

June 20, 2023

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

🍁 [The inside story of how N.L. health officials failed to act before a ransomware gang struck](#)

🍁 [Canadian firms slow in responding to cyber attacks, report suggests](#)

🍁 [N.S. identifies thousands more victims of global data hack, including school workers](#)

[From ChatGPT to HackGPT](#)

[Warning: GravityRAT Android trojan steals WhatsApp backups and deletes files](#)

[GameAbove elevates Eastern Michigan University's Cybersecurity Program with a \\$1.6M gift to its College of Engineering and Technology](#)

[US government agencies hit in global hacking spree](#)

[Cyberattacks on renewables: Europe power sector's dread in chaos of war](#)

[New report reveals Shuckworm's long-running intrusions on Ukrainian organizations](#)

[Reddit hackers warn of February breach data leak](#)

[State-backed hackers employ advanced methods to target Middle Eastern and African governments](#)

[BrutePrint: Bypassing smartphone fingerprint protection](#)

[Over 100,000 stolen ChatGPT Account Credentials sold on Dark Web Marketplaces](#)

The inside story of how N.L. health officials failed to act before a ransomware gang struck

Many numbers have been linked to the cyberattack on Newfoundland and Labrador's health-care system in the fall of 2021.

<https://www.cbc.ca/news/canada/newfoundland-labrador/nl-ransomware-attack-report-in-depth-1.6860899>

Click above link to read more.

[Back to top](#)

Canadian firms slow in responding to cyber attacks, report suggests

It can take Canadian organizations up to 48 days to detect and recover from a cyber attack, according to a new survey of infosec professionals.

<https://www.itbusiness.ca/news/canadian-firms-slow-in-responding-to-cyber-attacks-report-suggests/125297>

Click above link to read more.

[Back to top](#)

N.S. identifies thousands more victims of global data hack, including school workers

Nova Scotia's cybersecurity minister says his department has identified thousands more people affected by a recent global data breach.

<https://www.cbc.ca/news/canada/nova-scotia/moveit-hack-nova-scotia-cybersecurity-breach-1.6876382>

Click above link to read more.

[Back to top](#)

From ChatGPT to HackGPT

The emergence and continued development of artificial intelligence (AI) is creating endless new possibilities in the world of cybersecurity. Threats and weaknesses can be detected faster and more accurately, and the speed of action of security teams is faster than ever with AI. This is badly needed because as with all new resources that help humanity move forward, new techniques are also eagerly sought after by cybercriminals.

<https://blogs.blackberry.com/en/2023/06/from-chatgpt-to-hackgpt>

Click above link to read more.

[Back to top](#)

Warning: GravityRAT Android trojan steals WhatsApp backups and deletes files

An updated version of an Android remote access trojan dubbed GravityRAT has been found masquerading as messaging apps BingeChat and Chatico as part of a narrowly targeted campaign since June 2022.

<https://thehackernews.com/2023/06/warning-gravityrat-android-trojan.html>

Click above link to read more.

[Back to top](#)

GameAbove elevates Eastern Michigan University's Cybersecurity Program with a \$1.6M gift to its College of Engineering and Technology

GameAbove at Eastern Michigan University, an alumni-led philanthropic group advancing academic and athletic programs, announces a \$1.6 million gift to the university's College of Engineering and Technology (GACET). The new commitment will support the launch of a Cybersecurity for Embedded Systems initiative, enhance offerings within cybersecurity and the Internet of Things, including research in cybersecurity for vehicles and mobility, and establish a dedicated Cybersecurity Certificate Program that caters to students and business professionals alike.

<https://www.newswire.ca/news-releases/gameabove-elevates-eastern-michigan-university-s-cybersecurity-program-with-a-1-6m-gift-to-its-college-of-engineering-and-technology-833379142.html>

Click above link to read more.

[Back to top](#)

US government agencies hit in global hacking spree

The U.S. government has been hit in a global hacking campaign that exploited a vulnerability in widely used software but does not expect it to have significant impact, the nation's cyber watchdog agency said on Thursday.

<https://www.reuters.com/world/us/us-government-agencies-hit-global-cyber-attack-cnn-2023-06-15/>

Click above link to read more.

[Back to top](#)

Cyberattacks on renewables: Europe power sector's dread in chaos of war

Saboteurs target a nation leading the world in clean energy. They hack into vulnerable wind and solar power systems. They knock out digitalized energy grids. They wreak havoc.

<https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/>

Click above link to read more.

[Back to top](#)

New report reveals Shuckworm's long-running intrusions on Ukrainian organizations

The Russian threat actor known as Shuckworm has continued its cyber assault spree against Ukrainian entities in a bid to steal sensitive information from compromised environments.

<https://thehackernews.com/2023/06/new-report-reveals-shuckworms-long.html>

Click above link to read more.

[Back to top](#)

Reddit hackers warn of February breach data leak

Reddit attackers claim to have stolen 80 GB of Reddit data. They want \$4.5 million in ransom and Reddit to ditch its API pricing changes.

<https://cybernews.com/news/reddit-data-breach-alphv-blackcat/>

Click above link to read more.

[Back to top](#)

State-backed hackers employ advanced methods to target Middle Eastern and African governments

Governmental entities in the Middle East and Africa have been at the receiving end of sustained cyber-espionage attacks that leverage never-before-seen and rare credential theft and Exchange email exfiltration techniques.

<https://thehackernews.com/2023/06/state-backed-hackers-employ-advanced.html>

Click above link to read more.

[Back to top](#)

BrutePrint: Bypassing smartphone fingerprint protection

Fingerprint recognition is believed to be a fairly secure authentication method. Publications on different ways to trick the fingerprint sensor do pop up now and again, but all the suggested methods one way or another boil down to physical imitation of the phone owner's finger — whether using a silicone pad or conductive ink printout.

https://www.kaspersky.com/blog/fingerprint-brute-force-android/48303/?reseller=gb_kdaily-sm_awarn_ona_smm_all_b2c_some_sma_sm-team&utm_source=twitter&utm_medium=social&utm_campaign=uk_kdaily_db0077&utm_content=sm-post&utm_term=uk_twitter_organic_d36krxyne377mof

Click above link to read more.

[Back to top](#)

Over 100,000 stolen ChatGPT Account Credentials sold on Dark Web Marketplaces

Over 100,000 Stolen ChatGPT Account Credentials Sold on Dark Web Marketplaces

Over 101,100 compromised OpenAI ChatGPT account credentials have found their way on illicit dark web marketplaces between June 2022 and May 2023, with India alone accounting for 12,632 stolen credentials.

<https://thehackernews.com/2023/06/over-100000-stolen-chatgpt-account.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.

