Security Digest
Information Security Branch

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

January 22nd, 2019

January is Resolutions Month

Remember January 28th is Data Privacy Day!

Watch out for the 20th Annual Privacy and Security Conference from Feb.6th to 8th.

This week's stories:

'It's gotten out of hand': Toronto area taxi fare scam has defrauded victims of millions, police say

https://www.cbc.ca/news/canada/toronto/taxi-fare-scam-debit-1.4981593

Toronto police issued a warning on Thursday about an ongoing taxi fare scam that has already led to the arrests of five people who now face more than 260 charges for identity theft.

According to investigators, some taxi drivers are using customized point-of-sale machines — often called debit machines — to steal key financial information from customers. Police stressed that cab companies are "not directly involved" in the alleged scam and have co-operated with the investigation.

Click link above to read more

China threatens reprisals if Canada bans Huawei from its 5G networks

https://www.theglobeandmail.com/politics/article-china-threatens-reprisals-if-canada-bans-huawei-from-its-5g-networks/

China will retaliate if Ottawa bans Huawei Technologies from supplying gear for its next-generation 5G mobile networks over espionage concerns, the country's envoy said on Thursday, as he called the arrest of a company executive a "backstabbing" betrayal of Canada's relationship with China.

The United States is pressing its allies, including Canada, to ban the giant Chinese smartphone and telecommunications equipment maker from the infrastructure of future wireless networks – the Trudeau cabinet is awaiting the conclusion of a national security review before deciding.

Click link above to read more

Was The Facebook '10 Year Challenge' A Way To Mine Data For Facial Recognition AI?

https://www.forbes.com/sites/nicolemartin1/2019/01/17/was-the-facebook-10-year-challenge-a-way-to-mine-data-for-facial-recognition-ai/

Last week a new Facebook challenge went viral asking users to post a photo from 10 years ago and one from today captioning "how did aging effect you?" Now being called the "10-Year Challenge." Over 5.2 million, including many celebrities, participating in this challenge. It follows closely after the "Bird Box Challenge" and the "Top Nine Photos of the Year Challenge" but this one has caused quite a stir and some concern from users.

Speculation arose about the motive behind this viral challenge and had users questioning if this was a ploy by Facebook to use for facial recognition data. Kate O'Neill, a writer for Wired, wrote an op-ed exploring the possibility that this was more than just a fun challenge to share with friends.

"Imagine that you wanted to train a facial recognition algorithm on age-related characteristics and, more specifically, on age progression (e.g., how people are likely to look as they get older). Ideally, you'd want a broad and rigorous dataset with lots of people's pictures. It would help if you knew they were taken a fixed number of years apart—say, 10 years," said O'Neill.

Click link above to read more

MS Word Documents Spreading .Net RAT Malware

https://www.infosecurity-magazine.com/news/ms-word-documents-spreading-net/

A malicious MS Word document, titled "eml_-_PO20180921.doc," has been found in the wild, and according to researchers at Fortinet's FortiGuard Labs, the document contains auto-executable malicious VBA code.

Victims who receive and open the document are prompted with a security warning that macros have been disable. If the user then clicks on "enable content," the NanoCore remote access Trojan (RAT) software is installed on the victim's Windows system.

According to FortiGuard Labs, the NanoCore RAT was developed in the .Net framework back in 2013. Despite its continued use, the author was convicted by the FBI and sentenced to nearly three years in prison. Researchers captured a sample of this latest version (1.2.2.0), which uses NanoCore to execute malicious behavior.

Click link above to read more

Malware can now evade cloud security tools, as cybercriminals target public cloud users

https://www.techrepublic.com/article/malware-can-now-evade-cloud-security-tools-as-cybercriminals-target-public-cloud-users/

Malware samples associated with Chinese threat actor Rocke Group are now capable of uninstalling cloud security products, according to an analysis by researchers at Palo Alto Networks Unit 42, in a report published Thursday.

The newly-discovered malware samples are not exploiting a specific vulnerability of cloud security products; rather, the malware is engineered to gain administrator access on a given cloud instance and uninstall the software as any administrator would be capable of doing.

Click link above to read more

Facebook shuts hundreds of Russia-linked pages, accounts

https://www.ctvnews.ca/sci-tech/facebook-shuts-hundreds-of-russia-linked-pages-accounts-1.4257220

Facebook said Thursday it removed hundreds of Russia-linked pages, groups and accounts that it says were part of two big disinformation operations targeting users outside the U.S.

The social media company said its latest effort to fight misinformation came after it found two networks "that engaged in co-ordinated inauthentic behaviour" on Facebook and its Instagram service.

Click link above to read more

How the government shutdown is putting national cybersecurity at risk

https://www.cnbc.com/2019/01/14/government-shutdown-putting-national-cybersecurity-at-risk.html

The partial government shutdown is quickly turning into a nightmare scenario for the country's cybersecurity functions, often in unexpected ways. Even after Congress ultimately reaches a deal to end the shutdown, these negative effects could last far into the future.

Close to half of the employees within the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, or CISA — which works to help secure the nation's critical infrastructure industries, such as banking, water, energy and nuclear — are furloughed. Eighty-five percent of the National Institute of Standards and Technology workers have been furloughed as well, and these are the employees who help private- and public-sector companies stay up to date on the latest cyberattacks and mitigation techniques.

Click link above to read more

One month after controversial adult-content purge, far-right pages are thriving on Tumblr

https://thinkprogress.org/far-right-content-survived-tumblr-purge-36635e6aba4b/

The move was greeted with outrage, particularly from those who had used the site as a way to discover their own gender identity and sexuality and connect with users from similarly marginalized groups. Critics accused the site of attempting to please larger tech corporations, like Google and Verizon (which owns Tumblr), at the expense of these groups. Tumblr CEO Jeff D'Onofrio, however, maintained that the changes were made to foster a more "inclusive" community.

One group Tumblr apparently has no problem continuing to host, however, is far-right extremists, who seemingly survived much of last month's purge unscathed.

The website is currently littered with pages promoting Nazism, white supremacy, ethno-nationalism, and far-right terrorism. Despite their often flagrant violation of Tumblr's Community Guidelines, these pages remain largely active and easy to find.

Click link above to read more

Twitter bug revealed private tweets for some Android users for almost five years

https://www.zdnet.com/article/twitter-bug-revealed-private-tweets-for-some-android-users-for-almost-five-years/

Social media network Twitter revealed today that it fixed a bug that affected users of its Android app. The bug accidentally changed the visibility of protected tweets from private to public, the company said.

The social network didn't reveal how it found the bug, but said that it already notified all users who it believes were impacted, and also reset the "Protect your Tweets" option to its original setting, hiding those people's tweets from non-followers, non-registered users, and search engines.

Click link above to read more

UK Sentences Man for Mirai DDoS Attacks Against Liberia

https://www.inforisktoday.com/uk-sentences-man-for-mirai-ddos-attacks-against-liberia-a-11933

In 2016, the small West African country of Liberia became a target for the Mirai botnet, leading to widespread disruptions and demonstrating just how devastating distributed denial-of-service attacks can be, especially when they get executed using tens of thousands of hijacked, internet-connected devices.

On Friday, the perpetrator of the Lonestar attacks, 30-year-old Daniel Kaye of Egham, England, was sentenced in Blackfriars Crown Court to serve a sentence of two years and eight months, according to the U.K.'s National Crime Agency.

Click link above to read more

Why Do Phishing Attacks Continue to Plague Healthcare?

https://www.inforisktoday.com/do-phishing-attacks-continue-to-plague-healthcare-a-11953\

Several health data breaches involving phishing attacks - including one that potentially exposed data on more than 100,000 individuals - have been added to the federal health data breach tally this month.

In addition, of the breaches added to the tally during 2018, about 60 percent involved email. With so much media attention on phishing attacks, why do so many healthcare entities still fall victim to these assaults?

"Phishing attacks will definitely continue to increase because they work," says Rebecca Herold, president of Simbus, a privacy and cloud security services firm, and CEO of The Privacy Professor consultancy. "Cybercrooks will always use what gives them the data they want to steal and the disruption they seek to cause."

Click link above to read more