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

September 19, 2023

Challenge yourself with our Social Engineering Quiz!

Cybersecurity Issue of the Week: **PHISHING**

✪ Read our **PHISHING INFOSHEET** to learn more.

This past week's stories:

🍁 Multiple government websites down across Canada, cyberattacks blamed for 2

🍁 Former CyberNB website now promotes online casinos

🍁 Quebec government says data not compromised after websites hit by cyberattack

🍁 Weather Network affected by cybersecurity incident, some data systems down

✪ Microsoft warns of new phishing campaign targeting corporations via Teams messages

Caesars reportedly paid cyber ransom, MGM credit rating vulnerable following hack

Automotive supply chain vulnerable to attack as cybersecurity regulation looms

Free download manager site compromised to distribute Linux malware to users for 3+ years

PH, Estonia to sign memorandum for cybersecurity

New proposal aims to boost IoT security with a sticker

Australia's new cybersecurity strategy to build 6 "cyber shields" around the country

How NIST Cybersecurity Framework 2.0 tackles risk management

TikTok flooded by 'Elon Musk' cryptocurrency giveaway scams

Multiple government websites down across Canada, cyberattacks blamed for 2

Government websites in four provinces and territories were shut down Thursday, with at least two jurisdictions blaming cyberattacks for their outages.

https://globalnews.ca/news/9962363/government-websites-down-cyberattacks-provinces-territories/

Click above link to read more.

Back to top

Former CyberNB website now promotes online casinos

A website that used to promote New Brunswick's cybersecurity sector has been repurposed by an anonymous new owner and is now promoting a number of online casinos.

https://www.cbc.ca/news/canada/new-brunswick/cyber-nb-website-takeover-1.6950774

Click above link to read more.

Back to top

Quebec government says data not compromised after websites hit by cyberattack

The Quebec government has been hit with a denial-of-service style cyberattack allegedly carried out by the pro-Russian hacker group NoName, with some government-linked websites down as a result.

https://montreal.ctvnews.ca/quebec-government-sites-under-cyber-attack-1.6560005

Click above link to read more.

Back to top

Weather Network affected by cybersecurity incident, some data systems down

The parent company of The Weather Network says it was affected by a cybersecurity incident that took down some of its data systems.

https://nationalpost.com/news/canada/weather-network-cybersecurity

Click above link to read more.

[Back to top](#)

Microsoft warns of new phishing campaign targeting corporations via Teams messages

Microsoft is warning of a new phishing campaign undertaken by an initial access broker that involves using Teams messages as lures to infiltrate corporate networks.

https://thehackernews.com/2023/09/microsoft-warns-of-new-phishing.html

Click above link to read more.

[Back to top](#)

Caesars reportedly paid cyber ransom, MGM credit rating vulnerable following hack

News of cyber breaches afflicting Las Vegas Strip casino operators is getting worse. Just two days after MGM Resorts International (NYSE: MGM) confirmed it was the victim of a wide-ranging cyber attack, rival Caesars Entertainment (NASDAQ: CZR) will reportedly soon tell investors it was the target of a ransomware crime.

https://www.casino.org/news/caesars-reportedly-paid-hackers-ransomware-demand/

Click above link to read more.

[Back to top](#)

Automotive supply chain vulnerable to attack as cybersecurity regulation looms

Almost two-thirds (64%) of automotive industry leaders believe their supply chain is vulnerable to cyberattacks, with many businesses inadequately prepared for a connected automotive era. That's according to new Kaspersky research based on 200 interviews with C-level decision makers in large enterprises of at least 1,000 employees in the automotive sector. It revealed a vast range of attacks encountered by automotive companies - from vendor to supplier - at almost every stage of production.

https://www.csoonline.com/article/652299/automotive-supply-chain-vulnerable-to-attack-as-cybersecurity-regulation-looms.html

Click above link to read more.

Back to top

Free download manager site compromised to distribute Linux malware to users for 3+ years

A download manager site served Linux users malware that stealthily stole passwords and other sensitive information for more than three years as part of a supply chain attack.

https://thehackernews.com/2023/09/free-download-manager-site-compromised.html

Click above link to read more.

Back to top

PH, Estonia to sign memorandum for cybersecurity

The Philippines is partnering with Estonia to strengthen cybersecurity and digital innovations, the information and communications department said.

https://globalnation.inquirer.net/219364/ph-estonia-to-sign-memorandum-for-cybersecurity

Click above link to read more.

Back to top

New proposal aims to boost IoT security with a sticker

To better protect users of smart devices, the Federal Communications Commission (FCC) has proposed a cybersecurity labeling program.

https://cybernews.com/security/fcc-proposal-aims-boost-iot-security-with-labeling-program/

Click above link to read more.

Back to top

Australia’s new cybersecurity strategy to build 6 “cyber shields” around the country

The Australian federal government announced its first plans for what the 2023-30 national cybersecurity strategy will look like by educating citizens and businesses, investing in cyber skills and collaborating with national and international partners.

https://www.csoonline.com/article/652708/australias-new-cybersecurity-strategy-to-build-6-cyber-shields-around-the-country.html

Click above link to read more.

Back to top

How NIST Cybersecurity Framework 2.0 tackles risk management

The NIST Cybersecurity Framework 2.0 (CSF) is moving into its final stages before its 2024 implementation. After the public discussion period to inform decisions for the framework closed in May, it's time to learn more about what to expect from the changes to the guidelines.

https://securityintelligence.com/articles/how-nist-cybersecurity-framework-2-tackles-risk-management/

Click above link to read more.

Back to top

TikTok flooded by 'Elon Musk' cryptocurrency giveaway scams

TikTok is flooded by a surge of fake cryptocurrency giveaways posted to the video-sharing platform, with almost all of the videos pretending to be themes based on Elon Musk, Tesla, or SpaceX.

https://www.bleepingcomputer.com/news/security/tiktok-flooded-by-elon-musk-cryptocurrency-giveaway-scams/

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