January 31, 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 Cyber Security Resolutions Quiz!

This past week's stories:

- **International ransomware group claims responsibility for Okanagan College cyberattack**
- **Running Room Canada targeted by 'unauthorized group,' customer data stolen**
- **US hacks back against Hive ransomware crew**
- **Russian 'hacktivists' briefly knock German websites offline**
- **5 big pros and cons of ChatGPT for cybersecurity**
- **Ukraine hit with new Golang-based 'SwiftSlicer' wiper malware in latest cyber attack**
- **Gootkit malware continues to evolve with new components and obfuscations**
- **Realtek vulnerability under attack: Over 134 million attempts to hack IoT devices**
- **JD Sports says 10 million customers hit by cyber-attack**
- **The untold story of a crippling ransomware attack**
- **Google Fi says hackers accessed customers' information**
- **KeePass disputes vulnerability allowing stealthy password theft**

International ransomware group claims responsibility for Okanagan College cyberattack

An international ransomware group is claiming responsibility for the cyber attack at Okanagan College earlier this month.

A post by Vice Society was shared on Twitter by Brett Callow, a threat analyst with cyber security firm Emsisoft. It shows a blurred picture of Okanagan College, claiming it has infiltrated more than 850 gigabytes of data.

https://www.castanet.net/news/Kelowna/408424/International-ransomware-group-claims-responsibility-for-Okanagan-College-cyberattack

Click above link to read more.

Back to top

Running Room Canada targeted by 'unauthorized group,' customer data stolen

Sporting goods retailer Running Room has warned its customers in Canada that an outside group potentially accessed their sensitive data through a cyber incident.

On Friday, the retailer sent out emails to its customers, saying it "recently identified and addressed" an incident which involved "a subset of user data." Running Room added that the “unauthorized group” was able to access and “skim” customers' emails, names, addresses, phone numbers and credit card information during the period between November 19, 2022, and January 18, 2023.

https://www.insurancebusinessmag.com/ca/news/cyber/running-room-canada-targeted-by-unauthorized-group-customer-data-stolen-434399.aspx

Click above link to read more.

Back to top

US hacks back against Hive ransomware crew

The US has revealed it infiltrated a prolific cyber-crime gang to secretly sabotage their hacking attacks for more than six months.

The Department of Justice (DOJ) revealed the FBI gained deep access to the Hive ransomware group in late July 2022.

https://www.bbc.com/news/technology-64418723

Click above link to read more.

Back to top

Russian 'hacktivists' briefly knock German websites offline

Russian activist hackers knocked several German websites offline on Wednesday in response to Berlin's decision to send tanks to Ukraine, although Germany's BSI cyber agency said the digital blitz had little tangible effect.

Germany said on Wednesday it would supply its Leopard 2 tanks to Ukraine, overcoming misgivings about sending heavy weaponry that Kyiv sees as crucial to defeat Russia's invasion but Moscow casts as a dangerous provocation.

https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/

Click above link to read more.

Back to top

---

5 big pros and cons of ChatGPT for cybersecurity

History reveals to us that advanced technology, even when it’s developed with the best of intentions, will inevitably end up being used in ways that cause harm. AI is certainly no exception. But with OpenAI’s ChatGPT, both the positive and negative uses of the technology seem to have been taken up a notch. And when it comes to cybersecurity, there’s now mounting evidence that the AI-powered chatbot could be a powerful tool both for hackers and cyber defenders.

https://www.crn.com/news/security/5-big-pros-and-cons-of-chatgpt-for-cybersecurity

Click above link to read more.

Back to top

Ukraine hit with new Golang-based 'SwiftSlicer' wiper malware in latest cyber attack

Ukraine has come under a fresh cyber onslaught from Russia that involved the deployment of a previously undocumented Golang-based data wiper dubbed SwiftSlicer.

ESET attributed the attack to Sandworm, a nation-state group linked to Military Unit 74455 of the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).

https://thehackernews.com/2023/01/ukraine-hit-with-new-golang-based.html

Click above link to read more.

Back to top

Gootkit malware continues to evolve with new components and obfuscations

The threat actors associated with the Gootkit malware have made "notable changes" to their toolset, adding new components and obfuscations to their infection chains.

Google-owned Mandiant is monitoring the activity cluster under the moniker UNC2565, noting that the usage of the malware is "exclusive to this group."

https://thehackernews.com/2023/01/gootkit-malware-continues-to-evolve.html

Click above link to read more.

Back to top

Realtek vulnerability under attack: Over 134 million attempts to hack IoT devices

Researchers are warning about a spike in exploitation attempts weaponizing a critical remote code execution flaw in Realtek Jungle SDK since the start of August 2022.

According to Palo Alto Networks Unit 42, the ongoing campaign is said to have recorded 134 million exploit attempts as of December 2022, with 97% of the attacks occurring in the past four months.

https://thehackernews.com/2023/01/realtek-vulnerability-under-attack-134.html

Click above link to read more.

Back to top

JD Sports says 10 million customers hit by cyber-attack

Sportswear chain JD Sports has said stored data relating to 10 million customers might be at risk after it was hit by a cyber-attack.

The company said information that "may have been accessed" by hackers included names, addresses, email accounts, phone numbers, order details and the final four digits of bank cards.

https://www.bbc.com/news/business-64452986

Click above link to read more.

Back to top

The untold story of a crippling ransomware attack

It was a Sunday morning in mid-October 2020 when Rob Miller first heard there was a problem. The databases and IT systems at Hackney Council, in East London, were suffering from outages. At the time, the UK was heading into its second deadly wave of the coronavirus pandemic, with millions living under lockdown restrictions and normal life severely disrupted. But for Miller, a strategic director at the public authority, things were about to get much worse. “By lunchtime, it was apparent that it was more than technical stuff,” Miller says.

Two days later, the leaders of Hackney Council—which is one of London’s 32 local authorities and responsible for the lives of more than 250,000 people—revealed it had been hit by a cyberattack. Criminal hackers had deployed ransomware that severely crippled its systems, limiting the council’s ability to look after the people who depend on it. The Pysa ransomware gang later claimed responsibility for the attack and, weeks later, claimed to be publishing data it stole from the council.

https://www.wired.com/story/ransomware-attack-recovery-hackney/

Click above link to read more.

Back to top

Google Fi says hackers accessed customers’ information

Google’s cell network provider Google Fi has confirmed a data breach, likely related to the recent security incident at T-Mobile, which allowed hackers to steal millions of customers’ information.

In an email sent to customers on Monday, obtained by TechCrunch, Google said that the primary network provider for Google Fi recently informed the company that there had been suspicious activity relating to a third party support system containing a “limited amount” of Google Fi customer data.

https://techcrunch.com/2023/01/31/google-fi-customer-data-breach/

Click above link to read more.

Back to top

KeePass disputes vulnerability allowing stealthy password theft

The development team behind the open-source password management software KeePass is disputing what is described as a newly found vulnerability that allows attackers to stealthily export the entire database in plain text.

KeePass is a very popular open-source password manager that allows you to manage your passwords using a locally stored database, rather than a cloud-hosted one, such as LastPass or Bitwarden.

https://www.bleepingcomputer.com/news/security/keepass-disputes-vulnerability-allowing-stealthy-password-theft/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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