Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

April 28, 2020

Try our April Quiz – Working Remotely

Save the Date for Security Day - http://www.gov.bc.ca/securityday

Cyber Safety for Mobile Workers Information Sheet

This week's stories:

- **Toronto mayor retracts claims city is collecting cellphone location data in COVID-19 fight**
- **Facebook asks judge to toss Canadian privacy chief's findings on personal data probe**
- **Chinese 'Frontline' COVID-19 Research Firm Reported Hacked: Data Now on Dark Web**
- **Single Malicious GIF Opened Microsoft Teams to Nasty Attack**
- **Kaspersky report: Nearly half of employees don't know how to respond to ransomware attacks**
- **Payouts Generated from Sextortion Scams End up in Another Round of Frauds, New Study Reveals**
- **Twitter kills SMS-based tweeting in most countries**
- **Israel government tells water treatment companies to change passwords**
- **Fake Fedex and UPS delivery issues used in COVID-19 phishing**
- **Microsoft investigating Windows 10 KB4549951 BSOD reports**

Toronto mayor retracts claims city is collecting cellphone location data in COVID-19 fight

https://business.financialpost.com/technology/toronto-mayor-retracts-claims-city-is-collecting-cellphone-location-data-in-covid-19-fight

Toronto Mayor John Tory has walked back public claims he made Monday that the city was gathering cellphone data from telecommunications companies to spot places where residents continue to gather despite social-distancing measures to slow the spread of COVID-19.

As first reported by *The Logic*, Tory told thousands of attendees of an online event hosted by TechTO that the city had "cellphone companies give us all the data on the pinging off their network on the weekend so we could see, 'Where were people still congregating?'" He called such gatherings "the biggest enemy of fighting" COVID-19.

Click link above to read more

Facebook asks judge to toss Canadian privacy chief's findings on personal data probe

https://globalnews.ca/news/6844272/facebook-canada-personal-data/

Facebook wants a judge to toss out the federal privacy watchdog's finding that the social media giant's lax practices allowed personal data to be used for political purposes.

Privacy commissioner Daniel Therrien's probe "was neither impartial nor independent, and lacked procedural fairness," Facebook alleges in a submission to the Federal Court of Canada.

Click link above to read more

Chinese 'Frontline' COVID-19 Research Firm Reported Hacked: Data Now on Dark Web

https://www.forbes.com/sites/zakdoffman/2020/04/26/chinese-covid-19-detection-firm-just-got-hacked-data-for-sale-on-dark-web-new-report/#27d594125dec

It's a controversial subject—the use of CT scans to diagnose coronavirus—but it's an emerging field. And while the likes of the U.S. Centers for Disease Control and Prevention and the American College of Radiology have cautioned against it, one Chinese medical company has harnessed Intel's technology and Huawei's marketing channels to push its solutions into frontline hospitals.

Click link above to read more

Single Malicious GIF Opened Microsoft Teams to Nasty Attack

https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

Microsoft has fixed a subdomain takeover vulnerability in its collaboration platform Microsoft Teams that could have allowed an inside attacker to weaponize a single GIF image and use it to pilfer data from targeted systems and take over all of an organization's Teams accounts.

The attack simply involved tricking a victim into viewing a malicious GIF image for it to work, according to researchers at CyberArk who also created a proof-of-concept (PoC) of the attack.

Click link above to read more

Kaspersky report: Nearly half of employees don't know how to respond to ransomware attacks

https://www.itworldcanada.com/article/kaspersky-report-nearly-half-of-employees-dont-know-how-to-respond-to-ransomware-attacks/429811

Despite the threat of ransomware being at an all-time high, a recent report from cybersecurity firm Kaspersky says that 45 per cent of employees in the U.S and Canada wouldn't know how to respond to a ransomware attack. Thirty-seven per cent don't even know what it is.

Ransomware, characterized by attackers blocking access to critical data or services (usually through strong encryption) and demanding the victim to pay a ransom to regain access, can have devastating consequences. The report from Kaspersky estimated that ransomware could cost organizations $1 million on average, and in severe cases, more than $5 million.

Click link above to read more

Payouts Generated from Sextortion Scams End up in Another Round of Frauds, New Study Reveals

https://cyware.com/news/payouts-generated-from-sextortion-scams-end-up-in-another-round-of-frauds-new-study-reveals-7166aa57

- Millions of sextortion spam messages, sent between September 2019 and January 2020, had generated nearly $500,000 in profit for online scammers.
- However, the extorted funds were used to support illicit activities such as transacting on dark web marketplaces, gambling, and buying stolen credit card data.

A new study by researchers from Sophos has revealed that millions of sextortion spam messages, sent between September 1, 2019, and January 31, 2020, had generated nearly a half-million US dollars in profit for online scammers. This particular type of fraud attempts to capitalize on the behavior of people watching adult content.

Click link above to read more

Twitter kills SMS-based tweeting in most countries

https://www.bleepingcomputer.com/news/security/twitter-kills-sms-based-tweeting-in-most-countries/

Twitter announced today that it has turned off the Twitter via SMS service because of security concerns, a service which allowed the social network's users to tweet using text messages since its early beginnings.

"We want to continue to help keep your account safe," the company's support account tweeted earlier today.

"We've seen vulnerabilities with SMS, so we've turned off our Twitter via SMS service, except for a few countries."

Click link above to read more

Israel government tells water treatment companies to change passwords

https://www.zdnet.com/article/israel-says-hackers-are-targeting-its-water-supply-and-treatment-utilities/?&web_view=true

The Israeli government says that hackers have targeted its water supply and treatment facilities last week.

In a security alert sent by the Israeli National Cyber-Directorate (INCD), the agency is urging personnel at companies active in the energy and water sectors to change passwords for all internet-connected systems.

Click link above to read more

Fake Fedex and UPS delivery issues used in COVID-19 phishing

https://www.bleepingcomputer.com/news/security/fake-fedex-and-ups-delivery-issues-used-in-covid-19-phishing/

As people socially isolate and work from home, shopping online and home deliveries have increased.

Scammers are capitalizing on this by creating new scams using Coronavirus delivery issues as a lure to get people to visit malicious links or open malware.

In a new report by Kaspersky, researchers see a new wave of phishing scams that utilize a COVID-19 theme and impersonate well-known shipping carriers such as FedEx, UPS, and DHL.

Click link above to read more

Microsoft investigating Windows 10 KB4549951 BSOD reports

https://www.bleepingcomputer.com/news/microsoft/microsoft-investigating-windows-10-kb4549951-bsod-reports/

Microsoft is investigating Bluetooth issues, failures to install, and blue screen reports received from users who have installed or attempted to install the KB4549951 cumulative update released during this month's Patch Tuesday.

KB4549951 provides customers with security fixes for devices running Windows 10, version 1909, and Windows 10, version 1903, and it can be installed automatically by checking for updates via Windows Update or manually from the Microsoft Update Catalog.

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

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


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer