November 1, 2022

Register for SECURITY DAY!

Challenge yourself with our Online Shopping Security Quiz

This past week's stories:

- **Cyber criminals may use new techniques, state sponsored threats to lure Canadians: agency**
- **Thomson Reuters collected and leaked at least 3TB of sensitive data**
- **These cybersecurity vulnerabilities are most popular with hackers right now - have you patched them?**
- **These dropper apps on Play Store targeting over 200 banking and cryptocurrency wallets**
- **New York Post hacked with offensive headlines targeting politicians**
- **Bed, Bath & Beyond confirms data breach following employee phishing attack**
- **Australian Defence Department caught up in ransomware attack**
- **DHL named most-spoofed brand in phishing**
- **First on CNN: US banks report more than $1 billion in potential ransomware payments in 2021**
- **Twitter's verification chaos is now a cybersecurity problem**
- **U.S. Treasury thwarted attack by Russian hacker group last month-official**
- **Hackers selling access to 576 corporate networks for $4 million**

Cyber criminals may use new techniques, state sponsored threats to lure Canadians: agency

The federal cybersecurity centre says criminals who hold data for ransom are expected to use new techniques _ such as threatening a target's partners or clients _ to increase their chances of receiving payment.

In its threat forecast for 2023-24, the Canadian Centre for Cyber Security says cybercrime continues to be the online activity most likely to affect Canadians and their organizations.

https://globalnews.ca/news/9233717/cybersecurity-evolving-ransomware-tactics-state-sponsored-threats/

Click above link to read more.

Back to top

Thomson Reuters collected and leaked at least 3TB of sensitive data

Thomson Reuters, a multinational media conglomerate, left an open database with sensitive customer and corporate data, including third-party server passwords in plaintext format. Attackers could use the details for a supply-chain attack.

The Cybernews research team found that Thomson Reuters left at least three of its databases accessible for anyone to look at. One of the open instances, the 3TB public-facing ElasticSearch database, contains a trove of sensitive, up-to-date information from across the company's platforms. The company recognized the issue and fixed it immediately.

https://cybernews.com/security/thomson-reuters-leaked-terabytes-sensitive-data/

Click above link to read more.

Back to top

These cybersecurity vulnerabilities are most popular with hackers right now - have you patched them?

One of the most popular security vulnerabilities among cyber criminals during the past few months is a software flaw in Microsoft Office that's over five years old – and it continues to be exploited because, despite a longstanding available security update, many businesses still haven't applied it.

According to analysis by cybersecurity researchers at Digital Shadows, the most commonly discussed vulnerability among cyber criminals on underground forums over the last three months is CVE-2017-11882 – a security flaw in Microsoft Office first disclosed in 2017.

https://www.zdnet.com/article/these-cybersecurity-vulnerabilities-are-most-popular-with-hackers-right-now-have-you-patched-them/

Click above link to read more.

Back to top

These dropper apps on Play Store targeting over 200 banking and cryptocurrency wallets

Five malicious dropper Android apps with over 130,000 cumulative installations have been discovered on the Google Play Store distributing banking trojans like SharkBot and Vultur, which are capable of stealing financial data and performing on-device fraud.

"These droppers continue the unstopping evolution of malicious apps sneaking to the official store," Dutch mobile security firm ThreatFabric told The Hacker News in a statement.

https://thehackernews.com/2022/10/these-dropper-apps-on-play-store.html

Click above link to read more.

Back to top

New York Post hacked with offensive headlines targeting politicians

New York Post confirmed today that it was hacked after its website and Twitter account were used by the attackers to publish offensive headlines and tweets targeting U.S. politicians.

"The New York Post has been hacked. We are currently investigating the cause," the daily newspaper tweeted shortly after removing multiple disturbing tweets published earlier on Thursday.

https://www.bleepingcomputer.com/news/security/new-york-post-hacked-with-offensive-headlines-targeting-politicians/?&web_view=true

Click above link to read more.

Back to top

Bed, Bath & Beyond confirms data breach following employee phishing attack

U.S. retail giant Bed, Bath & Beyond has confirmed unauthorized access to company data after an employee was phished.

In an 8-K filing to the U.S. Securities and Exchange Commission, the home goods retailer said it became aware that an attacker had “improperly accessed” company data after a successful

phishing scam targeting an employee in October. This gave the hacker access to data on the employee's hard drive and other shared drives to which the employee had access.

https://techcrunch.com/2022/10/31/bed-bath-beyond-data-breach/

Click above link to read more.

Back to top

Australian Defence Department caught up in ransomware attack

The Department of Defence fears the personal data of personnel, such as dates of birth, may have been compromised after a communications platform used by the military was hit by a ransomware attack.

Hackers have targeted the ForceNet service, which is run by an external information and communications technology (ICT) provider, with the company initially telling Defence no data of current or former personnel appeared to have been compromised.

https://www.abc.net.au/news/2022-10-31/defence-department-ransomware-attack-forecenet-australia/101596230

Click above link to read more.

Back to top

DHL named most-spoofed brand in phishing

DHL is the most spoofed brand when it comes to phishing emails, according to Check Point.

Crooks most frequently used the brand name in their attempts to steal personal and payment information from marks between July and September 2022, with the shipping giant accounting for 22 percent of all worldwide phishing attempts intercepted by the cybersecurity outfit.

https://www.theregister.com/2022/10/24/dhl_phishing_scams/

Click above link to read more.

Back to top

First on CNN: US banks report more than $1 billion in potential ransomware payments in 2021

US financial institutions reported more than $1 billion in potential ransomware-related payments in 2021 — more than double the amount from the previous year and the most ever reported, according to Treasury Department data shared exclusively with CNN.

The five hacking tools that accounted for the most payments during the last half of 2021 are all connected to Russian hackers, according to the report from Treasury's Financial Crimes Enforcement Network (FinCEN).

https://www.cnn.com/2022/11/01/politics/us-banks-ransomware-payments-2021/index.html

Click above link to read more.

Back to top

Twitter's verification chaos is now a cybersecurity problem

Cybercriminals are already capitalizing on Twitter's ongoing verification chaos by sending phishing emails designed to steal the passwords of unwitting users.

The phishing email campaign, seen by TechCrunch, attempts to lure Twitter users into posting their username and password on an attacker's website disguised as a Twitter help form.

https://techcrunch.com/2022/10/31/twitter-verification-phishing/

Click above link to read more.

Back to top

U.S. Treasury thwarted attack by Russian hacker group last month-official

The U.S. Treasury last month repelled cyber attacks by a pro-Russian hacker group, preventing disruption and confirming the effectiveness of the department's stronger approach to financial system cybersecurity, a U.S. Treasury official said on Tuesday.

The Treasury has attributed the distributed denial of service (DDoS) attacks to Killnet, the Russian hacker group that claimed responsibility for disrupting the websites of several U.S. states and airports in October, said Todd Conklin, cybersecurity counselor to Deputy Treasury Secretary Wally Adeyemo.

https://www.reuters.com/world/us-treasury-targeted-by-russian-hacker-group-last-month-official-2022-11-01/

Click above link to read more.

Back to top

Hackers selling access to 576 corporate networks for $4 million

A new report shows that hackers are selling access to 576 corporate networks worldwide for a total cumulative sales price of $4,000,000, fueling attacks on the enterprise.

The research comes from Israeli cyber-intelligence firm KELA which published its Q3 2022 ransomware report, reflecting stable activity in the sector of initial access sales but a steep rise in the value of the offerings.

https://www.bleepingcomputer.com/news/security/hackers-selling-access-to-576-corporate-networks-for-4-million/

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