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

December 8th, 2020

Try our December - “Shopping Online” Quiz

This week’s stories:

- 🇨🇦 Canadian intelligence: 3 countries spread virus lies
- 🇨🇦 Ransomware attack led to 3 days of transit payment problems, TransLink says
- 🇨🇦 Cybersecurity strategies shift as Canadian businesses invest in digitization during COVID-19 pandemic
- 🇨🇦 Canadian cybersecurity leaders say ecosystem requires community to grow
- 🇨🇦 Ransomware update: Documents from Calgary energy firm released
- Darknet Drug Dealers Are Now Selling ‘Pfizer COVID Vaccines’ - Vice
- FBI Warning: ‘Tis the Season for Holiday Scams
- Phishing Campaign Targeted Universities Worldwide
- Cybersecurity in the Biden Administration, Experts Weigh in
- Research: Millions of smart devices vulnerable to hacking
- Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says
- SANS cybersecurity training firm suffers data breach due to phishing attack

🇨🇦 Canadian intelligence: 3 countries spread virus lies

https://www.aa.com.tr/en/americas/canadian-intelligence-3-countries-spread-virus-lies/2064934

TRENTON, Canada

Russia, China and Iran are behind dangerous misinformation campaigns about coronavirus, the intelligence agency responsible for keeping Canadians safe said in a report made public Thursday.

As well, Russia and China spies have traded “trench coats” for “lab coats” as they attempt to infiltrate Canadian research companies to steal secrets on virus vaccine developments, the Canadian Security Intelligence Service (CSIS) reported in late November.

The trio of countries have different motives for conducting social media COVID-19 misinformation campaigns, according to the report entitled, COVID-19: Global Effects and Canadian National Security Interests.

Click link above to read more

Ransomware attack led to 3 days of transit payment problems, TransLink says

https://www.cbc.ca/news/canada/british-columbia/translink-debit-credit-payment-down-1.5826868

TransLink says customers can return to using credit cards and debit cards at ticket vending machines and fare gates after three days of being unable to do so because of a ransomware attack on the Metro Vancouver transit authority.

CEO of Translink Kevin Desmond issued a statement Thursday afternoon to apologize for the inconvenience and provide more information about the mysterious cyberattack.

"We are now in a position to confirm that TransLink was the target of a ransomware attack on some of our IT infrastructure. This attack included communications to TransLink through a printed message," said Desmond.

Click link above to read more

Cybersecurity strategies shift as Canadian businesses invest in digitization during COVID-19 pandemic

https://markets.businessinsider.com/news/stocks/cybersecurity-strategies-shift-as-canadian-businesses-invest-in-digitization-during-covid-19-pandemic-1029864668

TORONTO, Dec. 4, 2020 /CNW/ - Most (97%) Canadian businesses (96% globally) say their cybersecurity strategies will shift as a result of the increased digitization during COVID-19 pandemic according to PwC Canada's Digital Trust Insights report. PwC surveyed more than 3,000 business and technology executives around the world, including a significant number of Canadian respondents, who tell us what's changing and what's next in cybersecurity, privacy and resilience.

Click link above to read more

Canadian cybersecurity leaders say ecosystem requires community to grow

https://betakit.com/canadian-cybersecurity-leaders-say-ecosystem-requires-community-to-grow/

As the COVID-19 pandemic continues, conversations tend to focus on job losses and skyrocketing unemployment. While it’s true that, at the start of the pandemic, Canada reached levels of unemployment not seen for decades, some industries are in desperate need of talent.

Cybersecurity is one of those industries, with an estimated 3.5 million job openings to fill globally by 2021. The problem for Canada is that only a small handful of the world’s top cybersecurity firms are Canadian. But that doesn’t mean Canada has to lose out on this massive opportunity.

Click link above to read more

Ransomware update: Documents from Calgary energy firm released

https://www.itworldcanada.com/article/ransomware-update-documents-from-calgary-energy-firm-released/439150

A ransomware gang that claims to have hit Parkland Corp., a multi-million dollar publicly-traded Calgary energy firm, has begun publishing what it says is copied data from the company, including a photocopy of one of the directors’ passports.

A Parkland spokesperson wouldn’t confirm the cyber incident it suffered Nov. 14 was ransomware, but this week the gang behind the Clop ransomware began publishing stolen data

Click link above to read more

Darknet Drug Dealers Are Now Selling ‘Pfizer COVID Vaccines’ – VICE

https://darknet-sites.com/?p=74966

The United Kingdom ordered 40 million doses of Pfizer/BioNTech’s much-lauded coronavirus vaccine in the lead up to next week, when the nation will become the first in the world to make the drug available for general use. Some 800,000 doses are expected to arrive within the next few days; a further 10 million will become available shortly thereafter; and at least 50 hospitals across the country are preparing for the staggered roll-out.

Click link above to read more

FBI Warning: ‘Tis the Season for Holiday Scams

https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/fbi-warning-tis-the-season-for-holiday-scams

During the holidays, scammers focus less on giving and more on stealing. Shoppers looking for a good deal this holiday season should be aware of increasingly aggressive and unorthodox scams designed by criminals to steal money and personal information. According to the FBI’s Internet Crime Complaint Center (IC3), in 2019 people living in the greater Erie area lost more than $170,000 due to a variety of scams. The number of victims reporting losses so far this year has doubled from last year. FBI Pittsburgh wants local shoppers to enjoy a scam-free holiday season by remaining vigilant against the following schemes.

Click link above to read more

Phishing Campaign Targeted Universities Worldwide

https://www.databreachtoday.com/phishing-campaign-targeted-universities-worldwide-a-15518

A hacking group targeted 20 universities and schools around the world earlier this year with a series of phishing attacks designed to steal credentials, according to researchers with RiskIQ.

The group, which the RiskIQ researchers call "Shadow Academy," targeted 14 universities and schools within the U.S. between July and October, when fall semester classes were beginning, according to the report. The first university struck was the University of Louisiana, but other schools, such as Manhattan College, Rochester Institute of Technology, Bowling Green State University, University of Arizona and University of Washington, were also victimized.

Click link above to read more

Cybersecurity in the Biden Administration: Experts Weigh In

https://www.darkreading.com/threat-intelligence/cybersecurity-in-the-biden-administration-experts-weigh-in/d/d-id/1339598

President-elect Joe Biden's transition team has recently been announcing appointments for the incoming administration. As the country learns who will lead it next, cybersecurity experts are speculating how the appointees will approach protecting the United States from cyberthreats.

"I think you'll finally see cyber and cybersecurity issues become a true national security, economic security, and diplomatic priority," said Chris Painter, president of the Global Forum on Cyber Expertise Foundation and former government cybersecurity official, in a panel today on the Biden cyber agenda hosted by the Institute for Security + Technology. "We've been moving toward that. I think it'll finally get there, and it won't take a 'cyber 9/11,' 'cyber Pearl Harbor' … that people have been predicting for years. I think we're finally at that level of maturity."

Click link above to read more

Research: Millions of smart devices vulnerable to hacking

https://www.ctvnews.ca/sci-tech/research-millions-of-smart-devices-vulnerable-to-hacking-1.5221458

BOSTON -- Researchers at a cybersecurity firm say they have identified vulnerabilities in software widely used by millions of connected devices -- flaws that could be exploited by hackers to penetrate business and home computer networks and disrupt them.

There is no evidence of any intrusions that made use of these vulnerabilities. But their existence in data-communications software central to internet-connected devices prompted the U.S. Cybersecurity and Infrastructure Security Agency to flag the issue in a bulletin.

Click link above to read more

Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says

https://londondaily.com/middle-east-facing-cyber-pandemic-as-covid-exposes-security-vulnerabilities-cyber-chief-says

The Middle East region is facing a “cyber pandemic” with Covid-19 related attacks skyrocketing this year, according to the United Arab Emirates government’s top cyber security chief.

“As we moved into a full online life, we saw a huge increase in many of those attacks,” Mohamed al-Kuwaiti, head of UAE Government Cyber Security, told a CNBC-moderated panel at the Gulf Information Security Expo and Conference in Dubai on Sunday.

Click link above to read more

SANS cybersecurity training firm suffers data breach due to phishing attack

https://www.techrepublic.com/article/sans-cybersecurity-training-firm-suffers-data-breach-due-to-phishing-attack/

Disclosing the incident in a website post, SANS said that a total of 513 emails were forwarded to an unknown external email address. Most of these emails were "harmless," according to the company. But some contained files with personally identifiable information (PII), pointing to the 28,000 records that were compromised.

SANS revealed that it found the following types of breached PII: email address, work title, first name, last name, work phone, company name, industry, address, and country of residence. However, it uncovered no evidence that passwords or financial data such as credit card numbers were compromised. SANS said it has identified the people whose accounts were compromised and will be contacting them by email.

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