July 6, 2021

Challenge yourself with our NEW Passwords Security quiz!

This week's stories:

Canada 'lucky' no big hits taken from world's largest ransomware attack: expert

Canadian companies are "lucky" that the world's largest ransomware attack to date hasn't affected them more substantially so far, one cybersecurity expert said.

On Friday, IT software provider Kaseya was hit with a ransomware attack that has since affected thousands of companies around the world. Ransomware is when a company's online system is hijacked and locked unless a ransom is paid.

https://globalnews.ca/news/8004670/revil-kaseya-ransomware-attack-canada/

Click above link to read more.

Back to top

Private moments captured on home security cameras being live streamed again on website

Authorities have tried to stop the site, but streaming unsecured cameras isn't illegal.

An elderly woman in bed next to a commode toilet in Quebec, a child playing in a living room in Alberta, a woman working from home in Ontario and kitchen staff working in a coffee shop.

These private moments have all been visible to anyone on the internet through a website that's live streaming thousands of unsecured cameras around the world in real time.

https://www.cbc.ca/news/canada/toronto/website-live-streaming-security-cameras-private-1.6083168

Click above link to read more.

Back to top

Cyberattack on Kaseya nets more than 1,000 victims, $70m ransom demand

A massive supply-chain ransomware attack targeting managed service providers (MSPs) who use the Kaseya Virtual System Administrator (VSA) has left data at more than 1,000 companies encrypted and the attackers demanding $70 million in ransom.

The attack—which the REvil ransomware group launched on July 2, just before the US holiday weekend—exploited multiple vulnerabilities, including a zero-day flaw that was in the process of remediation, according to security firms. REvil, a ransomware-as-a-service group, claims that more than a million systems were compromised and encrypted, and posted a ransomware demand to its blog on Sunday, July 4, saying if it receives the $70 million ransom payment, it will publicly publish the decryptor.

https://beta.darkreading.com/attacks-breaches/cyberattack-on-kaseya-nets-more-than-1-000-victims-70m-ransom-demand

Click above link to read more.

Back to top

CISA Offers New Mitigation for PrintNightmare bug

The U.S. government has stepped in to offer a mitigation for a critical remote code execution (RCE) vulnerability in the Windows Print Spooler service that may not have been fully patched by Microsoft's initial effort to fix it.

To mitigate the bug, dubbed PrintNightmare, the CERT Coordination Center (CERT/CC) has released a VulNote for CVE-2021-1675 urging system administrations to disable the Windows Print Spooler service in Domain Controllers and systems that do not print, the Cybersecurity Infrastructure and Security Administration (CISA) said in a release Thursday. CERT/CC is part of the Software Engineering Institute, a federally funded research center operated by Carnegie Mellon University.

https://threatpost.com/cisa-mitigation-printnightmare-bug/167515/

Click above link to read more.

Back to top

UK, US agencies warn of large-scale global brute force attack targeting enterprise and cloud environments

The US and UK cybersecurity agencies warning that the Russia-linked APT28 group is behind a series of large-scale Brute-Force Attacks.

This warning alert was issued by the US National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC).

https://cybersecuritynews.com/brute-force-attack-campaign/

Click above link to read more.

Back to top

Smart devices could expose homes to thousands of cyber attacks a week

A home filled with smart devices could be exposed to thousands of hacking or unknown scanning attacks from around the world in a single week, according to a new report.

A real-world study carried out by consumer group Which recorded more than 12,000 attack attempts in a week, including 2,435 specific attempts to maliciously log into the devices with a weak default username and password.

https://www.cityam.com/smart-devices-could-expose-homes-to-thousands-of-cyber-attacks-a-week/

Click above link to read more.

Back to top

Dutch police takes down DoubleVPN, a service used by cybercrime groups

In an investigation spearheaded by Dutch police, Europol said it took down this week a service called DoubleVPN that provided virtual private network (VPN) servers and anonymity to cybercriminal gangs.

The doublevpn.com website was seized on Tuesday, June 29, 2021.

https://therecord.media/dutch-police-takes-down-doublevpn-a-service-used-by-cybercrime-groups/

Click above link to read more.

Back to top

Google to clamp down on online financial scams in Britain

Google will clamp down on financial fraud on its platform in Britain, saying on Wednesday that all financial services will need to be verified by the regulator before they can advertise.

Britain's financial watchdog issued 1,200 consumer warnings last year about scams advertised via social media platforms by fake companies, double the number in 2019.

https://www.reuters.com/world/uk/google-introduce-measures-curb-online-financial-scams-uk-2021-06-30/

Click above link to read more.

Back to top

Malicious insiders: How to protect your business

Nowadays, most people are aware of the threat posed to businesses by tech-savvy lawbreakers operating from far-flung corners of the world, such as Russia and Nigeria.

Much less attention is being paid to the vast potential damage that can be caused by aggrieved or self-interested employees from only a few feet away.

While you may not have come across the term “malicious insider” before, it is possible that you know of – or maybe even know – one of them.

https://www.intheblack.com/articles/2021/07/01/malicious-insiders-protect-business

Click above link to read more.

Back to top

Secured-Core PCs may mitigate firmware attacks, but adoption lags

When firmware-security firm Eclyspium revealed four flaws last month in a Dell firmware utility that could allow attacks against the basic system software on laptops and other devices, the company maintained that vulnerabilities posed a significant threat to users of the systems.

Microsoft, however, has argued that laptops with the latest security-attestation technology, known as Secured Core, are not susceptible to such attacks because the technology was created with the assumption that the firmware is untrustworthy.

https://beta.darkreading.com/vulnerabilities-threats/secured-core-pcs-may-mitigate-firmware-attacks-but-adoption-lags

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