BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

June 19th, 2018

June is IoT (Internet of Things) Month

Take our monthly quiz and test your knowledge

This week's stories:

- New federal cyber strategy skirts questions of security vs. privacy 🇨🇦
- Canada's spy agency expands its cyber security role 🇨🇦
- Find Out if Your Password Has Been Leaked in a Data Breach With This Chrome Extension
- Apple to close iPhone security gap police use to collect criminal evidence
- Bank of Chile Trading Down After Hackers Rob Millions in Cyberattack
- Study finds hundreds of stalker apps, few ways of finding them on your phone
- iPhones will share your exact location with 911
- Chinese tech firm Huawei is fighting back in Australia following reports that authorities could ban it from any involvement in building 5G mobile networks in the country.
- Can we trust AI if we don't know how it works?
- Kaspersky Lab halts European cybercrime work
- Rootkit-Based Adware Wreaks Havoc Among Windows 10 Users in the US
- Gaming Companies Remove Analytics App After Massive User Outcry
- Android App Devs Find Clever Trick for Fooling Users Into Installing Their Crapware
- Europol Dismantles One of the Internet's Oldest Hacker Groups
- Police Use of Minority Report-Style Pre-Crime Tech Raises Inaccuracy Concerns

New federal cyber strategy skirts questions of security vs. privacy 🇨🇦

http://www.cbc.ca/news/politics/cyber-security-strategy-goodale-1.4703107

Canada's much anticipated cyber security strategy, released Tuesday, has exposed one of the key problems facing the federal government in the digital age.

The strategy warns of the need for better encryption to safeguard data — particularly against the lightning advances of quantum computing.

But it also places an extraordinary emphasis on increased national security and combating an explosion in cyber crime, which often stymies authorities by exploiting some of the best encryption available.

So the federal government has to somehow strike a balance between securing data and fighting the encryption used to secure it. The strategy unveiled today suggests that it hasn't struck that balance yet.

Click link above to read more

Canada’s spy agency expands its cyber security role 🇨🇦

https://www.thestar.com/news/canada/2018/06/12/canadas-spy-agency-expands-its-cyber-security-role.html

OTTAWA–Canada’s electronic spies have been given almost total responsibility for defending the federal government’s computer networks against cyber attacks and hacks.

Under the Liberal government’s updated cyber security plan, released Tuesday, the Communications Security Establishment (CSE) will become a “one-stop shop” for defending federal networks and systems.

The federal government has announced the establishment of a new Canadian Centre for Cyber Security. Public Safety Minister Ralph Goodale says the centre will provide expert support to governments, businesses and individuals. (The Canadian Press)

“(We’ll) be defending Government of Canada networks, unlike (our assistance) to the private sector where we’ll typically be providing advice and guidance,” Scott Jones, the head of CSE’s IT Security branch, told the Star.

“It’ll be an integrated defence for any Government of Canada organization.”

Currently the responsibility to protect the federal government’s networks is shared by multiple agencies. CSE already has an IT security role, in addition to its mandates to spy on foreign governments and individuals and assist domestic law enforcement.

Article Continued Below

But under the Liberals plan, CSE’s cyber security division would be transformed into the Canadian Centre for Cyber Security. The plan means an influx of cyber security staff at the spy agency, and $155.2 million over five years to get the centre up and running.

Click link above to read more

Find Out if Your Password Has Been Leaked in a Data Breach With This Chrome Extension

https://lifehacker.com/know-if-your-password-has-been-leaked-in-a-data-breach-1826373137

At this point, it seems like there’s a new data breach every week where users usernames, passwords, and other personal information has been exposed to hackers. Keeping track of them all can be quite the undertaking.

Passprotect is a Chrome extension that uses data from the site Have I Been Pwned to let you know if a password you’re using has been found in any data breaches. If it has, then it’s time to change it.

To get it, click on this link to the Google Chrome store and then click “Add to Chrome” from the top-right side of the page that pops up.

A good way to avoid this problem in the first place is to use a password manager such as 1Password to create and store secure passwords. Passwords are randomly generated and hard to crack, making them ultimately a bit safer than anything you probably can come up with on your own. 1Password already compares its passwords with the Pwned database.

Click link above to read more

Apple to close iPhone security gap police use to collect criminal evidence

https://globalnews.ca/news/4273751/apple-iphone-security-gap-police-evidence/

Apple is closing a security gap that allowed outsiders to pry personal information from locked iPhones without a password, a change that will thwart law enforcement agencies that have been exploiting the vulnerability to collect evidence in criminal investigations.

The loophole will be shut down in a forthcoming update to Apple’s iOS software, which powers iPhones.

Once fixed, iPhones will no longer be vulnerable to intrusion via the Lightning port used both to transfer data and to charge iPhones. The port will still function after the update, but will shut off data an hour after a phone is locked if the correct password isn't entered.

Click link above to read more

Bank of Chile Trading Down After Hackers Rob Millions in Cyberattack

https://money.usnews.com/investing/news/articles/2018-06-11/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack

Shares in the Bank of Chile were down on Monday after it confirmed hackers had siphoned off $10 million of its funds, mainly to Hong Kong, though the country's second-largest commercial bank said no client accounts had been impacted.

The cyber heist is the latest in a string of such attacks, including one in May in Mexico in which thieves used phantom orders and fake accounts to steal hundreds of millions of Mexican pesos out of the country's banks, including Banorte.

Shares in the Bank of Chile, which is controlled by the Chilean Luksic family and Citigroup, were down 0.47 percent at 100.4 Chilean pesos ($.16) in mid-day trading.

Click link above to read more

Study finds hundreds of stalker apps, few ways of finding them on your phone

https://globalnews.ca/news/4223784/find-stalker-apps-phone/

Hundreds of overt and covert spyware apps are available to abusive partners who want to turn a victim's Iphone or Android into a surveillance tool, a recent U.S. study found.

And malware detection programs the researchers tested are terrible at finding them, they discovered in a series of tests.

Spyware apps range from those explicitly marketed at people who want to keep track of an intimate partner (as seen below) to more innocent ones, like Find My Phone, which can be re-purposed as tracking tools.

The most intrusive "allow covert monitoring of all communications, remote activation of cameras and microphones, location tracking, and more," the study warns.

That places extreme demands on the victim's phone, which can be one way they find out they're being tracked, says Periwinkle Doerfler of New York University, one of the study's authors.

Click link above to read more

---

iPhones will share your exact location with 911

http://money.cnn.com/2018/06/18/technology/apple-911-location/index.html

Your smartphone knows your location well enough to send a car to where you're standing in a busy city, map a morning run through the woods, or navigate inside an airport.

But if you call 911 from that same mobile phone, emergency responders will only have a vague sense of where to send an ambulance, fire truck, or police car.

The difference in distances can be the difference between life and death.

Apple is rolling out a new feature in its next iPhone software update to send emergency responders instant, precise location information in the US. The update, coming in iOS 12 later this year, calculates a caller's location based on data collected from WiFi access points, nearby cellular towers, and GPS.

The tricky part isn't finding out where a caller is — Apple has been using its hybrid location technology since 2015 — but relaying that information to a fragmented and aging 911 system built for landlines.

Of the 240 million calls made to 911 each year, more than 80% are from mobile devices, according to NEMA.

Apple is working with a startup called RapidSOS, which specializes in sharing a cell phone's location information to the major programs used by the 6,300 emergency response departments across the US. RapidSOS offers its integration as a free software update to existing 911 dispatch systems.

Click link above to read more

Chinese tech firm Huawei is fighting back in Australia following reports that authorities could ban it from any involvement in building 5G mobile networks in the country.

http://money.cnn.com/2018/06/18/technology/huawei-australia-5g-china/index.html

The company, one of the world's biggest makers of smartphones and telecommunications equipment, took the unusual step of publishing an open letter to Australian lawmakers on Monday.

Recent public comments linking Huawei to security concerns "are ill informed and not based on facts," Huawei Australia's chairman and two board directors wrote in the letter.

Australian wireless carriers will soon need to hire companies to build new superfast mobile networks. But Huawei faces opposition from Australian national security agencies, according to reports last week from outlets including the Australian Financial Review and the Australian Broadcasting Corporation.

The concerns are linked to alleged ties between Huawei and the Chinese government, according to the reports.

Related: What is 5G?

In its open letter, the company insisted that it is "a private company, owned by our employees with no other shareholders."

But the company has been dogged by security concerns for years. In 2012, it was blocked from the bidding for a huge Australian national broadband network.

Huawei has also faced a lot of pressure in the United States, with lawmakers and security agencies accusing it of ties to the Chinese government. Huawei has repeatedly denied that its products pose security risks, but it has remained largely shut out of the US market.

In Australia, it has successfully bid for private contracts in the past. It's currently the country's largest supplier of wireless technology, with relationships with three of the major mobile carrier networks.

Click link above to read more

Can we trust AI if we don't know how it works?

https://www.bbc.com/news/business-44466213

We're at an unprecedented point in human history where artificially intelligent machines could soon be making decisions that affect many aspects of our lives. But what if we don't know how they reached their decisions? Would it matter?

Imagine being refused health insurance - but when you ask why, the company simply blames its risk assessment algorithm.

Or if you apply for a mortgage and are refused, but the bank can't tell you exactly why.

Or more seriously, if the police start arresting people on suspicion of planning a crime solely based on a predictive model informed by a data-crunching supercomputer.

These are some of the scenarios the tech industry is worrying about as artificial intelligence (AI) marches inexorably onwards, infiltrating more and more aspects of our lives.

AI is being experimented with in most sectors, including medical research and diagnosis, driverless vehicles, national surveillance, military targeting of opponents, and criminal sentencing.

A recent report by consultancy PwC forecasts that AI could boost the global economy by $15.7tn (£11.7tn) by 2030.

But at what cost? These software algorithms are becoming so complex even their creators don't always understand how they came up with the answers they did.

Click link above to read more

Kaspersky Lab halts European cybercrime work

https://www.bbc.com/news/technology-44501506

Computer security firm Kaspersky Lab has halted all cyber-crime collaboration with European agencies and organisations.

The decision is in protest against a European Parliament motion which called its software "malicious".

Kaspersky Lab said the accusation was "untrue" and demonstrated a "distinct lack of respect".

The row comes after the US and UK took steps to remove Kaspersky software from some government systems.

'No danger'

On 13 June, the European parliament adopted a cyber-security defence motion to combat the "unprecedented threat" the organisation faces from state-sponsored hacking.

Part of the strategy will involve a review of hardware and software used in its various institutions to find the "potentially dangerous programmes and devices".

The resolution, which has no legislative power, also calls for a ban on the programs and equipment "confirmed as malicious". It then names Kaspersky Lab and no other software firms.

Click link above to read more

Rootkit-Based Adware Wreaks Havoc Among Windows 10 Users in the US

https://www.bleepingcomputer.com/news/security/rootkit-based-adware-wreaks-havoc-among-windows-10-users-in-the-us/

When it was released back in 2015, one of the main perks of Windows 10 was the improved security features that made it harder for rootkits to get a foothold on Microsoft's new OS.

But three years later, security researchers from Romania-based antivirus vendor Bitdefender have detailed the operations of an adware strain named Zacinlo that uses a rootkit component to gain persistence across OS reinstalls, a rootkit component that's even effective against Windows 10 installations.

In fact, researchers say that 90% of all Zacinlo's recent victims are Windows 10 users, showing that crooks intentionally designed their "product" to work against Microsoft's latest OS.

Click link above to read more

Gaming Companies Remove Analytics App After Massive User Outcry

https://www.bleepingcomputer.com/news/gaming/gaming-companies-remove-analytics-app-after-massive-user-outcry/

Several gaming companies have announced plans to remove support for an analytics app they have bundled with their games.

The decision to remove the app came after several Reddit and Steam users noticed that many game publishers have recently embedded a controversial analytics SDK (software development kit) part of recent updates to their games.

Games rally against RedShell usage

The program bundled with all these games, and at the heart of all the recent controversy is RedShell, an analytics package provided by Innervate, Inc., to game publishers.

Game makers are supposed to embed this SDK within their games and run social marketing programs with specific affiliate IDs. If a new user buys and installs a game via one of these campaigns, the RedShell SDK embedded in the game pings back the publishers about the source of the new install.

But in several recent online discussions, users are complaining that besides logging the source of a new game install, the app also creates fingerprints for each gamer, with information about their online personas and gaming rigs.

Furthermore, many game studios have not told users that this SDK is now part of their games, or if they did, they made it an opt-out package instead of opt-in, as most privacy laws across the globe dictate.

Click link above to read more

Android App Devs Find Clever Trick for Fooling Users Into Installing Their Crapware

https://www.bleepingcomputer.com/news/mobile/android-app-devs-find-clever-trick-for-fooling-users-into-installing-their-crapware/

An expert in Android security is warning users that some developers of crappy Android apps have come up with a new trick for fooling users into installing their apps.

The trick relies on app devs registering Google Play Store developer accounts that mimic install counts, instead of their real name, such as "1 million installs," Installs 1,000,000," "100,000,000 Downloads," "5,000,000+," "1,000,000,000" and other similar formats.

The idea is that the official Google Play Store lists an app entry by displaying the app's icon, name, developer name, and a star rating.

Sneaky devs creating a fake sense of safety

By replacing the developer name with a faux install count, some developers are trying to fool users into thinking the app is extremely popular, and hence, somewhat safe to use.

But in reality, they are not. According to ESET malware researcher Lukas Stefanko, most of the apps using this trick that he analyzed were mostly adware. The majority were just empty shells, with little to no functionality except for showing ads on top of other apps or the user's screen.

Click link above to read more

Europol Dismantles One of the Internet's Oldest Hacker Groups

https://www.bleepingcomputer.com/news/security/europol-dismantles-one-of-the-internets-oldest-hacker-groups/

Europol, French, UK, and Thai police arrested eight people they suspect to have been involved or to have been part of a notorious hacker group known as Rex Mundi (Latin for "King of the World").

The group has been active since at least 2012. Its modus operandi revolved around hacking into companies' networks, stealing private information, and later contacting the victims to request the payment of a ransom fee.

Hackers demanded fees for not disclosing the hacks, but sometimes also asked for higher sums of money for revealing the security flaw they used to enter the victim's network.

Group left a trail of hacked firms in its wake

While the date the group formed is unknown, the earliest reports of Rex Mundi hacks go back to the summer of 2012.

In the early 2010s, when hacker groups like Anonymous or LulzSec were a bit more brash about their hacks, Rex Mundi often bragged about their recent victims, announcing hacks on Twitter, and often dumping data when companies didn't pay.

According to a trail of hacks documented on Softpedia's Security News section, past victims included —in chronological order— AmeriCash Advance, Webassur, Drake International, Buy Way, Hoststar, Websolutions.it, Numericable, Habeas, AlfaNet, Domino's Pizza, and Banque Cantonale de Geneve (BCGE).

Click link above to read more

Police Use of Minority Report-Style Pre-Crime Tech Raises Inaccuracy Concerns

https://www.bleepingcomputer.com/news/government/police-use-of-minority-report-style-pre-crime-tech-raises-inaccuracy-concerns/

Pre-crime, is a vast potpourri of information, on everyday activities, used to try to predict and prevent future behavior. In “predictive” policing, computer algorithms identify signs of pre-crime in a realm in which we are all potential suspects. Similar to the state of affairs depicted in the 2002 movie, “Minority Report,” psychic “precogs” discern which “criminals” to pursue *before* they commit a crime.

Hartford, CT is now using what some say looks an awful lot like pre-crime technology. "Like cities across the country, we've been grappling with ways to use this technology to make our residents safer and our communities stronger," Hartford Mayor Luke Bronin said in an interview with *Vice News*. "At the same time we're being very sensitive to concerns about civil liberties."

Click link above to read more

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