Security News Digest
Information Security Branch

OCIO | Office of the Chief Information Officer

January 14th, 2020

Try our January Quiz - Resolutions

Save the date - February 5th to 7th is the Privacy and Security Conference

This week's stories:

Understanding Canadian cybersecurity laws: the foundations

https://www.itworldcanada.com/blog/understanding-canadian-cybersecurity-laws-the-foundations/425979

The end of 2019 marked the end of a decade that has been shaped by rapid technological development, advancing data-use research, and an increasingly hyper-connective global infrastructure. Cyberspace is playing an undeniably fundamental role in our day-to-day lives and in business operations around the world, and yet human error still accounts for 95 per cent of all data breaches.

Click link above to read more

SPECIAL REPORT: Huawei technology reaches across Canadian, European research networks

https://www.tricitynews.com/special-report-huawei-technology-reaches-across-canadian-european-research-networks-1.24051731

Chinese telecommunications giant Huawei has a foot in the door of Canadian scientific research as well as international nuclear physics research, documents obtained under access to information show.

And, said a Calgary-based China expert, Canada's intelligence services need to more closely examine deals with the company.

Click link above to read more

Iranian hackers have been "password spraying" the US grid

https://arstechnica.com/information-technology/2020/01/iranian-hackers-have-been-password-spraying-the-us-grid/

In the wake of the US assassination of Iranian general Qassem Soleimani and the retaliatory missile strike that followed, Iran-watchers have warned that the country could deploy cyberattacks as well, perhaps even targeting US critical infrastructure like the electric grid. A new report lends some fresh details to the nature of that threat: by all appearances, Iranian hackers don't currently have the capability to start causing blackouts in the US. But they've been working to gain access to American electric utilities, long before tensions between the two countries came to a head.

Click link above to read more

Google tests biometric support for its Autofill password manager on Android

https://9to5google.com/2020/01/10/google-autofill-password-biometric-android-test/

To maintain a secure online lifestyle, it's important to use unique passwords anywhere you can. That's where a password manager comes in handy. Google's Autofill is built in to Android and its Chrome browser, and now, on the former, Google is testing biometric support.

Spotted by *XDA-Developers*, Google Autofill seems to finally be adding support for biometrics such as fingerprint and face unlock. Basically, anything that supports Google's new biometric API can be used.

Click link above to read more

Cyber Threats to North American Power Grid Are Growing

https://oilprice.com/Latest-Energy-News/World-News/Cyber-Threats-To-North-American-Power-Grid-Are-Growing.html

Threats of cyber-attacks on North America's electric network systems are growing, industrial cybersecurity firm Dragos said in a new report this week.

This year, the firm has identified two groups, Magnallium and Xenotime, which are increasingly probing to compromise electric assets in North America, expanding their targeting from the oil and gas sector to include electric assets.

Click link above to read more

Unpatched Citrix Flaw Now Has PoC Exploits

https://threatpost.com/unpatched-citrix-flaw-exploits/151748/

Over 25,000 servers globally are vulnerable to the critical Citrix remote code execution vulnerability.

Proof-of-concept (PoC) exploit code has been released for an unpatched remote-code-execution vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway products.

Click link above to read more

Burner phones are an eavesdropping risk for international travelers

https://www.helpnetsecurity.com/2020/01/07/burner-phones-eavesdropping-risk/

In recent years, burner phones have become an obligatory part of the international business traveler's toolkit. But though these devices are designed to minimize the amount of stored data available for capture by malicious actors in a foreign country, burner phones actually give attackers an opening to another, potentially more valuable, form of data: conversations that occur during key meetings in the vicinity of the device.

Click link above to read more

PCs still running Windows 7 will soon be significantly more at risk of ransomware

https://www.helpnetsecurity.com/2020/01/07/windows-7-ransomware/

PCs still running when Windows 7 reaches end of life on the 14th of January will be significantly more at risk of ransomware, Veritas Technologies has warned. According to experts, 26% of PCs are expected to still be running the Microsoft software after support for patches and bug fixes end.
The vulnerability to ransomware of PCs running unsupported software was demonstrated by WannaCry. Despite supported PCs being pushed patches for the cryptoworm, Europol estimated that 200,000 devices in 150 countries, running older, unsupported, software became infected by WannaCry.

Click link above to read more

Joker Android Malware Snowballs on Google Play

https://threatpost.com/joker-androids-malware-ramps-volume/151785/

Google has removed 17,000 Android apps to date from the Play store that have been conduits for the Joker malware (a.k.a. Bread) – and in an analysis of the code, said that Joker's operators have "at some point used just about every cloaking and obfuscation technique under the sun in an attempt to go undetected."

Click link above to read more

And now this …

Hackers Can Use Lasers to 'Speak' to Your Amazon Echo or Google Home

https://www.wired.com/story/lasers-hack-amazon-echo-google-home/

In the spring of last year, cybersecurity researcher Takeshi Sugawara walked into the lab of Kevin Fu, a professor he was visiting at the University of Michigan. He wanted to show off a strange trick he'd discovered. Sugawara pointed a high-powered laser at the microphone of his iPad—all inside of a black metal box, to avoid burning or blinding anyone—and had Fu put on a pair of earbuds to listen to the sound the iPad's mic picked up. As Sugawara varied the laser's intensity over time in the shape of a sine wave, fluctuating at about 1,000 times a second, Fu picked up a distinct high-pitched tone. The iPad's microphone had inexplicably converted the laser's light into an electrical signal, just as it would with sound…

… "It's possible to make microphones respond to light as if it were sound," says Sugawara. "This means that anything that acts on sound commands will act on light commands."

Click link above to read more

Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8

https:www.gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca