August 1, 2023

Challenge yourself with our Cryptocons Quiz!

This past week's stories:

- **Saskatoon woman loses $10,000 after scammers hijack iPad, trick her into withdrawing cash**
- **US Senator demands feds investigate Microsoft over China email and SolarWinds hack**
- **Romance scammer jailed for conning Holocaust survivor out of $2.8M**
- **New malvertising campaign distributing trojanized IT tools via Google and Bing Search ads**
- **Kenya cyber-attack: Why is eCitizen down?**
- **Hackers exploit Windows search feature to execute malware on infected systems**
- **AVRecon botnet leveraging compromised routers to fuel illegal proxy service**
- **Cybersecurity agencies warn against IDOR bugs exploited for data breaches**
- **New AI tool 'FraudGPT' emerges, tailored for sophisticated attacks**
- **How ML can help companies mitigate cyber threats**
- **Spyware app compromised over 60,000 Android devices to steal sensitive data**
- **IBM Security Verify Access flaw let attacker launch phishing attacks**

Saskatoon woman loses $10,000 after scammers hijack iPad, trick her into withdrawing cash

A Saskatoon senior is out $10,000 after an elaborate financial scam, and she's warning the public to be alert for this new type of trick.

https://saskatoon.ctvnews.ca/saskatoon-woman-loses-10-000-after-scammers-hijack-ipad-trick-her-into-withdrawing-cash-1.6498988

Click above link to read more.

Back to top

US Senator demands feds investigate Microsoft over China email and SolarWinds hack

Oregon Senator Ron Wyden is pushing three federal agencies to hold Microsoft accountable for security failures that led to two major hacking campaigns impacting multiple government offices – a recently discovered Chinese-led cyberespionage campaign and the infamous 2020 SolarWinds hack.

https://cybernews.com/security/us-senator-cisa-doj-ftc-microsoft-investigation-china-email-solarwinds-hack/

Click above link to read more.

Back to top

Romance scammer jailed for conning Holocaust survivor out of $2.8M

A woman from Florida has been jailed for 51 months for defrauding a Holocaust survivor out of $2.8 million in an online romance scam.

https://cybernews.com/news/romance-scammer-jailed-holocaust/

Click above link to read more.

Back to top

New malvertising campaign distributing trojanized IT tools via Google and Bing Search ads

A new malvertising campaign has been observed leveraging ads on Google Search and Bing to target users seeking IT tools like AnyDesk, Cisco AnyConnect VPN, and WinSCP, and trick them into downloading trojanized installers with an aim to breach enterprise networks and likely carry out future ransomware attacks.

https://thehackernews.com/2023/07/new-malvertising-campaign-distributing.html

Click above link to read more.

Back to top

Kenya cyber-attack: Why is eCitizen down?

Kenya's government has been fighting off a huge cyber-attack that has affected services on a key government online platform for almost a week. There are still questions over who was behind it and what was the motive.

https://www.bbc.com/news/world-africa-66337573

Click above link to read more.

Back to top

Hackers exploit Windows search feature to execute malware on infected systems

Malware authors persistently seek novel approaches to exploit unsuspecting users in the active cyber threat landscape.

https://cybersecuritynews.com/hackers-exploit-windows-search/

Click above link to read more.

Back to top

AVRecon botnet leveraging compromised routers to fuel illegal proxy service

More details have emerged about a botnet called AVRecon, which has been observed making use of compromised small office/home office (SOHO) routers as part of a multi-year campaign active since at least May 2021.

https://thehackernews.com/2023/07/avrecon-botnet-leveraging-compromised.html

Click above link to read more.

Back to top

Cybersecurity agencies warn against IDOR bugs exploited for data breaches

Cybersecurity agencies in Australia and the U.S. have published a joint cybersecurity advisory warning against security flaws in web applications that could be exploited by malicious actors to orchestrate data breach incidents and steal confidential data.

https://thehackernews.com/2023/07/cybersecurity-agencies-warn-against.html

Click above link to read more.

Back to top

New AI tool 'FraudGPT' emerges, tailored for sophisticated attacks

Following the footsteps of WormGPT, threat actors are advertising yet another cybercrime generative artificial intelligence (AI) tool dubbed FraudGPT on various dark web marketplaces and Telegram channels.

https://thehackernews.com/2023/07/new-ai-tool-fraudgpt-emerges-tailored.html

Click above link to read more.

Back to top

How ML can help companies mitigate cyber threats

In today's interconnected world, the prevalence of cyber threats has grown exponentially, posing significant challenges to businesses of all sizes. Cyberattacks jeopardise sensitive data and inflict financial losses and damage to a company's reputation.

https://www.analyticsinsight.net/how-ml-can-help-companies-mitigate-cyber-threats/

Click above link to read more.

Back to top

Spyware app compromised over 60,000 Android devices to steal sensitive data

Spywares are software that is used as a surveillance application to collect sensitive information from victims and send it to the person who installed the application.

https://cybersecuritynews.com/spyware-app-compromised/

Click above link to read more.

Back to top

IBM Security Verify Access flaw let attacker launch phishing attacks

An Open-redirect vulnerability was discovered by IBM, which could allow threat actors to spoof the original URL of IBM Security Verify Access to lure victims into a malicious website and steal sensitive information.

https://cybersecuritynews.com/ibm-security-verify-access-flaw/

Click above link to read more.

Back to top

---

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