Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

July 27, 2021

Challenge yourself with our Password Security quiz!

This week's stories:

🍁 **Canadian professionals named to IFSEC's annual security and fire influencers list**

Malware infects Japanese devices ahead of Olympic Games

Cyber-attacks: what is hybrid warfare and why is it such a threat?

Pegasus spyware: World leaders demand Israeli probe

Coveware: Median ransomware payment down 40% in Q2 2021

Ransomware victim Kaseya gets master key to unlock networks

Microsoft announces takedown of domains used for BEC schemes

Researchers create new approach to detect brand impersonation

XLoader Windows InfoStealer malware now upgraded to attack macOS systems

British man arrested in Spain over Twitter hack

Windows "HiveNightmare" bug could expose system files to non-admin users

Microsoft rushes fix for 'PetitPotam' attack PoC

Attackers rely on 'exotic' languages for malware creation

Canadian professionals named to IFSEC's annual security and fire influencers list

IFSEC recently revealed its annual Global Influencers for the fire and security industries, acknowledging several Canadians. Among those recognized for their achievements and leadership:

- Harold Wax, Security Director, PepsiCo
- David Sulston, Director of Security, Oxford Properties
- Sean Sportun, National Director, Strategic Accounts for Canada, GardaWorld
- Erin Cathleen Mann, Marketing & CX Manager, Multifamily, Allegion Canada (originally based in the U.S.)

https://www.canadiansecuritymag.com/canadian-professionals-named-to-ifsecs-annual-security-and-fire-influencers-list/

Click above link to read more.

Back to top

Malware infects Japanese devices ahead of Olympic Games

Olympics-themed malware that appears to be targeting Japanese PCs was discovered days before the opening ceremony.

The malware was found on July 21 and analyzed by Japanese security company Mitsui Bussan Secure Directions (MBSD), The Record reports. It's designed to wipe files from target systems; however, it doesn't delete everything. The malware searches for specific file types located in the personal Windows folder "C:/Users/<username>/".

https://www.darkreading.com/endpoint/malware-infects-japanese-devices-ahead-of-olympic-games

Click above link to read more.

Back to top

Cyber-attacks: what is hybrid warfare and why is it such a threat?

Washington and Moscow are engaged in a war of words over a spate of ransomware attacks against organisations and businesses in the US and other countries. These increasingly sophisticated cyber-attacks represent a new type of warfare aimed at disorganising and even destroying a nation’s economy.

This has been called “hybrid warfare”. It’s a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare.

https://www.canadiansecuritymag.com/cyber-attacks-what-is-hybrid-warfare-and-why-is-it-such-a-threat/

Click above link to read more.

Back to top

Pegasus spyware: World leaders demand Israeli probe

French President, US Lawmakers and Others Call for Urgent 'Hacking for Hire' Review

Calls are growing for an investigation into how commercial Pegasus spyware developed by Israel's NSO Group gets sold to autocratic governments and used to target journalists, lawyers, human rights advocates and others.

On Monday, four U.S. Democratic lawmakers called for legislation or an executive order to crack down on privately built spyware. They also called for consideration of potential sanctions again all individuals and organizations that sell such software.

https://www.bankinfosecurity.com/pegasus-spyware-world-leaders-demand-israeli-probe-a-17152

Click above link to read more.

Back to top

Coveware: Median ransomware payment down 40% in Q2 2021

The median ransomware payment declined 40% between the first and second quarter of this year, according to new research from incident response vendor Coveware.

In a blog post Friday, titled "Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority," Coveware included new ransomware statistics as well as various observations about the present and future state of ransomware as of the second quarter of 2021.

https://searchsecurity.techtarget.com/news/252504487/Coveware-Median-ransomware-payment-down-40

Click above link to read more.

Back to top

Ransomware victim Kaseya gets master key to unlock networks

The Florida company whose software was exploited in the devastating Fourth of July weekend ransomware attack, Kaseya, has received a universal key that will decrypt all of the more than 1,000 businesses and public organizations crippled in the global incident.

Kaseya spokeswoman Dana Liedholm would not say Thursday how the key was obtained or whether a ransom was paid. She said only that it came from a “trusted third party” and that Kaseya was distributing it to all victims.

https://www.canadiansecuritymag.com/ransomware-victim-kaseya-gets-master-key-to-unlock-networks/

Click above link to read more.

Back to top

Microsoft announces takedown of domains used for BEC schemes

Microsoft has announced the takedown of 17 domains that a threat group operating out of West Africa used to host fake Microsoft websites when conducting business email compromise attacks.

Sophisticated cybercriminals have engaged in a complex scheme to target Microsoft’s O365 customers and services and conduct malicious activity including business email compromise attacks, using stolen credentials to access O365 customer email accounts, imitate customer employees, and target their trusted networks, vendors, contractors and agents in an effort to deceive them into sending or approving fraudulent financial payments," Microsoft says in court documents.

https://www.bankinfosecurity.com/microsoft-announces-takedown-domains-used-for-bec-schemes-a-17114

Click above link to read more.

Back to top

Researchers create new approach to detect brand impersonation

A team of Microsoft researchers developed and trained a Siamese Neural Network to detect brand impersonation attacks.

Security researchers have designed a new way to detect brand impersonation using Siamese Neural Networks, which can learn and make predictions based on smaller amounts of data.

https://www.darkreading.com/endpoint/researchers-create-new-approach-to-detect-brand-impersonation/d/d-id/1341549

Click above link to read more.

Back to top

XLoader Windows InfoStealer malware now upgraded to attack macOS systems

Cybersecurity researchers on Wednesday disclosed details of an evolving malware that has now been upgraded to steal sensitive information from Apple's macOS operating system.

The malware, dubbed "XLoader," is a successor to another well-known Windows-based info stealer called Formbook that's known to vacuum credentials from various web browsers, collect screenshots, log keystrokes, and download and execute files from attacker-controlled domains.

https://thehackernews.com/2021/07/xloader-windows-infostealer-malware-now.html

Click above link to read more.

Back to top

British man arrested in Spain over Twitter hack

Spanish police have arrested a 22-year-old UK citizen in connection with the hacking of 130 high-profile Twitter accounts, including those of Elon Musk, Barack Obama and Kanye West.

The hacked accounts tweeted followers, encouraging them to join a Bitcoin scam, in July last year.

https://www.bbc.com/news/technology-57916521

Click above link to read more.

Back to top

Windows "HiveNightmare" bug could expose system files to non-admin users

Following a string of recent flaws discovered in Windows, the latest vulnerability dubbed "HiveNightmare" could allow someone to compromise your system by exploiting a security weakness that affects the Registry. At this point, no patch is available to fix the flaw; instead Microsoft is offering a series of workarounds designed to protect your computer from this new dilemma.

Specifically, HiveNightmare (also known as SeriousSAM) lets non-admin users access the contents of different Windows system files, including the Security Account Manager (SAM), SYSTEM, and SECURITY Registry hive files. Located in the system32\config directory, the SAM is home to such critical data as user accounts and passwords, so normally it's accessible only to privileged accounts and processes and locked when in use.

https://www.techrepublic.com/article/windows-hivenightmare-bug-could-expose-system-files-to-non-admin-users/?ftag=TREa988f1c&bhid=42420269&mid=13445865&cid=2176068089

Click above link to read more.

Back to top

Microsoft rushes fx for ‘PetitPotam’ attack PoC

Microsoft was quick to respond with a fix to an attack dubbed “PetitPotam” that could force remote Windows systems to reveal password hashes that could then be easily cracked. To thwart an attack, Microsoft recommends system administrators stop using the now deprecated Windows NT LAN Manager (NTLM).

Security researcher Gilles Lionel first identified the bug on Thursday and also published proof-of-concept (PoC) exploit code to demonstrate the attack. The following day, Microsoft issued an advisory that included workaround mitigations to protect systems.

https://threatpost.com/microsoft-petitpotam-poc/168163/

Click above link to read more.

Back to top

Attackers rely on 'exotic' languages for malware creation

Malware developers increasingly are relying on "exotic" programming languages - such as Go, Rust, DLang and Nim - to create malicious code that can avoid security detection by tools and add a layer of obfuscation to an attack, according to a report released Monday by BlackBerry.

The BlackBerry researchers found malware developers are creating a new array of loaders and droppers using these four languages to deliver or disguise remote access Trojans, or RATs, as well as malicious versions of legitimate tools, such as Cobalt Strike, to potential victims, the report notes.

https://www.bankinfosecurity.com/attackers-rely-on-exotic-languages-for-malware-creation-a-17142

Click above link to read more.

Back to top

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

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