January 17, 2023

Challenge yourself with our Cyber Security Resolutions Quiz!

This past week's stories:

- Why are there so many cyberattacks lately? An explainer on the rising trend
- As new AI ChatGPT earns hype, cybersecurity experts warn about potential malicious uses
- Progress made following Okanagan College cyberattack
- Royal Mail hit by Russia-linked ransomware attack
- Twitter says leaked emails not hacked from its systems
- IcedID malware strikes again: Active directory domain compromised in under 24 hours
- Companies warned to step up cyber security to become 'insurable'
- The big risk in the most popular, and aging, big tech default email programs
- Malware attack on CircleCI engineer's laptop leads to recent security incident
- Over 6K customer accounts breached, admits Norton LifeLock
- Raccoon and Vidar stealers spreading via massive network of fake cracked software
- Cisco issues warning for unpatched vulnerabilities in EoL business routers
- New backdoor created using leaked CIA's Hive malware discovered in the wild

---

Why are there so many cyberattacks lately? An explainer on the rising trend

A wave of high-profile cyberattacks has recently hit hospitals, businesses and organizations in Ontario, including the LCBO this week and Toronto's Hospital for Sick Children and Scouts Canada in December.

The Canadian Press spoke with cybersecurity experts about whether cyberattacks are on the rise, why they are happening, and what people and businesses can do to protect themselves.

https://globalnews.ca/news/9408198/why-are-there-so-many-cyberattacks-explainer/

Click above link to read more.

Back to top

As new AI ChatGPT earns hype, cybersecurity experts warn about potential malicious uses

As ChatGPT earns hype for its ability to solve complex problems, write essays, and perhaps help diagnose medical conditions, more nefarious uses of the chatbot are coming to light in dark corners of the internet.

Since its public beta launch in November, ChatGPT has impressed humans with its ability to imitate their writing — drafting resumes, crafting poetry, and completing homework assignments in a matter of seconds.

https://www.cbc.ca/news/science/chatgpt-cybercriminals-warning-1.6710854

Click above link to read more.

Back to top

Progress made following Okanagan College cyberattack

More Okanagan College computer systems are back up and running following a cyberattack that brought down network access.

"We've made good progress over the weekend and are pleased to confirm that more systems are operational and available to students and staff this morning following last week's outage," reads a statement from the college.

They said that guest Wi-Fi is live at all Okanagan College campuses, and ClassFinder is back online on the OC website, allowing students to check their course schedules and room locations.

https://globalnews.ca/news/9414131/progress-made-okanagan-college-cyberattack/

Click above link to read more.

Back to top

Royal Mail hit by Russia-linked ransomware attack

Severe disruption to Royal Mail's overseas deliveries has been caused by ransomware linked to Russian criminals, the BBC has been told.

The cyber-attack has affected the computer systems Royal Mail uses to despatch deliveries abroad.

https://www.bbc.com/news/business-64244121

Click above link to read more.

Back to top

Twitter says leaked emails not hacked from its systems

Twitter has denied that emails alleged to be linked to millions of its users' accounts were obtained using a hack.

In its first statement on the matter, it wrote "there is no evidence" the data came from a flaw in its systems.

https://www.bbc.com/news/technology-64243369

Click above link to read more.

Back to top

IcedID malware strikes again: Active directory domain compromised in under 24 hours

A recent IcedID malware attack enabled the threat actor to compromise the Active Directory domain of an unnamed target less than 24 hours after gaining initial access.

"Throughout the attack, the attacker followed a routine of recon commands, credential theft, lateral movement by abusing Windows protocols, and executing Cobalt Strike on the newly compromised host," Cybereason researchers said in a report published this week.

https://thehackernews.com/2023/01/icedid-malware-strikes-again-active.html

Click above link to read more.

Back to top

Companies warned to step up cyber security to become ‘insurable’

Businesses are at risk of finding that they are unable to secure cyber insurance cover as the volume of cyber attacks reaches new levels.

Companies are increasingly being required to put in place higher levels of cyber protection for their systems before they will be considered for cyber insurance.

https://www.computerweekly.com/news/252529132/Companies-warned-to-step-up-cyber-security-to-become-insurable

Click above link to read more.

Back to top

The big risk in the most popular, and aging, big tech default email programs

Back in January 2021, Microsoft announced that its software, specifically the software running some Microsoft Exchange servers, had been hacked by a criminal group sponsored by the Chinese government. Further, the company said, everyone using the software was vulnerable until it was patched.

All over the world, organizations of all sizes, including small businesses, scrambled to upload patches and to figure out if they’d been infiltrated. Despite the efforts, some were still ensnared; at least 200 ransomware attacks were attributed to the hack, with some businesses losing millions as they paid the criminals.

https://www.cnbc.com/2023/01/15/the-most-popular-big-tech-email-programs-are-old-and-vulnerable.html

Click above link to read more.

Back to top

Malware attack on CircleCI engineer's laptop leads to recent security incident

DevOps platform CircleCI on Friday disclosed that unidentified threat actors compromised an employee's laptop and leveraged malware to steal their two-factor authentication-backed credentials to breach the company's systems and data last month.

The CI/CD service CircleCI said the "sophisticated attack" took place on December 16, 2022, and that the malware went undetected by its antivirus software.

https://thehackernews.com/2023/01/malware-attack-on-circleci-engineers.html

Click above link to read more.

Back to top

Over 6K customer accounts breached, admits Norton LifeLock

Cyber-security services provider Norton LifeLock has been hit by a data breach where more than 6,000 of its customers had their accounts compromised.

The data breach may have allowed hackers to access their password managers, reports TechCrunch.

https://cio.economictimes.indiatimes.com/news/digital-security/over-6k-customer-accounts-breached-admits-norton-lifelock/97024815

Click above link to read more.

Back to top

Raccoon and Vidar stealers spreading via massive network of fake cracked software

A "large and resilient infrastructure" comprising over 250 domains is being used to distribute information-stealing malware such as Raccoon and Vidar since early 2020.

The infection chain "uses about a hundred of fake cracked software catalogue websites that redirect to several links before downloading the payload hosted on file share platforms, such as GitHub," cybersecurity firm SEKOIA said in an analysis published earlier this month.

https://thehackernews.com/2023/01/raccoon-and-vidar-stealers-spreading.html

Click above link to read more.

Back to top

Cisco issues warning for unpatched vulnerabilities in EoL business routers

Cisco has warned of two security vulnerabilities affecting end-of-life (EoL) Small Business RV016, RV042, RV042G, and RV082 routers that it said will not be fixed, even as it acknowledged the public availability of proof-of-concept (PoC) exploit.

The issues are rooted in the router's web-based management interface, enabling a remote adversary to sidestep authentication or execute malicious commands on the underlying operating system.

The most severe of the two is CVE-2023-20025 (CVSS score: 9.0), which is the result of improper validation of user input within incoming HTTP packets.

https://thehackernews.com/2023/01/cisco-issues-warning-for-unpatched.html

Click above link to read more.

Back to top

New backdoor created using leaked CIA's Hive malware discovered in the wild

Unidentified threat actors have deployed a new backdoor that borrows its features from the U.S. Central Intelligence Agency (CIA)'s Hive multi-platform malware suite, the source code of which was released by WikiLeaks in November 2017.

"This is the first time we caught a variant of the CIA Hive attack kit in the wild, and we named it xdr33 based on its embedded Bot-side certificate CN=xdr33," Qihoo Netlab 360's Alex Turing and Hui Wang said in a technical write-up published last week.

https://thehackernews.com/2023/01/new-backdoor-created-using-leaked-cias.html

Click above link to read more.

Back to top

OCIOSecurity@gov.bc.ca