

May 16, 2023

Challenge yourself with our [Vulnerability Management Quiz!](#)

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

🍁 [Government of Canada's DX journey riddled with cyber-struggles, technical debt and staffing concerns: Report](#)

🍁 [National Gallery of Canada recovering from ransomware incident](#)

[BurpGPT – ChatGPT-powered automated vulnerability detection tool](#)

[Cybersecurity firm Dragos discloses cybersecurity incident, extortion attempt](#)

[Multinational tech firm ABB hit by Black Basta ransomware attack](#)

[Twitter launches encrypted private messages, says Elon Musk](#)

[Risk of cyber-attack is main Eurovision worry, says BBC executive](#)

[New ransomware gang RA group hits U.S. and South Korean organizations](#)

[Researchers uncover powerful backdoor and custom implant in year-long cyber campaign](#)

[New phishing-as-a-service platform lets cybercriminals generate convincing phishing pages](#)

[1 million WordPress sites impacted by exploited plugin vulnerability](#)

[ChatGPT is about to revolutionize cybersecurity](#)

[Lessons from 'Star Trek: Picard' – a cybersecurity expert explains how a sci-fi series illuminates today's threats](#)

Government of Canada's DX journey riddled with cyber-struggles, technical debt and staffing concerns: Report

A new report by market intelligence firm International Data Corporation (IDC) found that digital transformation (DX) within public sector agencies has been significantly impaired by security challenges, disconnected inter-departmental systems, and staffing concerns.

<https://www.itworldcanada.com/article/government-of-canadas-dx-journey-riddled-with-cyber-struggles-technical-debt-and-staffing-concerns-report/538904>

Click above link to read more.

[Back to top](#)

National Gallery of Canada recovering from ransomware incident

Canada's national art museum has spent the last two weeks recovering from a ransomware attack that forced it to shut down its IT system.

<https://therecord.media/national-gallery-canada-recovering-from-ransomware-attack>

Click above link to read more.

[Back to top](#)

BurpGPT – ChatGPT-powered automated vulnerability detection tool

Cyber Security News came across a new ChatGPT-powered vulnerability detection tool called "BurpGPT," which helps security researchers to detect the vulnerabilities that traditional scanners might miss.

<https://cybersecuritynews.com/burpgpt/>

Click above link to read more.

[Back to top](#)

Cybersecurity firm Dragos discloses cybersecurity incident, extortion attempt

Industrial cybersecurity company Dragos today disclosed what it describes as a "cybersecurity event" after a known cybercrime gang attempted to breach its defenses and infiltrate the internal network to encrypt devices.

<https://www.bleepingcomputer.com/news/security/cybersecurity-firm-dragos-discloses-cybersecurity-incident-extortion-attempt/>

Click above link to read more.

[Back to top](#)

Multinational tech firm ABB hit by Black Basta ransomware attack

Swiss multinational company ABB, a leading electrification and automation technology provider, has suffered a Black Basta ransomware attack, reportedly impacting business operations.

<https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/>

Click above link to read more.

[Back to top](#)

Twitter launches encrypted private messages, says Elon Musk

Twitter has become the latest social media platform to launch an encrypted messaging service.

<https://www.bbc.com/news/technology-65533021>

Click above link to read more.

[Back to top](#)

Risk of cyber-attack is main Eurovision worry, says BBC executive

The risk of a cyber-attack is the “main worry” for broadcasters staging the Eurovision song contest on behalf of war-torn Ukraine, a BBC executive has said.

<https://www.theguardian.com/tv-and-radio/2023/may/10/risk-of-cyber-attack-is-main-eurovision-worry-says-bbc-executive>

Click above link to read more.

[Back to top](#)

New ransomware gang RA group hits U.S. and South Korean organizations

A new ransomware group known as RA Group has become the latest threat actor to leverage the leaked Babuk ransomware source code to spawn its own locker variant.

<https://thehackernews.com/2023/05/new-ransomware-gang-ra-group-hits-us.html>

Click above link to read more.

[Back to top](#)

Researchers uncover powerful backdoor and custom implant in year-long cyber campaign

Government, aviation, education, and telecom sectors located in South and Southeast Asia have come under the radar of a new hacking group as part of a highly-targeted campaign that commenced in mid-2022 and continued into the first quarter of 2023.

<https://thehackernews.com/2023/05/researchers-uncover-powerful-backdoor.html>

Click above link to read more.

[Back to top](#)

New phishing-as-a-service platform lets cybercriminals generate convincing phishing pages

A new phishing-as-a-service (PhaaS or PaaS) platform named Greatness has been leveraged by cybercriminals to target business users of the Microsoft 365 cloud service since at least mid-2022, effectively lowering the bar to entry for phishing attacks.

<https://thehackernews.com/2023/05/new-phishing-as-service-platform-lets.html>

Click above link to read more.

[Back to top](#)

1 million WordPress sites impacted by exploited plugin vulnerability

Exploitation of a critical vulnerability in the Essential Addons for Elementor WordPress plugin began immediately after a patch was released, WordPress security firm Defiant warns.

<https://www.securityweek.com/1-million-wordpress-sites-impacted-by-exploited-plugin-vulnerability/>

Click above link to read more.

[Back to top](#)

ChatGPT is about to revolutionize cybersecurity

Unless you purposely avoid social media or the internet completely, you've likely heard about a new AI model called ChatGPT, which is currently open to the public for testing. This allows cybersecurity professionals like me to see how it might be useful to our industry.

<https://venturebeat.com/security/chatgpt-is-about-to-revolutionize-cybersecurity/>

Click above link to read more.

[Back to top](#)

Lessons from 'Star Trek: Picard' – a cybersecurity expert explains how a sci-fi series illuminates today's threats

Editor's note: This article contains plot spoilers.

Society's understanding of technology and cybersecurity often is based on simple stereotypes and sensational portrayals in the entertainment media. I've written about how certain scenarios are entertaining but misleading. Think of black-clad teenage hackers prowling megacities challenging corporate villains. Or think of counterintelligence specialists repositioning a satellite from the back of a surveillance van via a phone call.

<https://theconversation.com/lessons-from-star-trek-picard-a-cybersecurity-expert-explains-how-a-sci-fi-series-illuminates-todays-threats-204433>

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.

