February 8, 2022

Challenge yourself with our Love Security quiz!

This past week's stories:

- A quarter of Canadian companies have been victims of a cyber attack in 2021: survey
- Don't forget your burner phone: Why cybersecurity in China is an Olympic event in itself
- How cybersecurity during the winter Olympics is a massive effort
- Intuit warns of phishing emails threatening to delete accounts
- Log4j: getting from stopgap remedies to long-term solutions
- FBI publishes indicators of compromise for LockBit 2.0 ransomware
- Shortage of KP Nuts and Hula Hoops looms after cyber-attack
- Low-detection phishing kits increasingly bypass MFA
- Cryptocurrency platform Wormhole hacked for an estimated $322 million
- Most Irish SMEs hit by cyber-attack last year
- Critical infrastructure hit again as German fuel suppliers victimized by cyber attack, oil shipments forced to use alternative depots
- Umbrella company Parasol confirms data breach linked to cyber attack five weeks ago
- Schoolgirls from the South compete to be cyber security champions

---

A quarter of Canadian companies have been victims of a cyber attack in 2021: survey

A quarter of Canadian businesses say they have already been the victim of a cyber attack in 2021, according to a Leger survey commissioned by technology firm NOVIPRO.

"The survey shows that cybersecurity is far from being a hypothetical risk," said NOVIPRO information security head Dominique Derrier. "As soon as a company generates value, it appears somewhere on a cyberthreat map."

https://montreal.ctvnews.ca/a-quarter-of-canadian-companies-have-been-victims-of-a-cyber-attack-in-2021-survey-1.5770718

Click above link to read more.

Back to top

Don't forget your burner phone: Why cybersecurity in China is an Olympic event in itself

For Canadian athletes, staff and media, and their counterparts around the world, braving a hostile cyber environment is the part of the price of admission to the 2022 Winter Olympics.

At the top of the packing list for these Olympics? A virtual private network, or VPN. From Switzerland to Great Britain, prominent National Olympic Committees have equipped team members with burner phones, and cybersecurity briefings have been part of their preparations for the Games.

https://nationalpost.com/sports/olympics/2022-winter-olympics-china-cybersecurity-burner-phones

Click above link to read more.

Back to top

How cybersecurity during winter Olympics is a massive effort

It requires a massive effort to make the Olympic games happen every two years.

But behind the scenes, there's an entire team of people working to make sure the broadcast you watch at home runs smoothly.

There is a security team of hundreds of people monitoring the cyber side of the games and blocking malicious cyberattacks every day.

https://www.nbcdfw.com/news/sports/beijing-winter-olympics/how-cybersecurity-during-winter-olympics-is-a-massive-effort/2881894/

Click above link to read more.

Back to top

Intuit warns of phishing emails threatening to delete accounts

Accounting and tax software provider Intuit has notified customers of an ongoing phishing campaign impersonating the company and trying to lure victims with fake warnings that their accounts have been suspended.

Intuit's alert follows reports received from customers who were emailed and told that their Intuit accounts were disabled following a recent server security upgrade.

https://www.bleepingcomputer.com/news/security/intuit-warns-of-phishing-emails-threatening-to-delete-accounts/

Click above link to read more.

Back to top

Log4j: getting from stopgap remedies to long-term solutions

This pervasive vulnerability will require continued care and attention to fully remediate and detect permutations. Here are some ways to get started.

While the worst of Log4Shell may be behind us and much work remains, let's say "Well done" to the security engineers and managers who labored in the trenches in recent weeks. But if you thought the Log4j vulnerability was last year's problem, think again. In 2022, this vulnerability will require care and attention to fully remediate and detect permutations.

https://www.darkreading.com/attacks-breaches/log4j-getting-from-stopgap-remedies-to-long-term-solutions

Click above link to read more.

Back to top

FBI publishes indicators of compromise for LockBit 2.0 ransomware

The FBI today issued a flash bulletin that details the specific indicators of compromise (IoCs) associated with LockBit 2.0, whose operators offer the ransomware variant via a ransomware-as-a-service model.

LockBit 2.0 moves quickly, mainly because it can automatically encrypt devices in a Windows domain using Active Directory (AD) group policies. The ransomware attackers using LockBit often also threaten to leak stolen victim data on their doxxing site if the victim doesn't pony up with their ransom demands. According to the FBI, LockBit 2.0 is "a heavily obfuscated ransomware application leveraging bitwise operations to decode strings and load required modules to evade detection."

https://www.darkreading.com/threat-intelligence/fbi-publishes-indicators-of-compromise-for-lockbit-2-0-ransomware

Click above link to read more.

Back to top

Shortage of KP Nuts and Hula Hoops looms after cyber-attack

A cyber-attack targeting KP Snacks could lead to a shortage of some of Britain’s most popular snacks including Hula Hoops, McCoy’s and Tyrrells crisps, Butterkist, Skips, Nik Naks and KP Nuts.

The company has sent a letter to stores saying the ransomware attack, which has crippled its IT and communications systems, could lead to supply issues until “the end of March at the earliest” as it “cannot safely process orders or dispatch goods”.

https://www.theguardian.com/business/2022/feb/03/shortage-of-kp-nuts-and-hula-hoops-looms-after-cyber-attack

Click above link to read more.

Back to top

Low-detection phishing kits increasingly bypass MFA

More and more phishing kits are focusing on bypassing multi-factor authentication (MFA) methods, researchers have warned – typically by stealing authentication tokens via a man-in-the-middle (MiTM) attack.

As MFA continues to see widespread consumer and business adoption – a full 78 percent of respondents in a recent poll said they used it in 2021 – cybercriminals have devoted resources into keeping up. According to an analysis from Proofpoint, MFA-bypass phishing kits are proliferating rapidly, "ranging from simple open-source kits with human readable code and no-frills functionality to sophisticated kits utilizing numerous layers of obfuscation and built-in modules that allow for stealing usernames, passwords, MFA tokens, Social Security numbers and credit-card numbers."

https://threatpost.com/low-detection-phishing-kits-bypass-mfa/178208/

Click above link to read more.

Back to top

Cryptocurrency platform Wormhole hacked for an estimated $322 million

A threat actor has abused a vulnerability in the Wormhole cryptocurrency platform to steal an estimated $322 million worth of Ether currency.

The attack took place earlier today and impacted Wormhole Portal, a web-based application—also known as a blockchain "bridge"—that allows users to convert one form of cryptocurrency into another.

https://therecord.media/cryptocurrency-platform-wormhole-hacked-for-an-estimated-322-million/?web_view=true

Click above link to read more.

Back to top

Most Irish SMEs hit by cyber-attack last year

95% of small and medium sized Irish businesses experienced a cyber-attack in the past year, according to the findings of a new survey.

The research by IT and cyber security firm Typetech reveals that the most common cyber-attacks were phishing, followed by ransomware and malware.

https://www.rte.ie/news/business/2022/0207/1278323-most-irish-smes-hit-by-cyber-attack-last-year/

Click above link to read more.

Back to top

Critical infrastructure hit again as German fuel suppliers victimized by cyber attack, oil shipments forced to use alternative depots

A cyber attack on two German logistics firms used by Shell has forced a temporary reroute to alternative supply depots, and echoes the attack on fuel supplier Colonial Pipeline as another example of cyber criminals directly targeting real-world critical infrastructure.

The identity of the attacker has yet to be confirmed, but there is speculation about the involvement of both Chinese and Russian threat groups. The exact type of cyber attack has also yet to be identified, but the extent of the disruption would indicate ransomware or a malicious malware attack that wiped files.

https://www.cpomagazine.com/cyber-security/critical-infrastructure-hit-again-as-german-fuel-suppliers-victimized-by-cyber-attack-oil-shipments-forced-to-use-alternative-depots/

Click above link to read more.

Back to top

Umbrella company Parasol confirms data breach linked to cyber attack five weeks ago

Umbrella company Parasol has confirmed that it is investigating details of a data breach that has come to light in the wake of a suspected ransomware attack on its systems last month.

Parasol, which is known to have at least 13,000 contractors on its books, sent out an email earlier today – signed by its CEO, Doug Crawford – in which it confirmed that its IT security team had discovered that "some data" had been copied and leaked online since the attack on its systems.

https://www.computerweekly.com/news/252513042/Umbrella-company-Parasol-confirms-data-breach-linked-to-cyber-attack-five-weeks-ago

Click above link to read more.

Back to top

Schoolgirls from the South compete to be cyber security champions

Schoolgirls from across the region have been putting their skills to the test in a bid to be crowned cyber security champions.

The CyberFirst Girls competition is run by the National Cyber Security Centre which is part of GCHQ.

https://www.itv.com/news/meridian/2022-02-06/schoolgirls-from-the-south-compete-to-be-cyber-security-champions

Click above link to read more.

Back to top

---

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