

**May 2, 2023**

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

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

🍁 [Ontario casinos faces long road to recovery after ransomware attack, expert says](#)

🍁 [B.C. senior defrauded of \\$7.5M in crypto scam, police say](#)

🍁 [Yellow Pages Canada confirms cyber attack as Black Basta leaks data](#)  
[Chinese hackers using MgBot malware to target international NGOs in Mainland China](#)

[Charming Kitten's new BellaCiao malware discovered in multi-country attacks](#)

[Google gets court order to take down CryptBot that infected over 670,000 computers](#)

[Hardenhuish School in Chippenham hit by cyber attack](#)

[CommScope employees left in the dark after ransomware attack](#)

[Vietnamese threat actor infects 500,000 devices using 'Malverposting' tactics](#)

[APT28 targets Ukrainian government entities with fake "Windows Update" emails](#)

[Clop, LockBit leveraging 3 known vulnerabilities in healthcare ransomware attacks, HHS warns](#)

[New Atomic macOS malware steals keychain passwords and crypto wallets](#)

[South Korea, US agree to cooperate on cybersecurity and combating North Korean digital heists](#)

---

**Ontario casinos faces long road to recovery after ransomware attack, expert says**

Several casinos in Ontario remain closed nearly two weeks after a cyberattack, with no official reopening date.

<https://barrie.ctvnews.ca/ontario-casinos-faces-long-road-to-recovery-after-ransomware-attack-expert-says-1.6375498>

*Click above link to read more.*

[Back to top](#)

---

### **B.C. senior defrauded of \$7.5M in crypto scam, police say**

A B.C. senior was defrauded of \$7.5 million in a months-long cryptocurrency scam, according to authorities.

<https://bc.ctvnews.ca/b-c-senior-defrauded-of-7-5m-in-crypto-scam-police-say-1.6374535#:~:text=A%20B.C.%20senior%20was%20defrauded,the%20detachment%20has%20ever%20investigated.%22>

*Click above link to read more.*

[Back to top](#)

---

### **Yellow Pages Canada confirms cyber attack as Black Basta leaks data**

Yellow Pages Group, a Canadian directory publisher has confirmed to BleepingComputer that it has been hit by a cyber attack.

<https://www.bleepingcomputer.com/news/security/yellow-pages-canada-confirms-cyber-attack-as-black-basta-leaks-data/>

*Click above link to read more.*

[Back to top](#)

---

### **Chinese hackers using MgBot malware to target international NGOs in Mainland China**

The advanced persistent threat (APT) group referred to as Evasive Panda has been observed targeting an international non-governmental organization (NGO) in Mainland China with malware delivered via update channels of legitimate applications like Tencent QQ.

<https://thehackernews.com/2023/04/chinese-hackers-using-mgbot-malware-to.html>

*Click above link to read more.*

[Back to top](#)

---

## **Charming Kitten's new BellaCiao malware discovered in multi-country attacks**

The prolific Iranian nation-state group known as Charming Kitten is actively targeting multiple victims in the U.S., Europe, the Middle East and India with a novel malware dubbed BellaCiao, adding to its ever-expanding list of custom tools.

<https://thehackernews.com/2023/04/charming-kittens-new-bellaciao-malware.html>

*Click above link to read more.*

[Back to top](#)

---

## **Google gets court order to take down CryptBot that infected over 670,000 computers**

Google on Wednesday said it obtained a temporary court order in the U.S. to disrupt the distribution of a Windows-based information-stealing malware called CryptBot and "decelerate" its growth.

<https://thehackernews.com/2023/04/google-gets-court-order-to-take-down.html>

*Click above link to read more.*

[Back to top](#)

---

## **Hardenhuish School in Chippenham hit by cyber attack**

Hardenhuish School in Chippenham, Wiltshire, has been hit by a ransomware attack, where hackers gain access to IT systems and demand a ransom in return for restored access.

<https://www.bbc.com/news/uk-england-wiltshire-65411450>

*Click above link to read more.*

[Back to top](#)

---

## **CommScope employees left in the dark after ransomware attack**

CommScope employees say they haven't heard from executives in over a week about how the company is responding to a ransomware attack, which allowed hackers to steal reams of corporate and employee data from its systems.

<https://techcrunch.com/2023/04/27/commscope-ransomware-data/>

*Click above link to read more.*

[Back to top](#)

---

## **Vietnamese threat actor infects 500,000 devices using 'Malverposting' tactics**

A Vietnamese threat actor has been attributed as behind a "malverposting" campaign on social media platforms to infect over 500,000 devices worldwide over the past three months to deliver variants of information stealers such as S1deload Stealer and SYS01stealer.

<https://thehackernews.com/2023/05/vietnamese-threat-actor-infects-500000.html>

*Click above link to read more.*

[Back to top](#)

---

## **APT28 targets Ukrainian government entities with fake "Windows Update" emails**

The Computer Emergency Response Team of Ukraine (CERT-UA) has warned of cyber attacks perpetrated by Russian nation-state hackers targeting various government bodies in the country.

The email messages come with the subject line "Windows Update" and purportedly contain instructions in the Ukrainian language to run a PowerShell command under the pretext of security updates.

<https://thehackernews.com/2023/05/apt28-targets-ukrainian-government.html>

*Click above link to read more.*

[Back to top](#)

---

## **Clop, LockBit Leveraging 3 Known Vulnerabilities in Healthcare Ransomware Attacks, HHS Warns**

Two Ransomware-as-a-Service groups, Clop and LockBit, have been leveraging known vulnerabilities in Fortra's GoAnywhere MFT solution and installations of PaperCut to target healthcare.

<https://healthitsecurity.com/news/clop-lockbit-leveraging-3-known-vulnerabilities-in-healthcare-ransomware-attacks-hhs-warns>

*Click above link to read more.*

[Back to top](#)

---

## **New Atomic macOS Malware Steals Keychain Passwords and Crypto Wallets**

Threat actors are advertising a new information stealer for the Apple macOS operating system called Atomic macOS Stealer (or AMOS) on Telegram for \$1,000 per month, joining the likes of MacStealer.

<https://thehackernews.com/2023/04/new-atomic-macos-stealer-can-steal-your.html>

*Click above link to read more.*

[Back to top](#)

---

## **South Korea, US agree to cooperate on cybersecurity and combating North Korean digital heists**

South Korea and the U.S. announced Wednesday that they have committed to signing a cybersecurity cooperation agreement, citing concerns about North Korea funding its weapons programs with the proceeds of cybercrime.

<https://therecord.media/south-korea-us-agree-to-cooperate-cybersecurity-north-korea>

*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.

