Security News Digest

Information Security Branch

BRITISH COLUMBIA OCIO | Office of the Chief Information Officer

January 3, 2023

Challenge yourself with our Cyber Security Resolutions Quiz!

This past week's stories:

🍁 **Ransomware group LockBit apologizes saying 'partner' was behind SickKids attack**

🍁 **Canadian mining firm shuts down mill after ransomware attack**

Ransomware attack at Louisiana hospital impacts 270,000 patients

Twitter in data-protection probe after '400 million' user details up for sale

BitKeep confirms cyber attack, loses over $9 million in digital currencies

US House bans TikTok on lawmakers' official phones

China and India governments among top targets for cyber attackers

Hackers using stolen bank information to trick victims into downloading BitRAT malware

RedZei Chinese scammers targeting Chinese students in the U.K.

Cybersecurity trends in 2023 that will directly impact everyday life

Rackspace identifies ransomware threat actor behind December attack via Exchange

ABCs of Information Security: A-Z Employee Guide

Ransomware group LockBit apologizes saying 'partner' was behind SickKids attack

A global ransomware operator has issued a rare apology after it claims one of its "partners" was behind a cyberattack on Canada's largest pediatric medical centre.

LockBit, a ransomware group the U.S. Federal Bureau of Investigation has called one of the most active and destructive in the world, posted a brief statement on what cybersecurity experts say is its data leak site claiming it has blocked its partner responsible for the attack on Toronto's Hospital for Sick Children and offering the code to restore the system.

https://www.cbc.ca/news/canada/toronto/ransomware-group-sickkids-cybersecurity-update-1.6701688

Click above link to read more.

Back to top

Canadian mining firm shuts down mill after ransomware attack

The Canadian Copper Mountain Mining Corporation (CMMC) in British Columbia has announced that it was the target of a ransomware attack that impacted its operations.

CMMC, partly owned by Mitsubishi Materials Corporation, is an 18,000-acre claim that produces an average of 100 million pounds of copper per year and has an estimated mineral reserve capacity for another 32 years.

https://www.bleepingcomputer.com/news/security/canadian-mining-firm-shuts-down-mill-after-ransomware-attack/

Click above link to read more.

Back to top

Ransomware attack at Louisiana hospital impacts 270,000 patients

The Lake Charles Memorial Health System (LCMHS) is sending out notices of a data breach affecting almost 270,000 people who have received care at one of its medical centers.

LCMHS is the largest medical complex in Lake Charles, Louisiana, comprising a 314-bed hospital, a 54-bed women's hospital, a 42-bed behavioral health hospital, and a primary care clinic for uninsured citizens.

https://www.bleepingcomputer.com/news/security/ransomware-attack-at-louisiana-hospital-impacts-270-000-patients/

Click above link to read more.

Back to top

Twitter in data-protection probe after '400 million' user details up for sale

A watchdog is to investigate Twitter after a hacker claimed to have private details linked to more than 400 million accounts.

The hacker, "Ryushi", is demanding $200,000 (£166,000) to hand over the data - reported to include that of some celebrities - and delete it.

https://www.bbc.com/news/technology-64109777

Click above link to read more.

Back to top

BitKeep confirms cyber attack, loses over $9 million in digital currencies

Decentralized multi-chain crypto wallet BitKeep on Wednesday confirmed a cyberattack that allowed threat actors to distribute fraudulent versions of its Android app with the goal of stealing users' digital currencies.

"With maliciously implanted code, the altered APK led to the leak of user's private keys and enabled the hacker to move funds," BitKeep CEO Kevin Como said, describing it as a "large-scale hacking incident."

https://thehackernews.com/2022/12/bitkeep-confirms-cyber-attack-loses.html

Click above link to read more.

Back to top

US House bans TikTok on lawmakers’ official phones

The U.S. House of Representatives has ordered its staff and lawmakers to delete TikTok from any government-issued mobile devices due to “security issues” with the popular video-sharing app.

The order to delete the app was issued by Catherine Szpindor, the chief administrative officer of the House, whose office warned in August that the app represented a “high risk to users” citing a “number of security concerns.”

https://techcrunch.com/2022/12/28/house-bans-tiktok-lawmakers-phones/

Click above link to read more.

Back to top

China and India governments among top targets for cyber attackers

China and India were among the most-targeted countries in the past two years when it comes attacks against the government sector, a study has found.

According to data by CloudSEK, an India-based cyber security company, cyber attacks against India's government intensified in 2022, as hacktivist groups such as Dragon Force Malaysia ramped up campaigns in the subcontinent.

https://www.computerweekly.com/news/252528772/China-and-India-governments-among-top-targets-for-cyber-attackers

Click above link to read more.

Back to top

Hackers using stolen bank information to trick victims into downloading BitRAT malware

A new malware campaign has been observed using sensitive information stolen from a bank as a lure in phishing emails to drop a remote access trojan called BitRAT.

The unknown adversary is believed to have hijacked the IT infrastructure of a Colombian cooperative bank, using the information to craft convincing decoy messages to lure victims into opening suspicious Excel attachments.

https://thehackernews.com/2023/01/hackers-using-stolen-bank-information.html

Click above link to read more.

Back to top

RedZei Chinese scammers targeting Chinese students in the U.K.

Chinese international students in the U.K. have been targeted by persistent Chinese-speaking scammers for over a year as part of an activity dubbed RedZei (aka RedThief).

"The RedZei fraudsters have chosen their targets carefully, researched them and realized it was a rich victim group that is ripe for exploitation," cybersecurity researcher Will Thomas (@BushidoToken) said in a write-up published last week.

https://thehackernews.com/2023/01/redzei-chinese-scammers-targeting.html

Click above link to read more.

Back to top

Cybersecurity trends in 2023 that will directly impact everyday life

There are a few certainties in cybersecurity: Ransomware will cause headaches for companies; Third parties will spark cyber incidents; And every December, cybersecurity analysts will put together lists of their predictions and trends they believe will have an impact in the coming year.

Most of the predictions are designed to help organizations build out their security programs, but every so often a trend will build slowly over time until its impact is clear.

https://www.cybersecuritydive.com/news/cyber-security-trends/639480/

Click above link to read more.

Back to top

Rackspace identifies ransomware threat actor behind December attack via Exchange

Rackspace Technology has confirmed the threat actor known as Play was behind the ransomware attack that disrupted email access for its Hosted Exchange customers in early December.

The threat actor was identified following a forensic investigation led by CrowdStrike, the FBI and other experts, Rackspace told Cybersecurity Dive Monday.

https://www.cybersecuritydive.com/news/rackspace-play-ransomware-exchange/639509/

Click above link to read more.

Back to top

ABCs of Information Security: A-Z Employee Guide

With ABCs of information security awareness, we can reduce the risk of losing private information, money, or reputation from cyberattacks. Here we detail the risks involved and prevention.

Information security or InfoSec describes the processes and tools designed and utilized to safeguard confidential company data against modification, interruption, destruction, and inspection.

https://cybersecuritynews.com/abcs-of-information-security/

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