




June 13, 2023

Challenge yourself with our [Spear Phishing quiz!](#)

[This past week's stories:](#)

-  [Cascades Casino cybersecurity attack may have breached personal employee information](#)
 -  [At least 100,000 Nova Scotians affected by cybertheft of government employee files](#)
 -  [Seneca Polytechnic, Microsoft Canada and Sobeys Inc. are preparing the next generation of cybersecurity analysts](#)
 - [Winning the mind game: The role of the ransomware negotiator](#)
 - [BBC, BA and Boots issued with ultimatum by cyber gang Clap](#)
 - [Google introduces SAIF, a framework for secure AI development and use](#)
 - [Asylum Ambuscade: A cybercrime group with espionage ambitions](#)
 - [Mattel experiments with ChatGPT in cybersecurity](#)
 - [Cybersecurity provider warns against fake ChatGPT apps stealing users' money](#)
 - [Swiss government targeted by series of cyber-attacks](#)
 - [Why now? The rise of attack surface management](#)
 - [Cybercriminals using powerful BatCloak engine to make malware fully undetectable](#)
-

Cascades Casino cybersecurity attack may have breached personal employee information

Current and former employees of Cascades Casino in Chatham are being warned their personal information may have been breached following a recent cybersecurity attack that shut down the casino for several weeks.

<https://windsor.ctvnews.ca/cascades-casino-cybersecurity-attack-may-have-breached-personal-employee-information-1.6437852>

Click above link to read more.

[Back to top](#)

At least 100,000 Nova Scotians affected by cybertheft of government employee files

Cybercriminals made off with the personal and banking information of at least 100,000 Nova Scotians last week, before the Nova Scotia government secured a file transfer service that had been breached as part of a global attack on MOVEit.

<https://www.cbc.ca/news/canada/nova-scotia/hack-cyberattack-digital-ns-government-1.6867221>

Click above link to read more.

[Back to top](#)

Seneca Polytechnic, Microsoft Canada and Sobeys Inc. are preparing the next generation of cybersecurity analysts

Seneca Polytechnic, Microsoft Canada and Sobeys Inc. are joining forces to help fill the critical shortage of cybersecurity analysts with a new, affordable series of short-term courses, or microcredentials, available across Canada.

<https://www.newswire.ca/news-releases/seneca-polytechnic-microsoft-canada-and-sobeys-inc-are-preparing-the-next-generation-of-cybersecurity-analysts-850240608.html>

Click above link to read more.

[Back to top](#)

Winning the mind game: The role of the ransomware negotiator

Ransomware is an industry. As such, it has its own business logic: organizations pay money, in crypto-currency, in order to regain control over their systems and data.

<https://thehackernews.com/2023/06/winning-mind-game-role-of-ransomware.html>

Click above link to read more.

[Back to top](#)

BBC, BA and Boots issued with ultimatum by cyber gang Clop

A prolific cyber crime gang thought to be based in Russia has issued an ultimatum to victims of a hack that has hit organisations around the world.

<https://www.bbc.com/news/technology-65829726>

Click above link to read more.

[Back to top](#)

Google introduces SAIF, a framework for secure AI development and use

The Google SAIF (Secure AI Framework) is designed to provide a security framework or ecosystem for the development, use and protection of AI systems.

<https://www.securityweek.com/google-introduces-saif-a-framework-for-secure-ai-development-and-use/>

Click above link to read more.

[Back to top](#)

Asylum Ambuscade: A cybercrime group with espionage ambitions

The threat actor known as Asylum Ambuscade has been observed straddling cybercrime and cyber espionage operations since at least early 2020.

<https://thehackernews.com/2023/06/asylum-ambuscade-cybercrime-group-with.html>

Click above link to read more.

[Back to top](#)

Mattel experiments with ChatGPT in cybersecurity

Toy maker Mattel is experimenting with generative-artificial-intelligence tools including ChatGPT to help its cybersecurity teams, but the company's head of cybersecurity said the risk of inaccurate results from the new technology is too great to deploy it broadly.

<https://www.wsj.com/articles/mattel-experiments-with-chatgpt-in-cybersecurity-c80a0965>

Click above link to read more.

[Back to top](#)

Cybersecurity provider warns against fake ChatGPT apps stealing users' money

In a report, Sophos provided details about these multiple apps masquerading as legitimate, ChatGPT-based chatbots to overcharge users and bring in thousands of dollars a month.

<https://www.gizguide.com/2023/06/fake-chatgpt-apps.html>

Click above link to read more.

[Back to top](#)

Swiss government targeted by series of cyber-attacks

The websites of several Swiss federal agencies and state-linked companies were inaccessible on Monday, June 12, 2023, due to a cyber-attack, Switzerland's finance ministry has confirmed.

<https://www.infosecurity-magazine.com/news/swiss-government-targeted-series/>

Click above link to read more.

[Back to top](#)

Why now? The rise of attack surface management

The term "attack surface management" (ASM) went from unknown to ubiquitous in the cybersecurity space over the past few years. Gartner and Forrester have both highlighted the importance of ASM recently, multiple solution providers have emerged in the space, and investment and acquisition activity have seen an uptick.

<https://thehackernews.com/2023/06/why-now-rise-of-attack-surface.html>

Click above link to read more.

[Back to top](#)

Cybercriminals using powerful BatCloak engine to make malware fully undetectable

A fully undetectable (FUD) malware obfuscation engine named BatCloak is being used to deploy various malware strains since September 2022, while persistently evading antivirus detection.

<https://thehackernews.com/2023/06/cybercriminals-using-powerful-batcloak.html>

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.

