March 15, 2022

Challenge yourself with our Fraud Prevention quiz!

This past week's stories:

- How B.C. tech is navigating Russian 'naughty list'
- Aviva Canada reveals top five risks facing Canadian businesses – report
- Russia-Ukraine: Is internet on verge of break-up?
- Beefing up its cybersecurity, Google buys Mandiant for $5.4B
- IOTW: Romanian oil company hit by 'complex cyber-attack'
- Cybersecurity: Attacker uses websites' contact forms to spread BazarLoader malware
- Ubisoft confirms 'cyber security incident', resets staff passwords
- Russian ransomware gang retool custom hacking tools of other APT groups
- Cyberattack on Norwood Clinic compromises data tied to 228K patients
- Android malware Escobar steals your Google Authenticator MFA codes
- 'For the first time in history anyone can join a war': Volunteers join Russia-Ukraine cyber fight
- Rosneft's German unit reports cyber attack- media reports
- Banks on alert for Russian reprisal cyber attacks on Swift

How B.C. tech is navigating Russian 'naughty list'

The day after Russia's invasion of Ukraine last month, the Canadian Centre for Cyber Security fired off a bulletin, warning citizens the war would be more than just an armed conflict.

A new malware known as HermeticWiper was targeting Ukrainian organizations, and weeks earlier, even before tough sanctions were enacted against Russia, the Cyber Centre was urging the "Canadian cybersecurity community – especially critical infrastructure network defenders – to bolster their awareness of and protection against Russian state-sponsored cyber threats."

https://biv.com/article/2022/03/how-bc-tech-navigating-russian-naughty-list

Click above link to read more.

Back to top

Aviva Canada reveals top five risks facing Canadian businesses – report

Canadian businesses have identified five major risks to their operation – and these reflect how their risk assessments have changed due to the COVID-19 pandemic, a new report by Aviva Canada has found.

Aviva Canada's Risk Insights Report is a new study conducted by the insurer, with 1,500 Canadian businesses of all types and sizes surveyed for the report. The insurer said that it is the first Canadian report of its kind, and it will kick off an ongoing series that "expands on Aviva's commitment to help businesses make sense of their specific risks, better manage those risks, and prepare for the future."

https://www.insurancebusinessmag.com/ca/news/breaking-news/aviva-canada-reveals-top-five-risks-facing-canadian-businesses--report-398123.aspx

Click above link to read more.

Back to top

Russia-Ukraine: Is internet on verge of break-up?

The world, both physical and digital, finds itself in unprecedented times as the conflict in Ukraine rages.

Corporate giants such as Meta, Google and Apple, who have always framed themselves as neutral tech firms, are now pinning their political colours to the mast - banning products in Russia in response to its invasion.

https://www.bbc.com/news/technology-60661987

Click above link to read more.

Back to top

Beefing up its cybersecurity, Google buys Mandiant for $5.4B

Google is fortifying its cloud services with a $5.4 billion acquisition of the cyber security firm Mandiant, the companies announced Tuesday.

The acquisition is the first of many that analysts foresee in the cyber security sector following Russia's invasion of Ukraine. Analysts and government officials have said they expect a wave of cyberattacks from Russia and others as geopolitical tensions rise.

https://abcnews.go.com/Business/wireStory/beefing-security-google-buys-mandiant-54-billion-83315471

Click above link to read more.

Back to top

IOTW: Romanian oil company hit by ‘complex cyber-attack’

Rompetrol, a Romanian gas station chain and part of KMG International, has confirmed it was subject to a “complex cyber-attack”.

Following the attack, which was confirmed on 7 March 2022 in a company Facebook post, the company sought to mitigate the impact on data by suspending operations of its website and its Fill&Go service at its gas stations.

https://www.cshub.com/attacks/news/iotw-romanian-oil-company-hit-by-complex-cyber-attack

Click above link to read more.

Back to top

Cybersecurity: Attacker uses websites’ contact forms to spread BazarLoader malware

Everyone in the IT industry should be aware by now that email is the most used vector for cybercriminals to try to infect employees with malware. Yet, when they are first approached via their website’s contact form, things might look different and fully legitimate, raising a false feeling of security. Here’s how this new social engineering method used to spread the infamous BazarLoader malware, and how to protect yourself from it.

https://www.techrepublic.com/article/cybersecurity-attacker-uses-websites-contact-forms-to-spread-bazarloader-malware/?utm_source=email&utm_medium=referral&utm_campaign=cybersecurity-insider

Click above link to read more.

Back to top

Ubisoft confirms 'cyber security incident', resets staff passwords

Video game developer Ubisoft has confirmed that it suffered a 'cyber security incident' that caused disruption to its games, systems, and services.

The announcement comes after multiple Ubisoft users had reported issues last week accessing their Ubisoft service.

Data extortion group LAPSUS$, who has claimed responsibility for hacking Samsung, NVIDIA, and Mercado Libre thus far, appears to be behind this incident.

https://www.bleepingcomputer.com/news/security/ubisoft-confirms-cyber-security-incident-resets-staff-passwords/

Click above link to read more.

Back to top

Russian ransomware gang retool custom hacking tools of other APT groups

A Russian-speaking ransomware outfit likely targeted an unnamed entity in the gambling and gaming sector in Europe and Central America by repurposing custom tools developed by other APT groups like Iran's MuddyWater, new research has found.

The unusual attack chain involved the abuse of stolen credentials to gain unauthorized access to the victim network, ultimately leading to the deployment of Cobalt Strike payloads on compromised assets, said Felipe Duarte and Ido Naor, researchers at Israeli incident response firm Security Joes, in a report published last week.

https://thehackernews.com/2022/03/russian-ransomware-gang-retool-custom.html

Click above link to read more.

Back to top

Cyberattack on Norwood Clinic compromises data tied to 228K patients

Alabama-based Norwood Clinic notified 228,103 patients that their data was potentially accessed or acquired after a cyberattack in October 2021.

Upon discovery, the systems were secured and the security team worked to “safely restore its systems and operations.” The notice does not disclose whether the attack was caused by ransomware. The investigation determined the hackers gained access to servers containing patient information during the incident.

https://www.scmagazine.com/analysis/breach/cyberattack-on-norwood-clinic-compromises-data-tied-to-228k-patients

Click above link to read more.

Back to top

Android malware Escobar steals your Google Authenticator MFA codes

The Aberebot Android banking trojan has returned under the name 'Escobar' with new features, including stealing Google Authenticator multi-factor authentication codes.

The new features in the latest Aberebot version also include taking control of the infected Android devices using VNC, recording audio, and taking photos, while also expanding the set of targeted apps for credential theft.

https://www.bleepingcomputer.com/news/security/android-malware-escobar-steals-your-google-authenticator-mfa-codes/

Click above link to read more.

Back to top

‘For the first time in history anyone can join a war’: Volunteers join Russia-Ukraine cyber fight

Cyber warfare related to the Ukraine-Russia conflict is surging as digital volunteers from around the world enter the fight.

The number of cyberattacks being waged by — and on behalf of — both countries since the outbreak of the war is “staggering,” according to the research arm of Check Point Software Technologies.

https://www.cnbc.com/2022/03/14/volunteers-sign-up-to-help-in-cyberwars-between-russia-and-ukraine-.html

Click above link to read more.

Back to top

Rosneft's German unit reports cyber attack- media reports

The German subsidiary of the Russian energy company Rosneft has reported a hacker attack, die Welt newspaper reported on Sunday, citing the country's BSI cybersecurity watchdog.

The paper said the BSI had offered support to overcome the problem, which occurred on Friday night or early Saturday morning, and had issued a cybersecurity warning to other companies in the energy sector.

https://www.reuters.com/business/energy/rosnefts-german-unit-reports-cyber-attack-media-reports-2022-03-13/

Click above link to read more.

Back to top

Banks on alert for Russian reprisal cyber attacks on Swift

Big banks fear that Swift faces a growing threat of Russian cyber attacks after seven of the country’s lenders were kicked off the global payments messaging system over the weekend.

VTB, Russia’s second-biggest bank, and Promsvyazbank, which finances Russia’s war machine, were among the lenders removed on Saturday from Swift as part of the west’s sanctions campaign against Moscow in response to its invasion of Ukraine.

https://www.ft.com/content/a2bdba3b-f1dd-4c9f-a0de-9ffff6e744e4

Click above link to read more.

Back to top

---

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