as they look into whether Trump campaign officials may have colluded in the efforts. But they also paint a worrisome picture for future elections: The newest portrayal of potentially deep vulnerabilities in the U.S.’s patchwork of voting technologies comes less than a week after former FBI Director James Comey warned Congress that Moscow isn’t done meddling. “They’re coming after America,” Comey told the Senate Intelligence Committee investigating Russian interference in the election. “They will be back.”

Kremlin Denials. Russian officials have publicly denied any role in cyber-attacks connected to the U.S. elections, including a massive "spear phishing" effort that compromised Hillary Clinton's campaign and the Democratic National Committee, among hundreds of other groups. President Vladimir Putin said in recent comments to reporters that criminals inside the country could have been involved without having been sanctioned by the Russian government.

Britney Spears's Instagram is Secretly Being Used by Russian Hackers

https://www.vox.com/world/2017/6/8/15762122/russian-hackers-britney-spears-instagram

In order to hack foreign governments, military officials, and embassies, Russian hackers are now using Britney Spears in their operations *by posting cryptic comments on her Instagram photos*. Hackers at Turla, a group believed to be linked to Moscow, are using Instagram comments on Britney Spears's photos *to control their hacking operation*, said researchers at Slovakian security firm ESET in a report on Tuesday.

Here's the comment that was posted in February (and has since been deleted) on a photo Spears posted in January: By Instagram user asmith2155: #2hot make loved to her, uupss #Hot #X The comment doesn't make sense and doesn't seem threatening to the untrained eye. *But, according to ESET, it's key to the hackers' success*. The process for how the whole operation works is *complicated*. *After compromising computers, hackers need a way to send them instructions and get data back*. They often set up a command and control server to do this. Security professionals defending against cyberattacks usually try to find the central server and shut it down in hopes of crippling the entire network. The comment on Britney Spears's photo is a clever strategy for announcing the location of a new command and control server after the previous one gets shut down. When decoded, it's actually the central server's internet address.

Compromised machines are programmed to periodically scan for these specially-targeted comments on the Spears Instagram page so they're able to continue communicating with the hackers even after the initial command and control server gets shut down. Turla has a long history of attacking governments and organizations. It previously targeted embassies in Ukraine, China, Germany and several other countries, a state electrical authority in the Middle East, and a medical organization in the US, according to Symantec, a security software company based in the US. *According to experts, Turla is likely linked to the Russian government*. "It is sophisticated malware that's linked to other Russian exploits, uses encryption and targets western governments," said Jim Lewis, a former US foreign service officer, in a Reuters article. *"It has Russian paw prints all over it."*

So why are the Russian hackers now targeting an American pop star's Instagram account? The answer is simple: Web traffic from users around the world is constantly flowing through Instagram. It would be *incredibly easy to hide malicious comments and links on photos posted by celebrities*. For example, Britney Spears currently has 16.9 million Instagram followers. The post that was targeted has more than 420,000 likes and 2,200 comments. *That makes it much harder for defenders to track hackers' actions* - if it wasn't for ESET's research, that one comment would've been lost.

Another reason is that it's very easy for the hackers to delete a comment, which would erase any trace of a hacking attempt. After deleting the comment, they could easily post another comment that would lead to a new central server. *In this case, the hackers didn't delete the comment, and ESET believe it was just a test of their new way of communicating*.

The discovery raises questions about what else is hiding in the comment sections of celebrities' social media pages and how Russian hackers are getting creative to avoid tracking.

Android Smartphones Targeted by WannaCry Lookalike

https://www.bleepingcomputer.com/news/security/android-smartphones-targeted-by-wannacry-lookalike/

Crooks in China have developed an Android ransomware that uses similar graphics to the WannaCry ransom note in an attempt to scare and trick users into quickly paying the ransom. Spotted by Qihoo 360 researchers, crooks are spreading this ransomware via Chinese gaming forums. The malicious app containing the ransomware tries is disguised as a plugin for the King of Glory, a very popular mobile game in China.

Some people just wanna get arrested. By the looks of it, the ransomware is obviously the work of amateur ransomware operators who have a fetish for getting arrested. Unlike 99.9% of today's ransomware, this WannaCry lookalike for Android devices is asking users to pay the ransom fee of 40 Chinese Renminbi ($6) via Chinese payment providers QQ, Alipay, or WeChat. Its authors have either not heard of Bitcoin before, or bumped their head and forgot they live in China, the country where authorities have the deeper access to data from technology firms. [ha, ha, good one..] It would take police minutes to track down who's on the receiving end of all the ransom payments and crack down on its operators.

WannaCry lookalike uses solid encryption. *Outside of the idiotic method of handling ransom payments, this WannaCry lookalike for Android is pretty solid code-wise*. For starters, the ransomware actually encrypts files, which is pretty impressive if we take into account that most Android ransomware is still at the screen-locker level. The ransomware uses AES encryption to lock files, and it will append a suffix to all encrypted files consisting of a mixture of Chinese and Latin characters. Because resources are limited on Android devices, the ransomware will only encrypt files under 10KB in size. To avoid ruining and crashing the Android OS, the ransomware doesn't encrypt files whose names start with a dot, or files located in folders that include ”android", "com", "DCIM", "download", or "miad" in their file path. According to Nikolaos Chrysaidos, security researcher for Avast, this ransomware - which the company named WannaLocker - only encrypts files on the smartphone's external storage.

Look at This Massive Click Fraud Farm that Was Just Busted In Thailand

https://motherboard.vice.com/en_us/article/look-at-this-massive-click-fraud-farm-that-was-just-busted-in-thailand

[Definition: **Click fraud** is an illegal practice that occurs when individuals click on a website's click through advertisements (either banner ads or paid text links) *to increase the payable number of clicks* to the advertiser. The illegal clicks could either be performed by having a person manually click the advertising hyperlinks or by using automated software or online bots that are programmed to click these banner ads and pay per click text ad links.]]

A significant portion of internet traffic isn't real. It's perpetuated by bots*, fake accounts set up to artificially inflate the popularity of a website, social media post, or advertisement. On Sunday, the world got a rare look at what the click fraud business really looks like*. When police raided a rented home in Thailand, they discovered Wang Dong, Niu Bang, and Ni Wenjin *were running an extensive fake click enterprise*. The three Chinese individuals were arrested on charges including working without a permit and smuggling SIM cards into the country.

Inside their house located near the Cambodian border was a makeshift metal rig fitted with 500 smartphones, which were each wired to a computer monitor. In total, Thai police reportedly seized almost 350,00 SIM cards, 21 SIM card readers, and nine computers from the men. *The officers initially believed the rig was used to run a fraudulent call center, a common crime in Southeast Asia. The trio explained that they were actually operating* ***a network of so-called sock puppet accounts*** *[an online identity used for the purpose of deception] on China's largest social network, WeChat*.

A company in China reportedly supplied the phones and paid the men 150,000 baht ($4403) a month for the operation, according to a Thai immigration officer. The click farm proprietors likely headquartered their business overseas because Thailand has relatively low smartphone usage fees. Buying SIM cards in bulk is also increasingly difficult in China. Last year, the government began requiring users (including foreigners) to provide identification before registering one. Thailand, though, has similar requirements. It's not clear how the Chinese nationals obtained so many SIM cards. The rig the Chinese men built isn't unique. *Dozens of similar click farm setups have been documented across China*.

It's difficult to estimate how large of a problem click fraud is on WeChat. The messaging platform, which has more than 880 million monthly active users, is considerably more private than open social networking sites like Twitter. Created in 2010, WeChat is designed for small groups and individuals to message one another. It works similarly to WhatsApp. Since all groups are visible by invitation-only, it's difficult to monitor problems like click fraud and fake news (there is an option for businesses and other groups to create "official accounts," which are public).

Criminal Gang Arrested for Selling Apple Users’ Private Data in China

https://www.theguardian.com/technology/2017/jun/09/apple-employees-arrested-selling-private-user-data-china-criminal

A massive underground criminal operation run by employees of an Apple “domestic direct sales company and outsourcing company” to steal and sell the private data of Apple users has been uncovered in China, according to authorities. Chinese law enforcement detained 22 people on suspicion of infringing the privacy of Apple users and illegally obtaining their digital personal information, according to local police in southern Zhejiang province. The authorities did not specify whether the data belonged to Chinese or

foreign Apple users. Of the 22 suspects, 20 were employees of companies who worked with Apple, who allegedly used internal systems to gather users' names, phone numbers, Apple IDs and other personal data, which was then sold as part of a scam worth more than 50m yuan (£5.8m).
A co-ordinated effort, following months of investigation and involving police across the Guangdong, Jiangsu, Zhejiang, and Fujian provinces, *saw the 22 suspects apprehended, their "criminal tools" confiscated and their online network dismantled*. *The suspects worked in direct marketing and outsourcing for Apple in China*, and allegedly charged between 10 yuan (£1.15) and 180 yuan (£20.76) for pieces of the illegally extracted data. The sale of personal information is common in China, which implemented a controversial new cybersecurity law aimed at protecting the country's networks and private user information on 1 June. In December, an investigation by the Southern Metropolis Daily newspaper exposed a black market for private data gathered from police and government databases. Reporters successfully obtained a trove of material on one colleague, such as flight history, hotel checkouts and property holdings, in exchange for a payment of 700 yuan (£80.77). Apple declined to comment.

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 Technology, Innovation and 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.

****