Security News Digest
August 08, 2017

Sent out Friday, August 04 (just like the magazines do it)
Have a Safe and Secure holiday weekend!

Play the new fun game: Dog Days of Summer quiz

Free Wi-Fi has Driven 88% of Canadians to Put Their Personal Info at Risk: Report

http://globalnews.ca/news/3647564/free-wifi-security-canadians/

A strong Wi-Fi signal is one major factor that helps Canadians decide where they want to stay when they go away for long weekends, said a risk report released by Norton last month. *And while a hefty majority of Canadians believe their information is safe while using public Wi-Fi networks at hotels, restaurants and elsewhere, the report reveals that these services aren't as secure as users might like to believe they are*. **"The most common misconception about public Wi-Fi is that it's secure,"** Kevin Haley, Norton's director of security response, said in an email. *Haley said that 64 per cent of Canadians feel their personal information is safe when using public Wi-Fi. That's higher than the global average of 60 per cent. However, "88 per cent of consumers have potentially put their information at risk while using public Wi-Fi by accessing their personal email, bank accounts or other financial information," he added*.
Risky behaviours on public Wi-Fi include logging into personal email accounts, checking bank accounts or accessing personal financial information. They also include sharing photos on social media or logging into work email. More than half of Canadians (53 per cent) don't know how to tell the difference between a secure and an unsecured public network, and therefore aren't taking necessary precautions to protect their personal information. "Public Wi-Fi hotspots are open networks, which means anyone with the right tools can access the information as it travels on the network," Haley added.
Sixty-six per cent of Canadians said that Wi-Fi access was a deciding factor when choosing a hotel, while 36 per cent said it was a deciding factor when choosing a place to eat or drink and 32 per cent said it helped them decide on an airline. Norton's study also found that almost half of Canadians (46 per cent) can't wait more than a few minutes before logging onto a Wi-Fi network or asking for the Wi-Fi password at a friend's place. One of the best ways to ensure your personal information is protected while using public Wi-Fi networks is to *use a VPN (virtual private network) from a trusted security vendor*. A VPN is used to create a secure, encrypted connection between a computer and a server, according to *PCMag.*
A user's information is encrypted when using a VPN, "so even if a hacker is snooping on the network, they can't see your information." There are many VPN services available to users who travel often or just want an extra layer of security when browsing the web. While 88 per cent of Canadians have put their personal information at risk over a public network, 84 per cent don't use a VPN to secure their Wi-Fi connections. Many Canadian cities see public Wi-Fi networks as gateways to smarter, more efficient communities - despite the risks. *Therefore, many popular destinations and websites have taken steps to improve the security of their Wi-Fi connections by adding HTTPS networks, which are secure connections that encrypt the data going back and forth*. "They've done this so that even when people access them in hostile environments, they're protected from some of the lowest common denominator attackers sitting on an open-end Wi-Fi network and looking for victims," said Chad Thunberg, COO of Leviathan Security Group in Seattle, told NBC News.
"So year-over-year, we are safer today when using public Wi-Fi than we were previously," he said.
Despite this, Haley warned frequent travelers and social media mavens not to let their guard down, as public Wi-Fi will always come with a certain degree of risk. "Wherever there are public Wi-Fi hotspots, you run the risk of a hacker tapping the network."

Confidential Documents Sent to Personal Email of Manitoba Premier's Wife

https://www.winnipegfreepress.com/local/confidential-documents-sent-to-personal-email-of-premiers-wife-438092753.html

[Manitoba Premier] Brian Pallister's wife Esther frequently communicated with senior government staffers, helping to arrange meetings for the premier and even receiving sensitive documents by email on his behalf. Over the past two days, the provincial NDP have released telephone and email records, gained through freedom of information legislation, that provide insight into how the premier does business - and his apparent dislike, even aversion, to smartphones and email.
Records show that a senior government official sent a draft of this spring's budget speech to Esther Pallister's private email account for the premier's perusal nine days before it was delivered in the legislature. Another time, the premier's wife received a legal opinion for her husband to read. The premier and his wife may not have broken any laws in handling sensitive legal and budget information the way they did. But politicians are coming under increasing scrutiny across North American on their handling of email - and the trend is to frown on the use of private email accounts in conducting government business.
The Pallister government at first resisted attempts to make Esther Pallister's phone and email records public, but the NDP appealed to the provincial ombudsman's office for assistance and the province relented, releasing the information on July 14. That same day, the government issued a new policy directive requiring that cabinet ministers and staff use their government assigned email accounts, phones, text and messaging applications when conducting government business. The fact that Esther Pallister's private cellphone and email accounts were used as a conduit to the premier raises questions about the government's past handling of sensitive information and whether cabinet confidentiality was broken.
NDP MLA Andrew Swan, a former justice minister, said the use of a private email account had security risks. He said the province employs a staff of technical experts whose job it is to "keep emails safe." "There's no valid reason why the premier of a province in 2017 could not figure out how to use a smartphone and how to use government email to conduct government business," he said. The premier may also have been attempting to hide his communications from freedom of information requests, Swan speculated, something that, if true, proved to be unsuccessful.
….. *Meanwhile, those who know the premier say his unwillingness to use email and smartphones is a matter of personal preference and work style*. Five years ago, when he was acclaimed as leader of the Progressive Conservative party, staff would often reach Pallister at odd hours through his wife's cellphone because it was said that he did not own one. Manitoba's 22nd premier is more apt to mail someone a handwritten note than fire off an email when he wants to communicate something that isn't urgent. "A lot of people question why he can't adapt to modern technology. He's got lots of help around him," said one observer. "I don't think he ever touches the email."

Many in Atlantic Canada Lose Cellphone, Internet Service in Major Outage

https://www.theglobeandmail.com/news/national/much-of-atlantic-canada-loses-cellphone-service-in-widespread-outage/article35881182/
[Aug4] Many Atlantic Canadian consumers and businesses lost cellphone and other network services on Friday, in *a widespread outage that hampered emergency communications, airports and other services*. *Bell called it a "major service outage" affecting internet, TV, wireless and landline phones, with landline 911 service intermittent*. Flights were delayed at multiple airports, some consumers couldn't use their debit and credit cards, and the TD bank said some branches in the region were "temporarily" closed.
"Bell apologizes for this situation and we are working to restore service as quickly as possible," Bell's Nathan Gibson said in a statement at about 1:30 p.m. AT. The outages weren't confined to Bell. Telus, which shares infrastructure with Bell, confirmed it is also down: "We're currently investigating a network issue affecting mobility customers in the East." Telus said on its web site that a "possible fibre cut on Bell network" was to blame.
[Follow-up from Global News: "A cut cable has been identified as the root cause of the network outage, affecting approximately 885 LTE cell sites throughout New Brunswick, Newfoundland, Nova Scotia, and Prince Edward Island," a service alert on the Telus website states. .."Technicians are on-site, and working towards restoring services as quickly as possible."]

Facebook to Step Up Fact-Checking in Fight Against Fake News

http://www.cbc.ca/news/entertainment/facebook-related-articles-fact-checking-1.4233412
Facebook is to send more potential hoax articles to third-party fact checkers and show their findings below the original post, the world's largest online social network said on Thursday as it tries to fight so-called fake news. The company said in a statement on its website it will start using updated machine

learning to detect possible hoaxes and send them to fact checkers, potentially showing fact-checking results under the original article. It's a further roll out of testing started in April.
Facebook has been criticized as being one of the main distribution points for so-called fake news, which many think influenced the 2016 U.S. presidential election. The issue has also become a big political topic in Europe, with French voters deluged with false stories ahead of the presidential election in May and Germany backing a plan to fine social media networks if they fail to remove hateful postings promptly, ahead of elections there in September.
On Thursday Facebook said in a separate statement in German that a test of the new fact-checking feature was being launched in the United States, France, the Netherlands and Germany. "In addition to seeing which stories are disputed by third-party fact checkers, people want more context to make informed decisions about what they read and share," said Sara Su, Facebook news feed product manager, in a blog. She added that Facebook would keep testing its "related article" feature, which suggests additional articles on the same topic from different viewpoints or outlets, and work on other changes to its news feed to cut down on false news.

Hackable Door Locks? Senators Want to Make Smart Gadgets More Secure

http://money.cnn.com/2017/08/02/technology/business/iot-bill-senate-security/index.html

Billions of internet-connected things like smart light bulbs are expected to pop up in our homes and businesses in the coming years. And a group of senators wants to help make them more secure. The bipartisan group introduced a bill on Tuesday to address some concerns regarding the so-called Internet of Things (IoT). *It would require any companies that provide the federal government with internet-enabled devices to meet basic security requirements. Devices must be able to receive software updates, have login credentials that can be changed by the user, and not have any known vulnerabilities*. The bill, introduced by Democrats Mark Warner and Ron Wyden and Republicans Cory Gardner and Steve Daines, *also requires devices to use standard technology protocols*.
Government agencies could ask to use devices that don't meet these requirements, but only if other security measures are in place. The proposed bill addresses the concern that devices connected to the internet - like cameras, coffee makers, and door locks - can be insecure gateways into home or business networks. Vulnerable devices can also be hijacked to create an army of zombie computers called a botnet. Last year, a big cyberattack turned vulnerable security cameras into a botnet that took down major websites including Netflix and Twitter. *The so-called Mirai attack motivated the drafting of Tuesday's bill because it revealed how insecure smart devices can cause real harm*, said Josh Corman, director of the Cyber Statecraft Initiative at the Atlantic Council. Senators consulted with Corman while drafting the bill.
"Every Christmas when we have more and more IoT devices like Hello Barbie and Amazon Echoes, there's more fertile soil for these attackers to launch bigger attacks," Corman told CNN Tech. The number of Internet of Things devices is expected to top 20 billion by 2020. *Also included in the bill is a provision that some security researchers should be able to look for vulnerabilities in smart devices without the threat of a lawsuit*. Currently, researchers are hamstrung by certain laws. ..While the bill targets companies that want to supply the government with smart devices, it will have a trickle-down effect on consumers. The government wants to protect itself and national security interests. But consumers buy smart devices, too. And tech companies won't make different versions depending on the customer.

Security Flaw Made 175,000 IoT Cameras Vulnerable to Becoming Spy Cams for Hackers

http://www.techrepublic.com/article/security-flaw-made-175000-iot-cameras-vulnerable-to-becoming-spy-cams-for-hackers/

Some 175,000 Internet of Things (IoT) connected security cameras are vulnerable to hacks that would allow cybercriminals to enter a user's network, spy on the owner, or become part of a malicious botnet, according to a new report from security provider Bitdefender. *The cameras are manufactured by Shenzhen Neo Electronics, a Chinese company that provides surveillance and security solutions such as sensors, alarms, and IP cameras. Researchers found several buffer overflow vulnerabilities present in two cameras studied: The iDoorbell model, and the NIP-22 model. However, it's likely that all cameras sold by the company use the same software, and are also vulnerable, the report noted*. "These vulnerabilities could allow, under certain conditions, remote code execution on the device," the report stated. "This type of vulnerability is also present on the gateway which controls the sensors and alarms." This could allow hackers to potentially disable alarms or sensors as well.

The cameras use Universal Plug and Play (UPnP) to open ports on the router, so they can be accessed from the outside world, the report stated. Using the Shodan search engine, researchers could find all cameras discoverable on the internet. They found between 100,000 and 140,000 devices when searching for the HTTP web server, and a similar number when searching for the RTSP server - both of which are vulnerable. However, researchers estimate the actual number of unique, at-risk devices is about 175,000. Researchers were able to compromise the vendor's IPTV and gateway products by remote exploitation that is easy to do due to the devices' use of UPnP.
In 2016, Bitdefender security researchers also detected multiple vulnerabilities in a number of IoT devices, including WeMo switches, LinkHub, LIFX Bulb, and the MUZO Cobblestone audio receiver. This proof of concept attack confirms once again that most Internet of Things devices are trivial to exploit because of improper quality assurance at the firmware level," the report stated.

Amazon Suspends Sales of Blu Phones for Including Preloaded Spyware, Again

https://www.theverge.com/2017/7/31/16072786/amazon-blu-suspended-android-spyware-user-data-theft

Blu, a Miami-based budget Android phone company, has been suspended from selling on Amazon after cybersecurity experts detailed how *software preloaded onto its devices collects sensitive user data and sends it overseas*, according to *CNET*. Kryptowire, a Virginia-based security firm, said last week during the BlackHat security conference in Las Vegas that spying software from Chinese company Shanghai Adups Technology was still present on certain Blu handsets. *The software leaves users vulnerable to remote takeovers and having their text messages and call logs recorded, as well as other forms of discrete data collection*. ..This is not the first time Blu has gotten into trouble for skirting both US privacy regulations and Amazon's marketplace rules. Blu was suspended back in October after Kryptowire first discovered Adups' spyware on the Blu R1 HD, the best-selling phone on Amazon and the company's most popular model. Adups called the implementation of tracking software a "mistake" at the time and removed it from the R1 HD and the Life One X2 models. However, this time around, Kryptowire discovered similar software, which was collecting device identification data and even location data from cell tower IDs, loaded onto slightly more expensive Blu phones.

Personal Info of 650,000 Voters Discovered on Poll Machine Sold on EBay

http://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462

When 650 thousand Tennesseans voted in the Memphis area, *they probably didn't expect their personal information would eventually be picked apart at a hacker conference at Caesars Palace Las Vegas*. The strength of the US voting system, according to former FBI director James Comey, is that it's "clunky" - every state and often every district can choose its own setup and whether to use paper or electronic machines. And there are over a dozen different manufacturers supplying voting machines to electoral districts. While that clunkiness helps prevent large-scale voter hacking, it provides more opportunities for hackers to access polling data.
When US government workers decommission old voting equipment and auction them off to the public, they're supposed to wipe voter information from the device's memory. But hackers given access to an ExpressPoll-5000 electronic poll book - the kind of device used to check in voters on Election Day - have discovered the personal records of 654,517 people who voted in Shelby Country, Tennessee. It's unclear how much of the personal information wasn't yet public. Some of the records, viewed by Gizmodo at the Voting Village, a collection of real, used voting machines that anyone could tinker with at the DEF CON hacker conference in Las Vegas, include not just name, address, and birthday, but also political party, whether they voted absentee, and whether they were asked to provide identification. Election Systems and Software (ES&S), which makes the ExpressPoll-5000, is one of the most popular e-poll book manufacturers in the country, said Barbara Simons, who sits on the board of Verified Voting, a nonpartisan research group that advocates for voting-machine security. There's no formal auditing process for how many of the machines are properly wiped, and thus no way to estimate how many machines have been sold that inadvertently contain voter records.
But the fact that only a handful of such machines were made available at DEF CON and one of them had personal records that were so easily available doesn't inspire confidence, said Matt Blaze, a renowned security researcher who has authored several studies on voting machine security and who helped organize the village. "How many other of these machines that also have data left on them have been sold to who knows who? There's no way of knowing," Blaze told Gizmodo.

After being sold at government auction, many machines are later resold, often for a few hundred dollars. Harri Hursti, a voting machine expert who famously found a critical flaw in Diebold voting systems, helped coordinate the machines' purchase for the conference by scouring eBay. The one seller he visited in person before buying had filled an entire warehouse with voting machines bought at auction, he said. Anyone with access to such a device - whether on Election Day or while playing with an ExpressPoll-5000 at home - would need only moderate computer skills to check for those records. They're stored on a removable memory card. Anyone who pulls out the drive and reads the memory card with their computer will see the drive's contents, including the giant database of personal records, if it hasn't been wiped. Josh Palmer, the security researcher who first discovered the database, said that once he held the memory card and a reader that connected to his laptop, it was simply a matter of finding and loading the giant file. ..Soon after Palmer's discovery, the conference confiscated the card to protect the voters included in the database. "We're notifying the county and letting them know of a potential data breach," Blaze said.

New Game of Thrones Episode Leak Wasn't Part of HBO Hack

https://www.theverge.com/2017/8/4/16094764/game-of-thrones-episode-4-leak-hack-star-india-hbo

[Aug4] An unaired episode of *Game of Thrones* appeared on the internet early this morning. *While HBO's servers were breached earlier this week, The Verge has learned that this episode leak was not part of that successful hacking attempt. Sources familiar with HBO's security breach tell The Verge that a leak from a distribution partner is the source of this episode appearing online*.

The distribution partner is Star India, and the company's logo appears watermarked throughout the leaked episode. *A Star India spokesperson confirmed the leak* in a statement to *The Verge*. "This confirms the compromise of episode 4 of Game of Thrones Season 7, earlier this afternoon," says a Star India spokesperson. "We take this breach very seriously and have immediately initiated forensic investigations at our and the technology partner's end to swiftly determine the cause. This is a grave issue and we are taking appropriate legal remedial action." HBO has struggled to run its own operations in India, and handed off distribution duties to Star India back in 2015. While additional episodes could leak from this particular distribution partner, it appears that the HBO hackers haven't managed to obtain full episodes. Hackers reportedly stole 1.5 terabytes of data, but have only published scripts for upcoming episodes.

Marcus Hutchins, IT Expert Who Stopped WannaCry Cyberattack, Arrested in U.S.

http://globalnews.ca/news/3646639/marcus-hutchins-wannacry-arrested/

Marcus Hutchins, the 22-year-old IT expert who helped thwart a global ransomware attack, was arrested in the United States. Hutchins made international news after he helped stop the WannaCry ransomware threat on a hunch earlier this year. WannaCry infected over 300,000 machines in 150 countries. He was in Las Vegas for the hacker conferences DefCon and Black Hat. He was arrested at the airport on Wednesday, a friend told Motherboard. The friend tried to visit Hutchins at Henderson Detention Center in Nevada the next morning, but was told Hutchins had been moved. "We still don't know why Marcus has been arrested," the friend, who was granted anonymity, told Motherboard.

Those who work in the industry say he was taken to an FBI facility. "We are aware of the situation," a spokesman for the U.K.'s National Cyber Security Centre told the BBC. "This is a law enforcement matter and it would be inappropriate to comment further." *U.S. law officials told CNN the charges are related to the creation and distribution of "the Kronos banking Trojan." A grand jury indictment was filed on July 12, 2017*. Colleagues of Hutchins have started defending him online. ..The Electronic Frontier Foundation, which says it defends civil liberties in the digital world, says, "EFF is deeply concerned about security researcher Marcus Hutchins' arrest. We are looking into the matter, and reaching out to Hutchins."

Someone has Emptied the Ransom Accounts from the WannaCry Attack

http://money.cnn.com/2017/08/03/technology/wannacry-bitcoin-ransom-moved/index.html

For months, the ransom money from the massive WannaCry cyberattack sat untouched in online accounts. Now, someone has moved it. *More than $140,000 worth of digital currency bitcoin has been drained from three accounts linked to the ransomware virus that hit hundreds of thousands of computers around the world in May. It's unclear, though, who emptied the accounts and why*. If the WannaCry hackers are finally trying to get their hands on the money, they'll have to outwit law enforcement agencies from around the globe.

It's a fresh twist in the mysterious attack that cybersecurity experts have linked to a hacking group associated with North Korea. When the WannaCry virus started spreading through more than 150 countries - infecting hospitals, businesses and government systems - it demanded that victims pay a $300 ransom using bitcoin. Bitcoin transactions and accounts are public, but they're also anonymous. The transfers from the WannaCry accounts late Wednesday first drew attention through the Twitter bot @[actual_ransom], which was set up to monitor them. *The funds were moved from the three main accounts tied to WannaCry to nine other bitcoin accounts. If the hackers who carried out the cyberattack are moving the ransom money, they're almost certainly aware they're being watched*.
…. Melanie Shapiro, CEO of identity security firm Token, said the funds in the bitcoin accounts are probably being moved to make them less traceable. "We can watch all of this bitcoin be moved around, but inevitably every move makes it harder to trace back to an individual," she said. *There are services called "tumblers" that let people break up funds into tiny transactions that are harder to trace, Shapiro noted*. For the time being, researchers and officials will be watching the new bitcoin accounts into which the money has been moved in order to track what happens to it next.

Interpol, Group-IB Unmask Pro-ISIS Hackers

http://www.securityweek.com/interpol-group-ib-unmask-pro-isis-hackers

Interpol has teamed up with Russian security firm Group-IB in an effort *to identify the members of a pro-ISIS hacker group that has taken credit for many website defacements and distributed denial-of-service (DDoS) attacks. The group, calling itself the United Islamic Cyber Force (UICF), has carried out numerous attacks since January 2014*. It has contributed to **hacktivist** campaigns such as OpFrance, which included attacks on the TV5Monde TV station and Notepad++, OpIsrael, OpIndia, Operation Free Palestine and Operation Free Al-Aqsa.
According to Group-IB, UICF has had over the years at least 40 members who were connected to over 60 pro-Islamic hacker groups from around the world. The security firm has traced the online monikers used by UICF hackers to individuals in Indonesia, Pakistan, Morocco, Algeria, Nigeria, India and Kosovo. Using the aliases and email addresses posted by the hackers on the websites they defaced, researchers managed to identify several individuals allegedly involved with UICF. *"Their low level of technical training, a sense of impunity and excessive ambitions cause hacktivists not to pay due attention to their own security, despite the various instructions for ensuring anonymity popular in their milieu,"* said Dmitry Volkov, Group-IB co-founder and head of the company's threat intelligence department. "Information published by the hacktivists helped us a great deal in our investigations." The email addresses and aliases were linked by Group-IB to personal websites and social media profiles that appear to have been registered using the hackers' real names.
The security firm's report includes censored pictures, social media accounts, and redacted phone numbers and email addresses allegedly belonging to members of the hacker group. "From their profiles, none of the hacktivists from the United Islamic Cyber Force looks like professional cybercriminals who attack banks, government institutions or strategic infrastructure facilities," Group-IB said in its report. "They are yesterday's schoolchildren and students, with a limited life experience, easily amenable to someone else's influence. *Their goal is not to steal money, but publicity – coverage of their actions by the world media.*"

Indonesia to Deport 153 Chinese for $450 Million Scam

http://www.securityweek.com/indonesia-deport-153-chinese-450-million-scam

Indonesia will deport 153 Chinese nationals arrested for alleged involvement in a multimillion-dollar cyber fraud ring targeting wealthy businessmen and politicians in China, police said Tuesday. *The syndicate, who ran their operation from abroad to avoid detection by Chinese officials but did not target any victims in their host country*, made around six trillion rupiah ($450 million) since beginning operations at the end of 2016, Indonesia police said. They were arrested following a tip-off from Chinese authorities. "We are conducting an intensive investigation and currently coordinating with the Chinese police to deport them," said national police spokesman Rikwanto, who goes by one name.
The group, based in several locations across Indonesia, contacted victims pretending to be Chinese police or law officials, promising to help resolve their legal cases in return for immediate cash transfers, Jakarta police said. The criminal network included IT specialists who would retrieve information on victims and develop communications systems for contacting them, he said. ..Cyber criminals targeting victims in China have increasingly exploited technological advances to operate from abroad, spreading

across Southeast Asia and beyond in recent years. ..China has become increasingly assertive in extraditing suspects.

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

****

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

****