Security Digest
Information Security Branch

BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer

March 26th, 2019

March is Fraud Awareness Month

This week's stories:

- **Malware attacks in Canada up 103 per cent over 2018, says SonicWall**
- **Healthcare organizations and DNS as a layer of defence and intelligence**
- **B.C. judge orders RCMP to give Meng data on devices seized during arrest**
- **Facebook left millions of passwords readable by employees**
- **Tesla Model 3 Hacked on the Last Day of Pwn2Own**
- **70% of Ransomware Attacks Targeted SMBs, BEC Attacks Increased by 130%**
- **The National Board of Examiners in Optometry to Pay $3.25M Settlement in Data Breach Case**
- **Aluminium plants hit by cyber-attack, global company turns to manual operations**
- **Google Play is flooded with hundreds of unsafe anti-virus products**
- **Popular family tracking app exposed real-time location data onto the internet – no password required**

Malware attacks in Canada up 103 per cent over 2018, says SonicWall

https://www.itworldcanada.com/article/malware-attacks-in-canada-up-103-per-cent-over-2018-says-sonicwall/416322

Canada faced the second biggest increase in malware attacks last year among customers of corporate security vendor SonicWall.

Malware attacks detected here by those using SonicWall firewalls and other security devices hit 432.2 million, up 103 per cent over 2017, according to a report released Tuesday by the company in its annual cyber threat report.

By comparison, attacks against Brazil were up 119 per cent over the previous year, up 99 per cent in Germany, up 62 per cent in the U.S., 57 per cent in the U.K., and 53 per cent in India.

Click link above to read more

Healthcare organizations and DNS as a layer of defence and intelligence

https://www.itworldcanada.com/article/healthcare-organizations-and-dns-as-a-layer-of-defence-and-intelligence/416205

Mark Gaudet from the Canadian Internet Registration Authority (CIRA) bears some grim news about Canadian healthcare organizations today. The move to electronic data records has made healthcare organizations a real target of cyber criminals, he said in a recent webinar ***Preparing for the Big Hack in Healthcare***.

“Healthcare data in the form of patient records and information about doctors provides cyber-criminals with all the information they need to do identity theft, to commit fraud, and to cross-reference personal information to implement other kinds of cyber crime.”

Click link above to read more

B.C. judge orders RCMP to give Meng data on devices seized during arrest

https://www.canadiansecuritymag.com/news/industry-news/bc-judge-orders-rcmp-to-give-meng-data-on-devices-seized-during-arrest

A judge has ordered the RCMP to provide copies of the content on seven electronic devices to an executive of Chinese tech giant Huawei Technologies after they were seized at Vancouver's airport during her arrest.

Justice Heather Holmes of the British Columbia Supreme Court said in an order issued after a brief hearing Friday that the RCMP must make copies for Meng Wanzhou of data on an iPhone, an iPad, a Macbook Air, a Huawei phone, two SIM cards and a flash drive.

Holmes said a representative of the Mounties must forward the electronics to an examiner of the force's technical crime unit within three days so content can be extracted onto devices provided by Meng.

Click link above to read more.

Facebook left millions of passwords readable by employees

https://www.canadiansecuritymag.com/news/data-security/facebook-left-millions-of-passwords-readable-by-employees

Facebook left hundreds of millions of user passwords readable by its employees for years, the company acknowledged Thursday after a security researcher exposed the lapse.

By storing passwords in readable plain text, Facebook violated fundamental computer-security practices. Those call for organizations and websites to save passwords in a scrambled form that makes it almost impossible to recover the original text.

"There is no valid reason why anyone in an organization, especially the size of Facebook, needs to have access to users' passwords in plain text," said cybersecurity expert Andrei Barysevich of Recorded Future.

Click link above to read more

Tesla Model 3 Hacked on the Last Day of Pwn2Own

https://www.bleepingcomputer.com/news/security/tesla-model-3-hacked-on-the-last-day-of-pwn2own/

Fluoroacetate is the team which won the competition earning $375,000 out of the total of $545,000 earned by security researchers who demoed their research during this year's Pwn2Own Vancouver 2019.

During the last day, Fluoroacetate's Amat Cama and Richard Zhu successfully targeted and successfully hacked their way into a Tesla Model 3's Chromium-based infotainment system as part of their automotive category demo, using "a JIT bug in the renderer to display their message."

Click link above to read more

70% of Ransomware Attacks Targeted SMBs, BEC Attacks Increased by 130%

https://www.bleepingcomputer.com/news/security/70-percent-of-ransomware-attacks-targeted-smbs-bec-attacks-increased-by-130-percent/

Beazley Breach Response (BBR) Services found that 71% of ransomware attacks targeted small businesses, with an average ransom demand of $116,324 and a median of $10,310, after analyzing 3,300 incidents involving its clients in 2018.

As further detailed by Beazley's 2019 Breach Briefing report, the highest ransom demanded from its insureds was of $8.5 million or 3,000 Bitcoin, while the highest ransom paid by one of its clients was of $935,000.

Click link above to read more

The National Board of Examiners in Optometry to Pay $3.25M Settlement in Data Breach Case

https://www.databreaches.net/the-national-board-of-examiners-in-optometry-to-pay-3-25m-settlement-in-data-breach-case/

There's a significant update to some data breach litigation that was revived last June. The American Optometric Association reports:

The National Board of Examiners in Optometry (NBEO) will allot $3.25 million in a cash settlement fund to compensate some 61,000 victims of an alleged data breach that gripped the profession in 2016.

Click link above to read more

Aluminium plants hit by cyber-attack, global company turns to manual operations

https://hotforsecurity.bitdefender.com/blog/aluminium-plants-hit-by-cyber-attack-global-company-turns-to-manual-operations-20982.html

Norsk Hydro, one of the world's largest producers of aluminium, says that it is battling an "extensive cyber-attack" that first hit its systems on Monday evening and then escalated overnight.

Norsk Hydro, often just referred to as Hydro, operates in some 50 countries worldwide, and is a major producer of hydroelectric power in Norway.

Click link above to read more

Google Play is flooded with hundreds of unsafe anti-virus products

https://hotforsecurity.bitdefender.com/blog/google-play-is-flooded-with-hundreds-of-unsafe-anti-virus-products-20976.html

A new study conducted by AV-Comparatives, a well-respected independent testing agency, has closely examined whether 250 security products for Android smartphones are capable of protecting users at all.

The test evaluated whether Android anti-virus products available in the official Google Play store can protect against the 2000 most common Android malware threats of 2018.

Compared to the total Android malware in existence, 2000 is a small number – but the fact that these samples were considered the most commonly encountered means that no anti-virus product worth its salt should be failing to detect them all.

Click link above to read more

Popular family tracking app exposed real-time location data onto the internet – no password required

https://hotforsecurity.bitdefender.com/blog/popular-family-tracking-app-exposed-real-time-location-data-onto-the-internet-no-password-required-21003.html

More than 238,000 individuals users have had their family's real-time location exposed for weeks on end after an app developer left sensitive data exposed on the internet, without a password.

Many users of "Family Locator", an iOS app developed by React Apps, is promoted as a tool for helping users stay informed about the location of their loved ones. For a one-off payment, the app's Australian developers offer to let you follow up to 10 family members or friends, getting "instant alerts when your loved one enters or exits a location" and providing a "detailed location history up to last three days."

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