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

January 25, 2022

Challenge yourself with our Cyber Security Resolutions quiz!

This past week's stories:

🍁 **Threat of Russian-backed cyber attacks growing amid Ukraine tensions, Canada's cybersecurity agency warns**

🍁 **Global Affairs Canada suffers 'cyber attack' amid Russia-Ukraine tensions: sources**

REvil ransomware gang arrests trigger uncertainty, concern in cybercrime forums

IOTW: Red Cross confirms cyber-attack compromising personal data

Are you prepared to defend against a USB attack?

There's no 'magic bullet' to enhance cybersecurity, say experts

The case for backing up source code

Cybersecurity in a hybrid work world: Taking a proactive approach in a perimeter-less environment

Dark Souls PC servers down amid hacking fears

Cyber security in 2022: A fresh look at some very alarming stats

COVID19 phishing emails surge 500% on Omicron concerns

Supply chain attack used legitimate WordPress add-ons to backdoor sites

---

Threat of Russian-backed cyber attacks growing amid Ukraine tensions, Canada's cybersecurity agency warns

Canada's digital cybersecurity agency is warning the country's "critical infrastructure" providers to be increasingly weary of attacks from Russia-backed hackers as tensions between the two countries increase over the threat of war in Ukraine.

Experts say those attacks could come in a range of forms, from a "widespread ransomware attack" to a "single, carefully focused" attempt to significantly impact core infrastructure.

https://nationalpost.com/news/politics/threat-of-russian-backed-cyber-attacks-growing-amid-ukraine-tensions-canadian-cybersecurity-agency-warns

Click above link to read more.

Back to top

Global Affairs Canada suffers ‘cyber attack’ amid Russia-Ukraine tensions: sources

Global Affairs Canada is scrambling to recover after a multi-day network disruption that security and government sources describe as a “cyber attack.”

While neither Global Affairs nor Canada’s cyber security agency, the Communications Security Establishment, could immediately comment, sources tell Global News the government is concerned the attack was conducted by Russia or Russian-backed hackers.

https://globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/

Click above link to read more.

Back to top

REvil ransomware gang arrests trigger uncertainty, concern in cybercrime forums

Law enforcement action typically does little to deter cybercriminal activity. But last week's arrests in Russia of several members of the notorious REvil ransomware group, as well as the dismantling of its criminal infrastructure, appear to have finally grabbed the attention of at least some threat actors.

Researchers from Trustwave who regularly track chatter on underground forums this week observed signs of considerable anxiety and consternation among Eastern-European cybercriminals in the days following the REvil arrests. Many threat actors apparently seem less confident about Russia being a haven for their operations and fear that cooperation between Russian and US authorities could pose major problems for them in the future.

https://www.darkreading.com/threat-intelligence/revil-arrests-trigger-uncertainty-concern-in-cybercrime-forums

Click above link to read more.

Back to top

IOTW: Red Cross confirms cyber-attack compromising personal data

The International Committee of the Red Cross (ICRC) has been subject to a cyber-attack against its computer servers.

On 19 January 2022 the ICRC confirmed in a statement that a cyber-attack has compromised the personal data and confidential information of more than 515,000 “highly vulnerable” people.

https://www.cshub.com/attacks/news/iotw-red-cross-confirms-cyber-attack-compromising-personal-data

Click above link to read more.

Back to top

Are you prepared to defend against a USB attack?

The FBI recently warned of advanced USB-based attacks by a group called FIN7. The campaign, believed to have started last August, targets American companies, including those in key critical infrastructure industries such as transportation, insurance, and defense. The attackers targeted victims by sending them packages that contain advanced attack tools on the USB devices. These "BadUSBs" pose a significant threat. Here's what you need to know — and do — about them.

https://www.darkreading.com/vulnerabilities-threats/are-you-prepared-to-defend-against-a-USB-attack-

Click above link to read more.

Back to top

There's no 'magic bullet' to enhance cybersecurity, say experts

Cybersecurity has taken on increased importance in the healthcare industry, particularly as domestic and international incidents continue to dominate the headlines.

Amid this dynamic environment, experts stress that an organization's defensive strategy should be flexible and adaptable.

https://www.healthcareitnews.com/news/theres-no-magic-bullet-enhance-cybersecurity-say-experts

Click above link to read more.

Back to top

The case for backing up source code

As enterprise data security concerns grow, security experts urge businesses to back up their GitLab, GitHub, and BitBucket repositories.

Never before have organizations handled more information — or been more concerned about how it may fall into the wrong hands. This concern applies to all data, but especially the source code they rely on to keep their processes running.

https://www.darkreading.com/dr-tech/source-code-security-the-case-for-making-backups

Click above link to read more.

Back to top

Cybersecurity in a hybrid work world: Taking a proactive approach in a perimeter-less environment

The hybrid work model can bring substantial benefits for employers and employees alike, but it also presents a myriad of IT challenges. IT departments are increasingly under pressure to provide ready access to users working outside of traditional office space.

Data increasingly resides outside of the traditional data center while users, corporate data and business-critical assets can reside anywhere. If your business has experienced a shift to the hybrid working model in the past 12 to 18 months, it may be time to reconsider and strengthen your cybersecurity approach.

https://www.bizjournals.com/twincities/news/2022/01/21/cybersecurity-in-a-hybrid-work-world-taking-a.html

Click above link to read more.

Back to top

Dark Souls PC servers down amid hacking fears

Action role-playing game Dark Souls 3 has been taken offline following reports of an exploit that could allow bad actors to take control of your PC.

Publisher Bandai Namco and developer FromSoftware have turned off player-v-player (PvP) servers, meaning gamers cannot play competitively.

The downtime affects Dark Souls 3, Dark Souls 2, and Dark Souls: Remastered.

But the purported exploit cannot affect console gamers and as such PvP remains available on PlayStation and Xbox.

https://www.bbc.com/news/technology-60115522

Click above link to read more.

Back to top

Cyber security in 2022: A fresh look at some very alarming stats

Last year I wrote two FORBES articles* that highlighted some of the more significant cyber statistics associated with our expanding digital ecosystem. In retrospect, 2021 was a very trying year for cybersecurity in so many areas. There were high profile breaches such as Solar Winds, Colonial Pipeline and dozens of others that had major economic and security related impact. Ransomware came on with a vengeance targeting many small and medium businesses.

https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=4f3107be6b61

Click above link to read more.

Back to top

COVID19 phishing emails surge 500% on Omicron concerns

The latest COVID-19 variant has led to a 521% increase in phishing attacks using the virus as a lure to trick users into clicking, according to Barracuda Networks.

Cyber-criminals often use newsworthy events in their social engineering attacks, and COVID-19 provided a bumper opportunity when it emerged in 2020.

The security vendor observed a 667% month-on-month surge in COVID-19 phishing emails from February to March that year. It recorded another significant increase when new vaccines were released at the start of 2021.

https://www.infosecurity-magazine.com/news/covid19-phishing-surge-500-omicron/

Click above link to read more.

Back to top

Supply chain attack used legitimate WordPress add-ons to backdoor sites

Dozens of legitimate WordPress add-ons downloaded from their original sources have been found backdoored through a supply chain attack, researchers said. The backdoor has been found on “quite a few” sites running the open source content management system.

The backdoor gave the attackers full administrative control of websites that used at least 93 WordPress plugins and themes downloaded from AccessPress Themes. The backdoor was discovered by security researchers from JetPack, the maker of security software owned by Automatic, provider of the WordPress.com hosting service and a major contributor to the development of WordPress. In all, Jetpack found that 40 AccessPress themes and 53 plugins were affected.

https://arstechnica.com/information-technology/2022/01/supply-chain-attack-used-legitimate-wordpress-add-ons-to-backdoor-sites/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity 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

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA
OCIO | Office of the Chief Information Officer