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

February 14, 2023

There has been an increase in fraudulent activity regarding the BC Services Card App. Please ensure that you only download BC Government documents and BC Services Card App from official sources (gov.bc.ca). The BC Services Card app is free and available for Android™ and iOS (iPhone® and iPad®).

Challenge yourself with our Raise Your Cyber Security Game Quiz!

This past week’s stories:

🍁 **Ross Memorial Hospital in Lindsay declares code grey after suspected cybersecurity incident**

🍁**Indigo payment systems, online store down after 'cybersecurity incident'**

🍁**Give tax break so small Canadian firms can invest in cybersecurity, Parliament told**

Seven Russians sanctioned over ransomware cyber-crime

Lockbit reaches new lows by targeting an IDD clinic

Popular Android diamond game spills players’ data

Hackers breach Reddit to steal source code and internal data

Researchers uncover obfuscated malicious code in PyPI Python packages

North Korean hackers targeting healthcare with ransomware to fund its operations

Several NATO websites suffer a cyber attack

Hackers targeting telecommunications industry – over 74 million clients’ data leaked

3 overlooked cybersecurity breaches

Scammers profit from Turkey-Syria earthquake

Ross Memorial Hospital in Lindsay declares code grey after suspected cybersecurity incident

Ross Memorial Hospital in Lindsay, Ont., issued a “Code Grey” following a suspected cybersecurity incident on Sunday night.

Although the hospital did not provide details on what was compromised, officials said its systems restoration plan is ongoing. The hospital is in communication with local, regional and provincial partners regarding the next steps.

https://globalnews.ca/news/9469977/ross-memorial-hospital-in-lindsay-declares-code-grey-after-suspected-cybersecurity-incident/

Click above link to read more.

Back to top

Indigo payment systems, online store down after 'cybersecurity incident'

Indigo's payment systems and online store are down after a "cybersecurity incident," the company announced on Wednesday evening.

The bookstore chain, which also owns Chapters and Coles, said in a statement posted to its website and social media accounts it is working with "third-party experts to investigate and resolve the situation."

https://www.ctvnews.ca/business/indigo-payment-systems-online-store-down-after-cybersecurity-incident-1.6266138

Click above link to read more.

Back to top

Give tax break so small Canadian firms can invest in cybersecurity, Parliament told

Ottawa should deploy a wide range of strategies, including tax breaks, to encourage small businesses to take cybersecurity more seriously, a member of a think tank told a parliamentary committee this week.

“I think the government should incentivize companies to adopt the latest security measures, such as the cybersecurity standard established by ISED (Innovation, Science and Economic Development) and CSE (the Canadian Security Establishment, the country’s electronic spy agency that also protects federal IT networks) for small and medium organizations,” Aaron Shull, managing director and general counsel of the Centre for International Governance Innovation (CIGI) told the House of Commons defence committee.

https://www.itbusiness.ca/news/give-tax-break-so-small-canadian-firms-can-invest-in-cybersecurity-parliament-told/124167

Click above link to read more.

Back to top

Seven Russians sanctioned over ransomware cyber-crime

Seven Russian men have been sanctioned by the UK and US for having links to recent ransomware attacks.

The UK's Foreign Office, along with US authorities, has released pictures of the men, frozen their assets and imposed travel restrictions.

US authorities have accused them of being members of loosely defined Russian-based hacking network Trickbot.

https://www.bbc.com/news/technology-64586361

Click above link to read more.

Back to top

Lockbit reaches new lows by targeting an IDD clinic

The prolific ransomware gang Lockbit likely breached support service for children with intellectual and developmental disabilities (IDD).

The Arc of Essex County, a New Jersey-based organization for children with IDD, has appeared on Lockbit’s blog, an underground website the gang uses to post its victims.

The countdown clock implies that the organization’s data will be made public if the Arc of Essex County doesn’t pay ransom until February 26.

https://cybernews.com/news/lockbit-targets-idd-clinic/

Click above link to read more.

Back to top

Popular Android diamond game spills players’ data

The research by Cybernews has discovered that the Sweet Diamond Shooter app had sensitive data hardcoded into the client side of the app.

This means that threat actors can get their hands on Google API (application programming interface) keys, Google Storage buckets URLs, and unprotected databases and exploit that information simply by reversing and analyzing publicly available information about the app.

https://cybernews.com/security/sweet-diamond-shooter-leak/

Click above link to read more.

Back to top

Hackers breach Reddit to steal source code and internal data

Reddit suffered a cyberattack Sunday evening, allowing hackers to access internal business systems and steal internal documents and source code.

The company says the hackers used a phishing lure targeting Reddit employees with a landing page impersonating its intranet site. This site attempted to steal employees' credentials and two-factor authentication tokens.

After one employee fell victim to the phishing attack, the threat actor was able to breach internal Reddit systems to steal data and source code.

https://www.bleepingcomputer.com/news/security/hackers-breach-reddit-to-steal-source-code-and-internal-data/

Click above link to read more.

Back to top

Researchers uncover obfuscated malicious code in PyPI Python packages

Four different rogue packages in the Python Package Index (PyPI) have been found to carry out a number of malicious actions, including dropping malware, deleting the netstat utility, and manipulating the SSH authorized_keys file.

The packages in question are aptx, bingchilling2, httops, and tkint3rs, all of which were collectively downloaded about 450 times before they were taken down.

https://thehackernews.com/2023/02/researchers-uncover-obfuscated.html

Click above link to read more.

Back to top

North Korean hackers targeting healthcare with ransomware to fund its operations

State-backed hackers from North Korea are conducting ransomware attacks against healthcare and critical infrastructure facilities to fund illicit activities, U.S. and South Korean cybersecurity and intelligence agencies warned in a joint advisory.

The attacks, which demand cryptocurrency ransoms in exchange for recovering access to encrypted files, are designed to support North Korea's national-level priorities and objectives.

https://thehackernews.com/2023/02/north-korean-hackers-targeting.html

Click above link to read more.

Back to top

Several NATO websites suffer a cyber attack

Several NATO websites have suffered a computer attack on Sunday night, leaving the NATO Special Operations Headquarters website, among others, temporarily inoperative.

"NATO cyber experts are actively dealing with an incident affecting some NATO websites. NATO deals with cyber incidents on a regular basis, and takes cyber security very seriously," an Atlantic Alliance official told DPA news agency.

https://www.msn.com/en-ca/news/world/several-nato-websites-suffer-a-cyber-attack/ar-AA17p0YN?li=AAggFp4

Click above link to read more.

Back to top

Hackers targeting telecommunications industry – over 74 million clients' data leaked

Among the most crucial industries to any nation's infrastructure is the one based on telecommunications. It serves as the foundation for communication and coordination, providing the necessary connectivity for people to stay connected and for businesses to operate efficiently.

The year 2023 is projected to have an impressive increase in the number of internet users, reaching a total of 311.3 million individuals. This represents a remarkable 91.8% penetration rate among the general population.

https://cybersecuritynews.com/hackers-telecommunications-industry/

Click above link to read more.

Back to top

---

3 overlooked cybersecurity breaches

Here are three of the worst breaches, attacker tactics and techniques of 2022, and the security controls that can provide effective, enterprise security protection for them.

https://thehackernews.com/2023/02/3-overlooked-cybersecurity-breaches.html

Click above link to read more.

Back to top

Scammers profit from Turkey-Syria earthquake

Scammers are using the earthquakes in Turkey and Syria to try to trick people into donating to fake causes, security experts have warned.

These scams claim to raise money for survivors, left without heat or water following the disasters that have killed more than 35,000 people.

https://www.bbc.com/news/world-europe-64599553

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