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

June 1, 2021

Challenge yourself with our NEW Phishing quiz!

Register for Security Day: June 23, 2021

This week's stories:

🍁Canada Post reports data breach to 44 large businesses, 950K customers affected

French authorities seize control of their third dark web marketplace

It's ransomware, or maybe a dark wiper, and it's striking targets in Israel

Vishing attacks are on the rise

Legality of collecting faces online challenged

Patient info released to media outlets after Waikato DHB cyberattack

Rowhammer reach extended for new attack method

Enterprises applying OS patches faster as endpoint risks grow

Fujitsu SaaS hack sends govt. of Japan scrambling

Nobelium phishing campaign poses as USAID

Canada Post reports data breach to 44 large businesses, 950K customers affected

A malware attack on one of Canada Post's suppliers has caused a data breach affecting 44 of the company's large business clients and their 950,000 receiving customers, the postal agency confirmed Wednesday.

It said the information affected is from July 2016 to March 2019, and 97 per cent of it comprised the names and addresses of receiving customers. The remaining three per cent contained email addresses and/or phone numbers, the company said.

https://globalnews.ca/news/7894760/canada-post-data-breach/

Click above link to read more.

Back to top

French authorities seize control of their third dark web marketplace

French authorities have dismantled their third dark web marketplace over the last four years after they seized control of “Le Monde Parallèle” (The Parallel World) last week.

Active since early 2020, the site was taken down in an operation coordinated by the French National Directorate of Intelligence and Customs Investigations.

https://therecord.media/french-authorities-seize-their-third-dark-web-marketplace/

Click above link to read more.

Back to top

It’s ransomware, or maybe a dark wiper, and it’s striking targets in Israel

Researchers say they have uncovered never-before-seen disk-wiping malware that is disguising itself as ransomware as it unleashes destructive attacks on Israeli targets.

Apostle, as researchers at security firm SentinelOne are calling the malware, was initially deployed in an attempt to wipe data but failed to do so, likely because of a logic flaw in its code.

https://arstechnica.com/gadgets/2021/05/disk-wiping-malware-with-irananian-fingerprints-is-striking-israeli-targets/

Click above link to read more.

Back to top

Vishing attacks are on the rise

Companies are becoming more aware of potential cybersecurity threats and taking measures to protect their critical assets and increase security. However, one aspect of cyberattacks that often goes unforeseen (until it’s too late) is vishing, and vishing attacks are on the rise.

The U.S. Federal Bureau of Investigation amid COVID-19 pandemic. Vishing, also known as “voice phishing,” is a form of cybercrime. It uses social engineering techniques over the phone to elicit and obtain information that could be personal or confidential. Vishing sounds like it would be easy to detect. However, most cybercriminals do ample research before carrying out an attack, making their pretexts or stories seem very believable.

https://www.social-engineer.com/vishing-attacks-are-on-the-rise/

Click above link to read more.

Back to top

Legality of collecting faces online challenged

Clearview AI, a US firm with a database of three billion facial images from the internet, is facing a new legal challenge from privacy campaigners.

Privacy International and others argue its methods of collecting photos and selling them to private firms and the police "go beyond what we could ever expect as online users".

https://www.bbc.com/news/technology-57268121

Click above link to read more.

Back to top

Patient info released to media outlets after Waikato DHB cyberattack

Yesterday, hackers who launched a cyberattack on Waikato District Health Board's system released patient information to several media outlets, including the NZ Herald.

"We are aware that the media have received what appears to be personal and patient information from Waikato DHB information systems," the hospital group said in an update.

The media agencies refused to divulge the information publicly and have turned it over to the police.

https://www.healthcareitnews.com/news/apac/patient-info-released-media-outlets-after-waikato-dhb-cyberattack

Click above link to read more.

Back to top

Rowhammer reach extended for new attack method

Google researchers have uncovered a new variation on the Rowhammer hardware attack that enables an adversary to flip transistor states from further distances than previously thought possible.

The new take on Rowhammer, dubbed "Half-Double," shows how an attacker can turn a targeted transistor to an on or off state by repeatedly flipping transistors from one and two rows over.

https://searchsecurity.techtarget.com/news/252501468/Rowhammer-reach-extended-for-new-attack-method

Click above link to read more.

Back to top

Enterprises applying OS patches faster as endpoint risks grow

Over the past 12 months, many organizations have become slightly faster at applying operating system patches on endpoint systems despite the challenges associated with maintaining remote devices, a new report from Absolute Software shows.

Even so, the length of time that enterprise endpoints were out-of-date with available OS patches remained relatively high at 80 days.

https://beta.darkreading.com/endpoint/enterprises-applying-os-patches-faster-as-endpoint-risks-grow

Click above link to read more.

Back to top

Fujitsu SaaS hack sends govt. of Japan scrambling

Threat actors have stolen files from several official government agencies of Japan by hacking into Fujitsu's software-as-a-service (SaaS) platform and gaining access to its systems.

The Japan-based tech giant temporarily disabled ProjectWEB enterprise after learning of the attack, which is known to have affected the Ministry of Land, Infrastructure, Transport, and Tourism; the Cabinet Secretariat; and the Narita Airport so far but may have had other victims, according to a post on analyst firm Recorded Future's The Record.

https://threatpost.com/fujitsu-saas-hack-japan-scrambling/166517/

Click above link to read more.

Back to top

Nobelium phishing campaign poses as USAID

Microsoft uncovered the SolarWinds crooks using mass-mail service Constant Contact and posing as a U.S.-based development organization to deliver malicious URLs to more than 150 organizations.

The cybercriminal group behind the notorious SolarWinds attack is at it again with a sophisticated mass email campaign aimed at delivering malicious URLs with payloads enabling network persistence so the actors can conduct further nefarious activities.

https://threatpost.com/solarwinds-nobelium-phishing-attack-usaid/166531/

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