September 6, 2022

Challenge yourself with our Ransomware Quiz!

This past week's stories:

- **Rogers Cybersecure Catalyst at Toronto Metropolitan University launches CyberStart Canada, a gamified cybersecurity learning experience for youth**
- **'Emotional part of it I think was the key': Newmarket man warns others of grandparent scam after he lost 100K**
- **Businesses spending higher percentage of technology budgets on cybersecurity, Sophos research reveals**
- **Hackers target politicians with fake news website**
- **Multifactor authentication has its limits, but don't blame the technology**
- **Electricity grid to be future ready, insulated from cyber attacks: RK Singh**
- **Montenegro blames criminal gang for cyber attacks on government**
- **Microsoft discloses 'high-severity' TikTok vulnerability**
- **Google Chrome bug lets sites silently overwrite system clipboard content**
- **Researchers detail emerging cross-platform BianLian ransomware attacks**
- **Samsung says hackers obtained some customer data in newly disclosed breach**
- **Okta CEO pushes for passwordless future in wake of phishing attacks**
- **TikTok denies security breach after hackers leak user data, source code**
- **New Worok cyber-espionage group targets governments, high-profile firms**

Rogers Cybersecure Catalyst at Toronto Metropolitan University launches CyberStart Canada, a gamified cybersecurity learning experience for youth

Today, Rogers Cybersecure Catalyst, Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity, launched CyberStart Canada. The new youth-focused learning experience seeks to increase cyber knowledge and safety among high school girls and close the gender gap in cybersecurity.

Funded by Public Safety Canada's Cyber Security Cooperation Program, together with support from SANS Institute, Cyberstart Canada will use gamification to measurably improve cyber-related knowledge and skills, and increase interest in cybersecurity careers among an engaged community of girls and young women across Canada.

https://www.newswire.ca/news-releases/rogers-cybersecure-catalyst-at-toronto-metropolitan-university-launches-cyberstart-canada-a-gamified-cybersecurity-learning-experience-for-youth-817913458.html

Click above link to read more.

Back to top

'Emotional part of it I think was the key': Newmarket man warns others of grandparent scam after he lost 100K

A Newmarket senior is warning others after he fell victim to a grandparent scam, also known as an emergency scam, and lost $100,000.

The victim, Nicky (not his real name), is an 81-year-old grandfather who reported to the York Regional Police that he was scammed out of $100,000 between March and May, 2022.

https://www.thestar.com/local-newmarket/news/crime/2022/09/01/emotional-part-of-it-i-think-was-the-key-newmarket-man-warns-others-of-grandparent-scam-after-he-lost-100k.html

Click above link to read more.

Back to top

Businesses spending higher percentage of technology budgets on cybersecurity, Sophos research reveals

Sophos, a global leader in next-generation cybersecurity, today released additional findings from its survey report, The Future of Cybersecurity in Asia Pacific and Japan, in collaboration with Tech Research Asia (TRA), revealing businesses are increasingly prioritising budget for cybersecurity. In 2022, 11 per cent of technology budgets across India are dedicated to cybersecurity.

Organisations in India have identified threat hunting as a key consideration for strengthening cybersecurity defences. Most organisations (95 per cent) undertook threat hunting to bolster their cybersecurity capabilities in 2021; of those that did, 85 per cent stated the approach is critical or important to their company’s overall cybersecurity capabilities.

https://www.apnnews.com/businesses-spending-higher-percentage-of-technology-budgets-on-cybersecurity-sophos-research-reveals/

Click above link to read more.

Back to top

Hackers target politicians with fake news website

Hackers created a fake news website to harvest data from Australian government officials, journalists and others, according to a top US security company.

The targets received emails claiming to be from Australian news outlets, which linked them to a malicious website.

https://www.bbc.com/news/62728084

Click above link to read more.

Back to top

Multifactor authentication has its limits, but don't blame the technology

Multifactor authentication is widely regarded as a must-have among cybersecurity professionals and authorities, but it's not always a quick fix.

Threat actors can still evade and even exploit MFA via phishing or social engineering attacks, as evidenced by the persistent and widespread text-message phishing campaign dubbed Oktapus or Scatter Swine.

Technology companies, telecommunications providers and organizations or individuals linked to cryptocurrency have been targeted since the attacks began in March. The adversary compromised almost 10,000 user credentials across 136 organizations, according to Group-IB, sometimes targeting employees at specific companies once access was gained directly or via third-party vendors.

https://www.cybersecuritydive.com/news/multifactor-authentication-limits/631046/

Click above link to read more.

Back to top

Electricity grid to be future ready, insulated from cyber attacks: RK Singh

India's power network will soon be more future-ready and insulated from cyber attacks with the provision of routine inspections and timely action under the Electricity Amendment Bill, Union Power Minister RK Singh said.

Cyber attract threat has been an issue and the government did all what it takes to address that. Now through the Electricity Amendment Bill 2022, the power ministry has made a provision for inspection of the national electricity grid for maintaining cyber hygiene in the network.

https://www.business-standard.com/article/economy-policy/electricity-grid-to-be-future-ready-insulated-from-cyber-attacks-rk-singh-122090100961_1.html

Click above link to read more.

Back to top

Montenegro blames criminal gang for cyber attacks on government

Montenegro on Wednesday blamed a criminal group called Cuba ransomware for cyber attacks that have hit its government digital infrastructure since last week, described by officials as unprecedented.

Public Administration Minister Maras Dukaj told state television the group had created a special virus for the attack called Zerodate, with 150 work stations in 10 state institutions becoming infected.

https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/

Click above link to read more.

Back to top

Microsoft discloses 'high-severity' TikTok vulnerability

Microsoft disclosed a verification bypass vulnerability in TikTok's Android application, raising concerns about the security and functionality of the popular social media app.

In a blog post Wednesday, Microsoft detailed the TikTok vulnerability, tracked as CVE-2022-28799, which could enable threat actors to hijack accounts and publicize private videos, send messages and upload videos under the users' accounts. While TikTok fixed the flaw and Microsoft confirmed it did not observe in-the-wild exploitation, the vulnerability heightened concerns over access to private data as well as the in-app browser functionality.

https://www.techtarget.com/searchsecurity/news/252524495/Microsoft-discloses-high-severity-TikTok-vulnerability

Click above link to read more.

Back to top

Google Chrome bug lets sites silently overwrite system clipboard content

A "major" security issue in the Google Chrome web browser, as well as Chromium-based alternatives, could allow malicious web pages to automatically overwrite clipboard content without requiring any user consent or interaction by simply visiting them.

The clipboard poisoning attack is said to have been accidentally introduced in Chrome version 104, according to developer Jeff Johnson.

https://thehackernews.com/2022/09/google-chrome-bug-lets-sites-silently.html

Click above link to read more.

Back to top

Researchers detail emerging cross-platform BianLian ransomware attacks

The operators of the emerging cross-platform BianLian ransomware have increased their command-and-control (C2) infrastructure this month, a development that alludes to an increase in the group's operational tempo.

BianLian, written in the Go programming language, was first discovered in mid-July 2022 and has claimed 15 victim organizations as of September 1, cybersecurity firm [redacted] said in a report shared with The Hacker News.

https://thehackernews.com/2022/09/researchers-detail-emerging-cross.html

Click above link to read more.

Back to top

Samsung says hackers obtained some customer data in newly disclosed breach

Samsung has disclosed another cybersecurity incident. While an intrusion earlier this year led to hackers getting their hands on Galaxy source code, this time around, attackers obtained some customers' personal information.

The company says that Social Security numbers, as well as credit and debit card numbers, were not accessed. However, the event "may have affected information such as name, contact and demographic information, date of birth and product registration information." It hasn't revealed how many people may have been affected. The company is notifying some customers directly via email.

https://finance.yahoo.com/news/samsung-data-breach-customer-personal-information-163502854.html

Click above link to read more.

Back to top

Okta CEO pushes for passwordless future in wake of phishing attacks

The persistent phishing campaign that tricked some Okta customers into sharing their credentials with a threat actor on spoofed sites earlier this month lends further credence to the need for a passwordless future, according to Okta CEO and Co-Founder Todd McKinnon.

“We need to move to having no password,” McKinnon said, describing it as Okta’s vision and a paramount need for its customers. Okta’s platform can help organizations meet that goal, but they have to apply the proper configurations, he said Wednesday on Okta’s earnings call for the fiscal second quarter, which ended July 31.

https://www.cybersecuritydive.com/news/okta-ceo-passwordless/631133/

Click above link to read more.

Back to top

TikTok denies security breach after hackers leak user data, source code

TikTok denies recent claims it was breached, and source code and user data were stolen, telling BleepingComputer that data posted to a hacking forum is "completely unrelated" to the company.

On Friday, a hacking group known as 'AgainstTheWest' created a topic on a hacking forum claiming to have breached both TikTok and WeChat. The user shared screenshots of an alleged database belonging to the companies, which they say was accessed on an Alibaba cloud instance containing data for both TikTok and WeChat users.

https://www.bleepingcomputer.com/news/security/tiktok-denies-security-breach-after-hackers-leak-user-data-source-code/

Click above link to read more.

Back to top

New Worok cyber-espionage group targets governments, high-profile firms

A newly discovered cyber-espionage group has been hacking governments and high-profile companies in Asia since at least 2020 using a combination of custom and existing malicious tools.

The threat group, tracked as Worok by ESET security researchers who first spotted it, has also attacked targets from Africa and the Middle East.

https://www.bleepingcomputer.com/news/security/new-worok-cyber-espionage-group-targets-governments-high-profile-firms/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer