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

January 12th, 2021

Try our January “Resolutions” Quiz

This week’s stories:

- 🇨🇦 NDP call on privacy commissioner to investigate potential security breach of Sask. hunters' info
- 🇨🇦 Stolen Sask. health care data could fetch big money on dark web, expert says
- 🇨🇦 Cyberattack on Saint John could push up city's insurance costs even more
- The attack on the Capitol may pose a cybersecurity risk. Here’s how
- Exclusive: FBI probes Russian-linked postcard sent to FireEye CEO after cybersecurity firm uncovered hack - sources
- New Attack Could Let Hackers Clone Your Google Titan 2FA Security Keys
- The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group
- DarkSide ransomware decryptor recovers victims' files for free
- Cybersecurity: This 'costly and destructive' malware is the biggest threat to your network

🇨🇦 NDP call on privacy commissioner to investigate potential security breach of Sask. hunters' info)

https://regina.ctvnews.ca/ndp-call-on-privacy-commissioner-to-investigate-potential-security-breach-of-sask-hunters-info-1.5262433

REGINA -- The provincial Opposition is calling on the Information and Privacy Commissioner to investigate a possible security breach in the Hunting, Angling and Trapping License (HAL) System.

The NDP said some hunters have received emails with other individuals’ names and account numbers.

The online registration system is operated on the provincial government’s behalf by an American company.

Click link above to read more

🇨🇦 Stolen Sask. health care data could fetch big money on dark web, expert says

https://globalnews.ca/news/7566304/stolen-sask-health-care-data-could-fetch-big-money-on-dark-web-expert-says/

While the ransom demanded by the software used in a 2020 cyberattack wasn’t paid, an IT expert says Saskatchewan residents aren’t out of the woods.

A report recently released by Saskatchewan’s Information and Privacy Commissioner (IPC) notes that roughly 547,000 of the files stolen by ransomware from provincial health care servers last January likely contained personal information.

Click link above to read more

🇨🇦 Cyberattack on Saint John could push up city's insurance costs even more

https://www.cbc.ca/news/canada/new-brunswick/saint-john-cyber-attack-1.5868015

The City of Saint John's insurance costs are rising 26 per cent this year, a number that could change when the city gets a final quote on renewing its cyber liability policy.

"The insurance industry is in a hard market not seen in 20 years," Ian Fogan, director of strategic affairs, wrote in a report prepared for the city council meeting Monday night.

Click link above to read more

The attack on the Capitol may pose a cybersecurity risk. Here’s how

https://www.latimes.com/business/technology/story/2021-01-07/dc-riots-capitol-cybersecurity-infosec

The pro-Trump mob that stormed the U.S. Capitol’s Senate floor and Capitol rotunda on Wednesday may have breached more than just the building’s physical security.

Photos show rioters in congressional offices, including that of House Speaker Nancy Pelosi (D-San Francisco). Any computers left on could be vulnerable, and so could papers — such as personal schedules or mail — that weren’t locked away, information security experts said. Sen. Jeff Merkley (D-Ore.) said his office was ransacked and a laptop stolen. An aide to Pelosi said a laptop used only for presentations was snatched from a conference room.

Click link above to read more

Exclusive: FBI probes Russian-linked postcard sent to FireEye CEO after cybersecurity firm uncovered hack - sources

https://www.msn.com/en-us/news/us/exclusive-fbi-probes-russian-linked-postcard-sent-to-fireeye-ceo-after-cybersecurity-firm-uncovered-hack-sources/ar-BB1cFb9n

(Reuters) - The FBI is investigating a mysterious postcard sent to the home of cybersecurity firm FireEye's chief executive days after it found initial evidence of a suspected Russian hacking operation on dozens of U.S. government agencies and private American companies.

U.S. officials familiar with the postcard are investigating whether it was sent by people associated with a Russian intelligence service due its timing and content, which suggests internal knowledge of last year's hack well before it was publicly disclosed in December.

Click link above to read more

New Attack Could Let Hackers Clone Your Google Titan 2FA Security Keys

https://thehackernews.com/2021/01/new-attack-could-let-hackers-clone-your.html

Hardware security keys—such as those from Google and Yubico—are considered the most secure means to protect accounts from phishing and takeover attacks.

But a new research published on Thursday demonstrates how an adversary in possession of such a two-factor authentication (2FA) device can clone it by exploiting an electromagnetic side-channel in the chip embedded in it.

Click link above to read more

The SolarWinds Hackers Shared Tricks With a Notorious Russian Spy Group

https://www.wired.com/story/solarwinds-russia-hackers-turla-malware/

EVER SINCE THE December revelation that hackers breached the IT-management software firm SolarWinds, along with an untold number of its customers, Russia has been the prime suspect. But even as US officials have pinned the attack on the Kremlin with varying degrees of certainty, no technical evidence has been published to support those findings. Now

Russian cybersecurity firm Kaspersky has revealed the first verifiable clues— three of them, in fact—that appear to link the SolarWinds hackers and a known Russian cyberespionage group.

Click link above to read more

DarkSide ransomware decryptor recovers victims' files for free

https://www.bleepingcomputer.com/news/security/darkside-ransomware-decryptor-recovers-victims-files-for-free/

Romanian cybersecurity firm Bitdefender has released a free decryptor for the DarkSide ransomware to allow victims to recover their files without paying a ransom.

DarkSide is a human-operated ransomware that has already earned millions in payouts since it started targeting enterprises in August 2020.

The operation has seen a spike in activity between October and December 2020 when the amount of DarkSide sample submissions on the ID-Ransomware platform more than quadrupled.

Click link above to read more

Cybersecurity: This 'costly and destructive' malware is the biggest threat to your network

https://www.zdnet.com/article/cybersecurity-this-costly-and-destructive-malware-is-the-most-prolific-threat-to-your-network/

A spam campaign that targeted over 100,000 users a day over Christmas and New Year has seen Emotet secure its spot as the most prolific malware threat.

Analysis by cybersecurity company Check Point suggests that Emotet was used to target 7% of organisations around the world during December.

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:

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.

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