Security Digest
Information Security Branch

British Columbia

OCIO
Office of the Chief Information Officer

January 15th, 2019

January is Resolutions Month

This week's stories:

- Canadian Cyber Threat Exchange now actively recruiting SMBs 🇨🇦
- Nova Scotia privacy commissioner blames government department for data breaches 🇨🇦
- Top Huawei executive arrested in Poland for espionage
- Fake Movie File Infects PC to Steal Cryptocurrency, Poison Google Results
- Del Rio City Hall Forced to Use Paper After Ransomware Attack
- U.S. Government Shutdown Leaves Its Sites with Expired TLS Certificates
- US Carriers Promise Again to Stop Selling Customer Location Data
- Cybercrime Gangs Advertise Fresh Jobs, Hacking Services
- BEC Scam Leads to Theft of $18.6 Million
- Old tweets reveal hidden secrets

Canadian Cyber Threat Exchange now actively recruiting SMBs 🇨🇦

https://www.itworldcanada.com/article/canadian-cyber-threat-exchange-now-actively-recruiting-smbs/414102

After broadening and lowering its pricing, the Canadian Cyber Threat Exchange is now actively urging small and mid-sized business to join to help improve their awareness of and response to online threats.

Officially the new pricing categories, which start at $500 a year for organizations with up to 99 employees, started at the beginning of the year. Until then a small firm had to pay $5,000 a year, while mid-sized firms paid $20,000 a year.

Click link above to read more

Nova Scotia privacy commissioner blames government department for data breaches 🇨🇦

https://www.itworldcanada.com/article/nova-scotia-privacy-commissioner-blames-government-department-for-data-breaches/414154

A "serious lack of security testing" of Nova Scotia's new freedom of information website was one of the main factors that allowed two people to hack the site 2018 and make off with 7,000 documents including personal information of 740 people, says the province's privacy commissioner.

Click link above to read more

Top Huawei executive arrested in Poland for espionage

https://www.itworldcanada.com/article/top-huawei-executive-arrested-in-poland-for-espionage/414045

The Wall Street Journal reports that a Huawei executive has been arrested in Poland after being discovered as a spy for the Chinese government.

The person arrested is a former Huawei sales director in Poland and has worked with government customers. He allegedly conducted high-level espionage on behalf of China.

Click link above to read more

Fake Movie File Infects PC to Steal Cryptocurrency, Poison Google Results

https://www.bleepingcomputer.com/news/security/fake-movie-file-infects-pc-to-steal-cryptocurrency-poison-google-results/

A malicious Windows shortcut file posing as a movie via The Pirate Bay torrent tracker can trigger a chain of mischievous activities on your computer, like injecting content from the attacker into high-profile web sites such as Wikipedia, Google and Yandex Search or by stealing cryptocurrency.

Malware on TPB is not a new thing, but the method used to infect a victim's computer and the large amount of varied malicious activities discovered by BleepingComputer are quite interesting.

Click link above to read more

Del Rio City Hall Forced to Use Paper After Ransomware Attack

https://www.bleepingcomputer.com/news/security/del-rio-city-hall-forced-to-use-paper-after-ransomware-attack/

The City Hall of Del Rio, Texas was hit by a ransomware attack on Thursday, which led to multiple computers on the network being turned off and disconnected from the Internet to contain and analyze the malware.

Victoria Vargas Public Relations Manager for Del Rio's City Hall told BleepingComputer that around 30 to 45 computers were turned off after detecting the attack during the morning of January 10 and that the ransom note contained a phone number to be used to contact the attackers for instructions on how to pay the ransom.

Click link above to read more

U.S. Government Shutdown Leaves Its Sites with Expired TLS Certificates

https://www.bleepingcomputer.com/news/security/us-government-shutdown-leaves-its-sites-with-expired-tls-certificates/

Following a partial U.S. government shutdown caused by a deadlock on the issue of the Mexican border wall between the Democratic Party and Donald Trump, tens of government websites can no longer be accessed or have been marked as using insecure connections because their TLS certificates have not been renewed.

The websites of the U.S. Department of Justice, NASA, and the Court of Appeals are some of the ones hit by the government's failure to extend around 80 TLS certificates used on .gov domains.

Click link above to read more

US Carriers Promise Again to Stop Selling Customer Location Data

https://www.bleepingcomputer.com/news/security/us-carriers-promise-again-to-stop-selling-customer-location-data/

Everyone knows that major mobile service providers such as AT&T, T-Mobile, and Sprint are actively collecting their customers' location data, but not many know that they're also selling it to the highest bidder.

As discovered by Motherboard's Joseph Cox, you can locate anyone as long as you know their phone number and, of course, if you are willing to pay for it.

Click link above to read more

Cybercrime Gangs Advertise Fresh Jobs, Hacking Services

https://www.databreachtoday.com/cybercrime-gangs-advertise-fresh-jobs-hacking-services-a-11934

Calling all hackers for hire: Do you have what it takes to send "violent and graphic" emails and text messages to schoolchildren's parents, blackmail healthcare organizations, manufacturers, technology companies and law firms, or leak unaired episodes of "Orange is the New Black," preferably while also being fluent in Arabic, Chinese or German?

Click link above to read more

BEC Scam Leads to Theft of $18.6 Million

https://www.databreachtoday.com/bec-scam-leads-to-theft-186-million-a-11930

In a case of business email compromise, Chinese hackers stole $18.6 million from the Indian arm of Tecnimont SpA, an Italian engineering company, through an elaborate cyber fraud scheme that included impersonating the firm's chief executive, the Economic Times reports.

The scammers sent emails requesting funds to the India head of Tecnimont, part of the publicly traded Maire Tecnimont, from an account that looked deceptively similar to one used by the Italian group's CEO, and also organized conference calls to discuss a "confidential" acquisition in China, the ET report said. The company has filed a complaint with Indian police.

Click link above to read more

Old tweets reveal hidden secrets

https://nakedsecurity.sophos.com/2019/01/11/old-twitter-posts-reveal-hidden-secrets-say-researchers/

Old Twitter posts could reveal more about you than you think, according to a research paper released this month. Tweets could reveal places you visited and things you did, even if you didn't explicitly mention them.

Researchers from the Foundation for Research and Technology in Greece and the University of Illinois found all this out after writing a tool called LPAuditor. The software mines publicly available tweet data that anyone can download from Twitter via its application programming interface (API).

Using the tool, they analyzed the metadata – hidden information about a tweet embedded in the post – to identify users' homes, workplaces and sensitive places that they visited. In dozens of cases, they were also able to identify the users behind anonymous Twitter accounts.

Click link above to read more

Click Unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Information Security Branch
www.gov.bc.ca/informationsecurity

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer