

**July 4, 2023**

Challenge yourself with our [Malvertising Quiz!](#)

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

🍁 [HHS among targets in government hacking attack](#)

🍁 [Canada cyberspy agency blocked trillions of 'malicious actions' against feds last year](#)

🍁 [Indigo lost \\$50M last year, in large part due to February cyberattack](#)

🍁 [Cybersecurity incident at Suncor knocks Canadian gas stations offline](#)

🍁 [Endpoint security in the hybrid era](#)

[ThirdEye infostealer poses new threat to Windows users](#)

[Dallas city council approves \\$4 million contract for cybersecurity monitoring](#)

[Fluhorse: Flutter-based Android malware targets credit cards and 2FA codes](#)

[Pro-Russia DDoSia hacktivist project sees 2,400% membership increase](#)

[Evasive Meduza Stealer targets 19 password managers and 76 crypto wallets](#)

[Why cyberpsychology is such an important part of effective cybersecurity](#)

[Microsoft denies data breach—Anonymous Sudan claims 30 million customer accounts stolen](#)

---

## **HHS among targets in government hacking attack**

The Department of Health and Human Services (HHS) is among several federal agencies that were impacted by a global cyberattack that exploited a software vulnerability.

<https://thehill.com/policy/cybersecurity/4073588-hhs-among-targets-in-government-hacking-attack/>

*Click above link to read more.*

[Back to top](#)

---

## **Canada cyberspy agency blocked trillions of 'malicious actions' against feds last year**

In the last year, Canada's cyberspy agency blocked on average 6.3 billion "malicious actions" a day against the federal government, and received ministerial authorization to conduct more active foreign cyber operations than ever before, a new report reveals.

<https://www.ctvnews.ca/politics/canada-cyberspy-agency-blocked-trillions-of-malicious-actions-against-feds-last-year-1.6461213?autoPlay=true>

*Click above link to read more.*

[Back to top](#)

---

## **Indigo lost \$50M last year, in large part due to February cyberattack**

Indigo lost \$50 million in its last fiscal year as its highly publicized cybersecurity incident walloped what was otherwise a profitable year, the book retailer said Wednesday.

<https://www.cbc.ca/news/business/indigo-earnings-cyberattack-1.6891154>

*Click above link to read more.*

[Back to top](#)

---

## **Cybersecurity incident at Suncor knocks Canadian gas stations offline**

Suncor, a major Canadian energy company, has confirmed that a cyberattack has hit the systems of its gas station chain Petro-Canada. In some stations, paying cash is still the only option.

<https://cybernews.com/news/cyberattack-suncor-petro-canada/>

*Click above link to read more.*

[Back to top](#)

---

## **ThirdEye infostealer poses new threat to Windows users**

A new infostealer called ThirdEye has been observed in the wild, potentially targeting Windows users.

<https://www.infosecurity-magazine.com/news/thirdeye-infostealer-threat-windows/>

*Click above link to read more.*

[Back to top](#)

---

## **Endpoint security in the hybrid era**

Our world has changed; hybrid work is here to stay. According to Statistics Canada, at the end of last summer 28 per cent of all Canadian workers and 47 per cent of professional services workers were hybrid. Many people have embraced the flexibility and work-life balance benefits that come with hybrid work.

<https://www.itworldcanada.com/blog/endpoint-security-in-the-hybrid-era/541632>

*Click above link to read more.*

[Back to top](#)

---

## **Dallas city council approves \$4 million contract for cybersecurity monitoring**

Still recovering from a May ransomware attack that closed a number of vital city services, Dallas is putting up \$4 million for an improved cyber-security system.

<https://www.audacy.com/krlD/news/local/dallas-city-council-approves-usd4-million-cybersecurity>

*Click above link to read more.*

[Back to top](#)

---

## **Fluhorse: Flutter-based Android malware targets credit cards and 2FA codes**

Cybersecurity researchers have shared the inner workings of an Android malware family called Fluhorse.

<https://thehackernews.com/2023/06/fluhorse-flutter-based-android-malware.html>

*Click above link to read more.*

[Back to top](#)

---

## **Pro-Russia DDoSia hacktivist project sees 2,400% membership increase**

The pro-Russia crowdsourced DDoS (distributed denial of service) project, 'DDoSia,' has seen a massive 2,400% growth in less than a year, with over ten thousand people helping conduct attacks on Western organizations.

<https://www.bleepingcomputer.com/news/security/pro-russia-ddosia-hacktivist-project-sees-2-400-percent-membership-increase/>

*Click above link to read more.*

[Back to top](#)

---

## **Evasive Meduza Stealer targets 19 password managers and 76 crypto wallets**

In yet another sign of a lucrative crimeware-as-a-service (CaaS) ecosystem, cybersecurity researchers have discovered a new Windows-based information stealer called Meduza Stealer that's actively being developed by its author to evade detection by software solutions.

<https://thehackernews.com/2023/07/evasive-meduza-stealer-targets-19.html>

*Click above link to read more.*

[Back to top](#)

---

## **Why cyberpsychology is such an important part of effective cybersecurity**

Insight into how the human mind works can help combat the evils of social engineering, boosting the fight against phishing and other mind-manipulation techniques.

<https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html>

*Click above link to read more.*

[Back to top](#)

---

## **Microsoft denies data breach—Anonymous Sudan claims 30 million customer accounts stolen**

Anonymous Sudan recently announced on Telegram the sale of a valuable Microsoft user data collection with a price tag of \$50,000 for the full database.

<https://cybersecuritynews.com/microsoft-denies-data-breach/>

*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.

