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

August 22, 2023

Challenge yourself with our Cryptocons Quiz!

This past week's stories:

🍁 HRM has insufficient oversight of its cybersecurity risks, AG report says
🍁 Aeroplan numbers, personal information leaked in LCBO data breach
🍁 'This looked legit': Mom scammed trying to buy Taylor Swift tickets for daughter
NoFilter Attack: Sneaky privilege escalation method bypasses Windows security
China-linked Bronze Starlight group targeting gambling sector with Cobalt Strike beacons
QR code hacks are another thing to worry about now
Mass phishing campaign attacking Zimbra users' to steal login credentials
Saturn app gaining popularity with students raises security concerns from parents and experts
HiatusRAT malware resurfaces: Taiwan firms and U.S. military under attack
Japanese watchmaker Seiko breached by BlackCat ransomware gang
New WinRAR vulnerability could allow hackers to take control of your PC

HRM has insufficient oversight of its cybersecurity risks, AG report says

In her final act as Halifax's Auditor General, Evangeline Colman-Sadd presented the findings of a management of cybersecurity audit on Wednesday.

https://globalnews.ca/news/9900429/halifax-hrm-insufficient-oversight-cybersecurity-risks-auditor-general/

Click above link to read more.

Back to top

Aeroplan numbers, personal information leaked in LCBO data breach

The Liquor Control Board of Ontario (LCBO) says customers' personal Information has been compromised in a data breach – for the second time this year.

https://toronto.ctvnews.ca/aeroplan-numbers-personal-information-leaked-in-lcbo-data-breach-1.6521748

Click above link to read more.

Back to top

'This looked legit': Mom scammed trying to buy Taylor Swift tickets for daughter

When Einav Feldman heard Taylor Swift was coming to Toronto for six shows next year, she knew she had to try to get tickets for her daughter, saying it would make her overjoyed.

https://globalnews.ca/news/9897224/mom-scammed-trying-to-buy-taylor-swift-tickets/

Click above link to read more.

Back to top

NoFilter Attack: Sneaky privilege escalation method bypasses Windows security

A previously undetected attack method called NoFilter has been found to abuse the Windows Filtering Platform (WFP) to achieve privilege escalation in the Windows operating system.

https://thehackernews.com/2023/08/nofilter-attack-sneaky-privilege.html

Click above link to read more.

Back to top

China-linked Bronze Starlight group targeting gambling sector with Cobalt Strike beacons

An ongoing cyber attack campaign originating from China is targeting the Southeast Asian gambling sector to deploy Cobalt Strike beacons on compromised systems.

https://thehackernews.com/2023/08/china-linked-bronze-starlight-group.html

Click above link to read more.

[Back to top](#)

QR code hacks are another thing to worry about now

Along with Zoom and those little silicone thingies that allow you to attach hand sanitizer bottles to the zipper of your fanny pack, one of the technologies Covid has thrust into our lives is the QR code.

https://www.bloomberg.com/news/newsletters/2023-08-18/qr-code-phishing-spam-email-is-the-next-cybersecurity-threat

Click above link to read more.

[Back to top](#)

Mass phishing campaign attacking Zimbra users' to steal login credentials

A group of researchers recently published a significant mass-spreading phishing campaign. It targets Zimbra account users, shedding light on a campaign that has been active since April 2023.

https://cybersecuritynews.com/mass-phishing-campaign-zimbra/

Click above link to read more.

[Back to top](#)

Saturn app gaining popularity with students raises security concerns from parents and experts

A popular app used by high schoolers is raising concerns from parents and cybersecurity experts. The Saturn app is promoted as a way for high school students to view their schedule, chat, and create a social calendar for meeting up, and planning for school events.

https://www.koaa.com/news/covering-colorado/high-school-calendar-app-gaining-popularity-with-students-raises-security-concerns-from-parents-and-experts

Click above link to read more.

[Back to top](#)

HiatusRAT malware resurfaces: Taiwan firms and U.S. military under attack

The threat actors behind the HiatusRAT malware have returned from their hiatus with a new wave of reconnaissance and targeting activity aimed at Taiwan-based organizations and a U.S. military procurement system.

https://thehackernews.com/2023/08/hiatusrat-malware-resurfaces-taiwan.html

Click above link to read more.

Back to top

Japanese watchmaker Seiko breached by BlackCat ransomware gang

The BlackCat/ALPHV ransomware gang has added Seiko to its extortion site, claiming responsibility for a cyberattack disclosed by the Japanese firm earlier this month.

https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/

Click above link to read more.

Back to top

New WinRAR vulnerability could allow hackers to take control of your PC

A high-severity security flaw has been disclosed in the WinRAR utility that could be potentially exploited by a threat actor to achieve remote code execution on Windows systems.

https://thehackernews.com/2023/08/new-winrar-vulnerability-could-allow.html

Click above link to read more.

Back to top

Back to (cybersecurity) school: 5 tips from ITS

The digital realm is riddled with email and phishing scams, hoaxes, fake websites, spam and sundry schemes that hackers and identity thieves conjure up to trick people into revealing bank account and credit card numbers, Social Security numbers and other confidential information.

https://news.syr.edu/blog/2023/08/21/back-to-cybersecurity-school-5-tips-from-its/

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