Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

November 22, 2022

Challenge yourself with our Online Shopping Security Quiz

This past week's stories:

🍁 **Around 100 emergency services potentially impacted by cybersecurity incident**

🍁 **Montreal-area city hit by ransomware: Report**

🍁 **Beware of gift card fraud — don't let it hijack your perfect present**

🍁 **Some in Ontario broader public sector are "struggling" with cybersecurity: Panel chair**

Iran-linked threat actors exploiting Log4Shell via unpatched VMware, feds warn

Nokia warns 5G security 'breaches are the rule, not the exception'

How training and continuing education are crucial for healthcare cybersecurity leaders and staff

High severity vulnerabilities reported in F5 BIG-IP and BIG-IQ devices

How BlackBerry moved from iconic cellphones to cybersecurity

Chinese 'Mustang Panda' hackers actively targeting governments worldwide

Upskilling workers in technology and cyber security roles is 'paramount'

Cybercriminals strike understaffed organizations on weekends and holidays

---

Around 100 emergency services potentially impacted by cybersecurity incident

Around 100 emergency services across Ontario may have been impacted by a potential cybersecurity incident.

As a result, a paramedic services' third-party platform used to record patient data run by ESO has been taken offline.

The Hamilton Paramedic Service and Haldimand County EMS has confirmed they have been affected by the incident.

https://www.chch.com/around-100-emergency-services-potentially-impacted-by-cybersecurity-incident/

Click above link to read more.

Back to top

Montreal-area city hit by ransomware: Report

A Montreal-area city was hit by ransomware over the weekend, according to a Quebec news service.

La Presse reported this morning that the city of Westmount mayor Christina Smith confirmed the attack. Westmount is a municipality of about 21,000 people within Montreal.

The Lockbit ransomware gang has claimed credit, saying it copied 14 TB of data and will release it in two weeks unless a ransom is paid. The city's website hasn't been affected by the attack.

https://www.itworldcanada.com/article/montreal-area-city-hit-by-ransomware-report/514484

Click above link to read more.

Back to top

Beware of gift card fraud — don't let it hijack your perfect present

The past few years have been a wild ride for online shoppers, and the 2022 holiday season probably won't be much different. Experts are expecting aftershocks from the notorious supply chain crisis — namely inflation, understaffing and inventory uncertainties — to impact holiday shopping again.

Smart consumers are ahead of the game. A recent survey by RetailMeNot revealed that more than 50% of holiday shoppers plan on circumventing these issues by going the gift card route this year. The only problem? The very real dangers of gift card fraud.

https://ca.news.yahoo.com/gift-card-fraud-malwarebytes-154531275.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAB2pusM3fH8NXqtO6qt1IwWKfr3vAt3qDyi1R-CgqsCLt4MmLmGP4YWu944e-Eqykd2evZ3nsiAqjMipmWWulAsIFVp82mgUgJjcssPhw-R5yAoPe3ywtO53AkbXGiE0dArHbHbdiBUXjAFDAr4eDktulOH_9c1iZhh8vUg0juj4

Click above link to read more.

Back to top

Some in Ontario broader public sector are "struggling" with cybersecurity: Panel chair

The poor state of cybersecurity of some of Ontario's school boards, child welfare agencies, municipalities, and hospitals worries the head of the province's expert panel that just evaluated the condition of the broader public sector.

"Some townships, small municipalities are really struggling," Robert Wong, former chief information officer (CIO) of Toronto Hydro and currently a member of the board of Ontario's Independent Electricity System Operator, said in an interview. He is particularly concerned about smaller institutions and their smaller financial and personnel resources.

https://financialpost.com/technology/some-in-ontario-broader-public-sector-are-struggling-with-cybersecurity-panel-chair

Click above link to read more.

Back to top

Iran-linked threat actors exploiting Log4Shell via unpatched VMware, feds warn

State-backed Iranian threat actors are exploiting a Log4Shell vulnerability inside an unpatched VMware server at a federal civilian agency, the Cybersecurity and Infrastructure Security Agency warned in a joint advisory with the FBI Wednesday.

After conducting an investigation from mid-June into July, authorities discovered that attackers installed XMRig cryptomining software and moved laterally into a domain controller. The actors stole credentials and installed Ngrok reverse proxies to maintain persistence inside the network.

https://www.cybersecuritydive.com/news/iran-threat-log4shell-unpatched-vmware/636780/

Click above link to read more.

Back to top

Nokia warns 5G security 'breaches are the rule, not the exception'

5G was supposed to make wireless networks more secure, but that’s not panning out, according to research conducted by GlobalData and commissioned by Nokia.

Nearly three-quarters of the 5G network operators surveyed said they’ve experienced up to six security breaches or cyberattacks in the past year, according to the report published Tuesday. These breaches resulted in network downtime, customer data leaks, regulatory liabilities, fraud and monetary theft.

https://www.cybersecuritydive.com/news/5g-security-breaches/636693/

Click above link to read more.

Back to top

How training and continuing education are crucial for healthcare cybersecurity leaders and staff

Training is one of the main components of protecting against cyberattacks. And this goes not just for healthcare provider organization employees but also the security managers and staff – especially those looking to get ahead.

This is the topic of "In-house Career Development: Hiring from Within," an educational session at the HIMSS Healthcare Cybersecurity Forum, December 5-6 in Boston.

https://www.healthcareitnews.com/news/how-training-and-continuing-education-are-crucial-healthcare-cybersecurity-leaders-and-staff

Click above link to read more.

Back to top

High severity vulnerabilities reported in F5 BIG-IP and BIG-IQ devices

Multiple security vulnerabilities have been disclosed in F5 BIG-IP and BIG-IQ devices that, if successfully exploited, to completely compromise affected systems.

Cybersecurity firm Rapid7 said the flaws could be abused to remote access to the devices and defeat security constraints. The issues impact BIG-IP versions 13.x, 14.x, 15.x, 16.x, and 17.x, and BIG-IQ Centralized Management versions 7.x and 8.x.

https://thehackernews.com/2022/11/high-severity-vulnerabilities-reported.html

Click above link to read more.

Back to top

How BlackBerry moved from iconic cellphones to cybersecurity

BlackBerry was once at the top of the smartphone market in the U.S. In 2010, almost half of smartphone subscribers in the U.S. used BlackBerrys, according to Comscore.

The phones were well-known for having a tactile keyboard and for BlackBerry's advanced cybersecurity — often favored among businesses and governments.

https://www.cnbc.com/2022/11/19/how-blackberry-moved-from-iconic-cellphones-to-cybersecurity.html

Click above link to read more.

Back to top

Chinese 'Mustang Panda' hackers actively targeting governments worldwide

A notorious advanced persistent threat actor known as Mustang Panda has been linked to a spate of spear-phishing attacks targeting government, education, and research sectors across the world.

The primary targets of the intrusions from May to October 2022 included counties in the Asia Pacific region such as Myanmar, Australia, the Philippines, Japan, and Taiwan, cybersecurity firm Trend Micro said in a Friday report.

https://thehackernews.com/2022/11/chinese-mustang-panda-hackers-actively.html

Click above link to read more.

Back to top

Upskilling workers in technology and cyber security roles is 'paramount'

Top business lobby, the Australian Industry Group, says the new technologies arriving in freight transport and handling require "the simultaneous upskilling of the workforce to manage and utilise them efficiently".

Such needs can be met by co-ordinating the implementation of skills requirements across the country; through diplomas and other vocational education and training qualifications, AiG says in a submission to the Productivity Commission's current maritime inquiry.

https://www.theaustralian.com.au/special-reports/upskilling-workers-in-technology-and-cyber-security-roles-is-paramount/news-story/9d705ca34af6592936fac22524899ff6

Click above link to read more.

Back to top

Cybercriminals strike understaffed organizations on weekends and holidays

More than one-third of respondents said it took their organization longer to assess the scope, stop and recover from a holiday or weekend attack compared to a weekday, according to a Cybereason survey published Wednesday. Larger organizations with more than 2,000 employees were even more likely to experience delays.

https://www.cybersecuritydive.com/news/cyberattacks-weekends-holidays/636956/

Click above link to read more.

Back to top

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