

**May 30, 2023**

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

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

🍁 [Few answers in norther medical school cyber attack](#)

🍁 [More Canadian privacy authorities investigating ChatGPT's use of personal information](#)

🍁 [Chinese hackers targeted U.S. infrastructure, security agencies warn](#)

🍁 ['Foreseeable' cyberattack on N.L. health network hit majority of province: report](#)

[Hackers attempt to sell personal data of 1.5 million women](#)

[Minister attacks Meta boss over Facebook message encryption plan](#)

[New PowerExchange backdoor used in Iranian cyber attack on UAE government](#)

[Predator Android Spyware: researchers uncover new data theft capabilities](#)

[Hyundais, Kias remain easy targets as concerns grow over auto cybersecurity](#)

[Ransomware gangs increasingly 'professional' - WithSecure report](#)

[The risks of using ChatGPT-like services](#)

[Hackers selling access to school IT systems, cyber security firm says](#)

---

### **Few answers in northern medical school cyber attack**

There are still more questions than answers following a cyber attack at the Northern Ontario School of Medicine.

<https://northernontario.ctvnews.ca/few-answers-in-northern-medical-school-cyber-attack-1.6416671>

*Click above link to read more.*

[Back to top](#)

---

## **More Canadian privacy authorities investigating ChatGPT's use of personal information**

Federal and provincial privacy authorities in Canada are pursuing a joint investigation into OpenAI, the company that makes ChatGPT, after receiving a complaint about the firm's disclosure of personal information.

<https://www.cbc.ca/news/canada/british-columbia/canada-privacy-investigation-chatgpt-1.6854468>

*Click above link to read more.*

[Back to top](#)

---

## **Chinese hackers targeted U.S. infrastructure, security agencies warn**

State-sponsored hackers from China have been targeting U.S. critical infrastructure, cybersecurity officials from around the world — including Canada — warned Wednesday in a co-ordinated effort to root out the perpetrators.

<https://www.cbc.ca/news/politics/chinese-hackers-targeting-infrastructure-1.6853667>

*Click above link to read more.*

[Back to top](#)

---

## **'Foreseeable' cyberattack on N.L. health network hit majority of province: report**

The ransomware attack that hit Newfoundland and Labrador's health-care IT systems in 2021 was "almost an inevitability" and likely resulted in the theft of personal data from the "vast majority" of the province's population, says a report released Wednesday.

<https://atlantic.ctvnews.ca/foreseeable-cyberattack-on-n-l-health-network-hit-majority-of-province-report-1.6411131>

*Click above link to read more.*

[Back to top](#)

---

## **Hackers attempt to sell personal data of 1.5 million women**

The personal information of more than 1.5 million women has been put up for sale on the dark web following an alleged data breach of Indian lingerie brand Zivame.

<https://www.cshub.com/attacks/news/hackers-attempt-to-sell-personal-data-of-15-million-women>

*Click above link to read more.*

[Back to top](#)

---

## **Minister attacks Meta boss over Facebook message encryption plan**

A government minister has attacked Meta boss Mark Zuckerberg for the "extraordinary moral choice" to roll out encryption in Facebook messages.

<https://www.bbc.com/news/technology-65686989>

*Click above link to read more.*

[Back to top](#)

---

## **New PowerExchange backdoor used in Iranian cyber attack on UAE government**

An unnamed government entity associated with the United Arab Emirates (U.A.E.) was targeted by a likely Iranian threat actor to breach the victim's Microsoft Exchange Server with a "simple yet effective" backdoor dubbed PowerExchange.

<https://thehackernews.com/2023/05/new-powerexchange-backdoor-used-in.html>

*Click above link to read more.*

[Back to top](#)

---

## **Predator Android Spyware: researchers uncover new data theft capabilities**

Security researchers have shared a deep dive into the commercial Android spyware called Predator, which is marketed by the Israeli company Intellexa (previously Cytrox).

<https://thehackernews.com/2023/05/predator-android-spyware-researchers.html>

*Click above link to read more.*

[Back to top](#)

---

## **Hyundais, Kias remain easy targets as concerns grow over auto cybersecurity**

Nearly three months ago, Hyundai and Kia unveiled software that was designed to thwart an epidemic of thefts of their vehicles, caused by a security flaw that was exposed on TikTok and other social media sites.

<https://www.10tv.com/article/news/local/hyundais-kias-remain-easy-targets-concerns-grow-over-auto-cybersecurity/530-1c0a2d0c-31b2-458b-80aa-0bb04fbe5ae4>

*Click above link to read more.*

[Back to top](#)

---

## **Ransomware gangs increasingly 'professional' - WithSecure report**

The success of ransomware gangs has spurred a significant trend of professionalisation amongst cyber criminals, where different groups develop specialised services to offer one another, according to a new report from WithSecure (formerly known as F-Secure Business).

<https://securitybrief.com.au/story/ransomware-gangs-increasingly-professional-withsecure-report>

*Click above link to read more.*

[Back to top](#)

---

## **The risks of using ChatGPT-like services**

ChatGPT and other AI/machine learning (ML) platforms have recently captured our attention and imagination, amazing even luddites with recent leaps forward and the potential applications of this technology.

<https://www.cpomagazine.com/cyber-security/the-risks-of-using-chatgpt-like-services/>

*Click above link to read more.*

[Back to top](#)

---

## **Hackers selling access to school IT systems, cyber security firm says**

A cyber security firm says hackers are selling access to IT systems at hundreds of New Zealand schools and tertiary institutes, as well as stolen personal data from thousands of staff and students.

<https://www.rnz.co.nz/news/national/490864/hackers-selling-access-to-school-it-systems-cyber-security-firm-says>

*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](mailto: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.

