November 9, 2021

Challenge yourself with our Online Shopping quiz!

Multi-Factor Authentication is currently rolling out across the BC Government now through Early 2022.

Check your inbox regularly for an MFA registration email.

This week's stories:

- B.C. residents losing millions to fraudsters using sophisticated crypto scams on social media, dating sites
- N.L. premier says feds offered 'full depth and breadth' of support after cyberattack
- How InfoSec should use the Minimum Viable Secure Product checklist
- US Department of Justice recovers $6 million and indicts two REvil principals
- Phishing attack blends spoofed Amazon order and fraudulent customer service agents
- US arrests and charges Ukrainian man for Kaseya ransomware attack
- DDoS attacks shatter records in Q3, report finds
- U.S. offers reward of up to $10 million for information on REvil ransomware group
- Pros and cons of using open-source software
- Types of penetration testing
- Hacker steals $55 million from bZx DeFi platform
- Law enforcement operation targets Clop ransomware
- BlackBerry uncovers initial access broker linked to three distinct hacker groups
- Robinhood trading app hit by data breach affecting seven million

---

B.C. residents losing millions to fraudsters using sophisticated crypto scams on social media, dating sites

Officials are warning the public about "sophisticated" crypto investment scams that have cost residents millions of dollars so far in 2021.

According to a joint release from RCMP, British Columbia Securities Commission (BCSC), and the Canadian Anti-Fraud Centre (CAFC), residents across the province reported losses totalling $3.5 million in the first eight months of 2021.

https://www.cheknews.ca/b-c-residents-losing-millions-to-fraudsters-using-sophisticated-crypto-scams-on-social-media-dating-sites-906879/

Click above link to read more.

Back to top

N.L. premier says feds offered 'full depth and breadth' of support after cyberattack

Newfoundland and Labrador Premier Andrew Furey says Ottawa has offered to help the province recover from a cyberattack last weekend that has crippled its health system's IT network.

Furey told reporters Intergovernmental Affairs Minister Dominic LeBlanc has offered the "full depth and breadth" of support from the federal government, as has the prime minister.

https://www.canadiansecuritymag.com/n-l-premier-says-feds-offered-full-depth-and-breadth-of-support-after-cyberattack/

Click above link to read more.

Back to top

How InfoSec should use the Minimum Viable Secure Product checklist

A team of tech companies including Google, Salesforce, Slack, and Okta recently released the Minimum Viable Secure Product (MVSP) checklist, a vendor-neutral security baseline listing minimum acceptable security requirements for B2B software and business process outsourcing suppliers.

The news arrives at a time when many organizations are growing concerned about the security of third-party tools and processes they use. After attacks such as those involving SolarWinds and Kaseya, businesses are increasingly aware of how third-party tools and services could serve as a gateway to attackers.

https://www.darkreading.com/operations/how-infosec-should-use-the-minimum-viable-secure-product-checklist

Click above link to read more.

Back to top

US Department of Justice recovers $6 million and indicts two REvil principals

The DOJ promises a whole of government approach to fighting ransomware groups no matter which country they operate from.

It didn't take long for the White House's ransomware initiative to be fruitful, as evidenced by the successful international law enforcement efforts targeting members of the Sodinokibi/REvil criminal enterprise. The Department of Justice (DoJ) unsealed two grand jury indictments on November 8, 2021,

on individuals associated with the group – Yaroslave Vasinskyi and Yevgeniy Polyanin– both with Sodinokibi/REvil ransomware.

https://www.csoonline.com/article/3639624/us-department-of-justice-recovers-6-million-and-indicts-two-revil-principals.html

Click above link to read more.

Back to top

Phishing attack blends spoofed Amazon order and fraudulent customer service agents

A new multistage phishing campaign spoofs Amazon's order notification page and includes a phony customer service voice number where the attackers request the victim's credit card details to correct the errant "order."

The campaign, highlighted in new research from Avanan on Thursday, underscores how phishing attacks are growing in sophistication by using a combination of email and voice lures and leveraging popular brands such as Amazon to scam potential victims.

https://www.darkreading.com/attacks-breaches/new-lure-impersonates-popular-amazon-brand-and-combines-email-phishing-with-a-voice-scam-

Click above link to read more.

Back to top

US arrests and charges Ukrainian man for Kaseya ransomware attack

The US Department of Justice has charged today a 22-year-old Ukrainian national for orchestrating the ransomware attacks on Kaseya servers that took place over the July 4 weekend this year.

The suspect, named Yaroslav Vasinskyi, was detained last month following an arrest warrant issued by the US. He was detained by Polish authorities at a border station while crossing from Ukraine into Poland.

In court documents unsealed today, the DOJ said that Vasinskyi was a long-time collaborator of the REvil (Sodinokibi) ransomware operation.

https://therecord.media/us-arrests-and-charges-ukrainian-man-for-kaseya-ransomware-attack/

Click above link to read more.

Back to top

DDoS attacks shatter records in Q3, report finds

The third quarter saw the sheer volume of distributed denial-of-service (DDoS) attacks surge to several thousand hits per day, signaling a re-distribution of tactics by malicious actors away from cryptomining and toward the use of DDoS as a tool of intimidation, disinformation and straight-up extortion.

The latest DDoS report for Q3 from Kaspersky details a record-breaking frenzy of recent activity by threat actors.

https://threatpost.com/ddos-attacks-records-q3/176082/

Click above link to read more.

Back to top

U.S. offers reward of up to $10 million for information on REvil ransomware group

The U.S. Department of State said it was offering a reward of up to $10 million for information leading to the identification or location of anyone holding a key position in the REvil ransomware crime group.

The department also said it was offering a reward offer of up to $5 million for information leading to the arrest or conviction of any individual participating in a REvil variant ransomware incident.

https://www.reuters.com/technology/us-offers-reward-up-10-million-information-revil-ransomware-group-2021-11-08/

Click above link to read more.

Back to top

Pros and cons of using open-source software

Since the late 1980s, when it pioneered, open-source software has come a long way. A lot of IT experts recommend both medium and small enterprises use open-source software in the IT strategy.

Today, popular open-source software such as WordPress is an essential part of most organizations. Open-source software caters to virtually every aspect from operating systems to telecommunication systems and accounting systems, among others.

In this post, you learn about open source software, its pros, and its cons.

https://cybersecuritynews.com/pros-and-cons-of-using-open-source-software/

Click above link to read more.

Back to top

Types of penetration testing

If you are thinking about performing a penetration test on your organization, you might be interested in learning about the different types of tests available. With that knowledge, you'll be better equipped to define the scope for your project, hire the right expert and, ultimately, achieve your security objectives.

Penetration testing, commonly referred to as "pen testing," is a technique that simulates real-life attacks on your IT systems to find weaknesses that could be exploited by hackers. Whether to comply with security regulations such as ISO 27001, gain customer and 3rd party trust, or achieve your own peace of mind, penetration testing is an effective method used by modern organizations to strengthen their cyber security posture and prevent data breaches.

https://thehackernews.com/2021/11/types-of-penetration-testing.html

Click above link to read more.

Back to top

Hacker steals $55 million from bZx DeFi platform

A hacker has stolen an estimated $55 million worth of cryptocurrency assets from bZx, a decentralized finance (DeFi) platform that allows users to borrow, loan, and speculate on cryptocurrency price variations.

“A bZx developer was sent a phishing email to his personal computer with a malicious macro in a Word document that was disguised as a legitimate email attachment,” the company said in a preliminary post mortem of the attack published on Friday night, hours after the hack.
bZx said the email attachment ran a script on the developer’s computer that compromised the employee’s mnemonic wallet phrase.

https://therecord.media/hacker-steals-55-million-from-bzx-defi-platform/

Click above link to read more.

Back to top

Law enforcement operation targets Clop ransomware

Following the arrest of suspected Clop ransomware operation members in Ukraine, Red Notices issued by Interpol seek the arrest of six more members of the Russian-speaking crime group, as part of what law enforcement agencies have dubbed Operation Cyclone.

The agency issued two Red Notices on Friday, alerting its 194 member countries following a request by South Korea’s cybercrime investigation division via Interpol’s National Central Bureau in Seoul.

https://www.bankinfosecurity.com/law-enforcement-operation-targets-clop-ransomware-a-17858

Click above link to read more.

Back to top

BlackBerry uncovers initial access broker linked to three distinct hacker groups

A previously undocumented initial access broker has been unmasked as providing entry points to three different threat actors for mounting intrusions that range from financially motivated ransomware attacks to phishing campaigns.

BlackBerry's research and intelligence team dubbed the entity "Zebra2104," with the group responsible for offering a means of a digital approach to ransomware syndicates such as MountLocker and Phobos, as well as the advanced persistent threat (APT) tracked under the moniker StrongPity (aka Promethium).

https://thehackernews.com/2021/11/blackberry-uncover-initial-access.html

Click above link to read more.

Back to top

Robinhood trading app hit by data breach affecting seven million

US share-trading app Robinhood has been hit by a security breach that has exposed the names or email addresses of more than seven million people.

The company says the breach affected "a limited amount of personal information for a portion of our customers".

And it does not believe the most sensitive information it gathers - US social security numbers and financial information - was revealed.

https://www.bbc.com/news/technology-59209494

Click above link to read more.

Back to top


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