July 20, 2021

Challenge yourself with our Password Security quiz!

This week's stories:

Canada joins allies blaming Chinese-backed groups for Microsoft email attack

The federal government is blaming Chinese state-sponsored cyber activity for a recent "unprecedented and indiscriminate exploitation" of Microsoft exchange servers, in an attack they say continues to put Canadians' intellectual property and personal information at risk.

In a joint statement issued Monday, Foreign Affairs Minister Marc Garneau, Defence Minister Harjit Sajjan, and Public Safety Minister Bill Blair said Canada is "confident" that China's Ministry of State Security (MSS) was behind the recent Microsoft Exchange Server hack.

https://www.ctvnews.ca/politics/canada-joins-allies-blaming-chinese-backed-groups-for-microsoft-email-attack-1.5514638

Click above link to read more.

Back to top

Microsoft Warns of Another Windows Print Spooler Vulnerability

Microsoft discovered another vulnerability in Windows Print Spooler, and until a security update arrives, the only way to defend against the flaw leaves Windows PCs unable to print documents.

"An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations," the company says. "An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights."

https://www.pcmag.com/news/microsoft-warns-of-another-windows-print-spooler-vulnerability

Click above link to read more.

Back to top

Leaked NSO group data hints at widespread Pegasus spyware infections

Israeli-based NSO Group is being blasted in a groundbreaking report that alleges that the company's controversial Pegasus malware is being used to target activists, journalists, business executives and politicians on a widespread level, using a variety of exploits — including a zero-click zero-day in iOS.

A consortium of journalists leveled the allegations in a report called Pegasus Project, which was published Sunday. It examined leaked data from the NSO Group, which revealed a cache of more than 50,000 mobile phone numbers worldwide that the firm was storing, according to the report published by the Guardian newspaper.

https://threatpost.com/nso-group-data-pegasus/167897/

Click above link to read more.

Back to top

U.S. government launches "StopRansomware" site

The U.S. government's first interagency initiative to address the growing threat of ransomware launched Wednesday.

StopRansomware.gov, a website managed by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) along with the Department of Justice (DOJ) and the White House, offers cybersecurity resources, tools and other information. The site offers tips and guidance for ransomware attack preparation, prevention and response, with focuses on best practices such as restricting users' permissions, which may prevent malware from running or limit its capability to spread through a network. More importantly, incidents can be reported directly through the website.

https://searchsecurity.techtarget.com/news/252504063/US-government-launches-StopRansomware-site

Click above link to read more.

Back to top

Abu Dhabi working to fight cybercrime in healthcare with new strategy

Abu Dhabi's Department of Health (DoH) has revealed it is working towards "securely and effectively" reducing cyber threats with the introduction of a new policy.

Unveiled earlier this week, the "Abu Dhabi Healthcare Information Security Strategy"– said to be the first of its kind in the region's healthcare sector – will focus on improving its information infrastructure to protect it from the current increase of cyberattacks taking place globally.

https://www.healthcareitnews.com/news/emea/abu-dhabi-working-fight-cybercrime-healthcare-new-strategy

Click above link to read more.

Back to top

China's cyberspies targeting Southeast Asian government entities

A sweeping and "highly active campaign" that originally set its sights on Myanmar has broadened its focus to strike a number of targets located in the Philippines, according to new research.

Russian cybersecurity firm Kaspersky, which first spotted the infections in October 2020, attributed them to a threat actor it tracks as "LuminousMoth," which it connected with medium to high confidence to a Chinese state-sponsored hacking group called HoneyMyte or Mustang Panda, given its observed victimology, tactics, and procedures.

https://thehackernews.com/2021/07/chinas-cyberspies-targeting-southeast.html

Click above link to read more.

Back to top

SonicWall warns of 'imminent ransomware campaign' targeting its EOL equipment

Networking equipment vendor SonicWall has released an urgent security alert to its customers to warn companies of **"**an imminent ransomware campaign" targeting some of its equipment.

While SonicWall did not, the company, which also operates a cybersecurity division, said the attackers are targeting an old vulnerability that has been fixed in recent versions of its firmware.

https://therecord.media/sonicwall-warns-of-imminent-ransomware-campaign-targeting-its-eol-equipment/

Click above link to read more.

Back to top

FCC finalizes plan to rip and replace Chinese telecom gear

The Federal Communications Commission has finalized a $1.9 billion plan that will help smaller, rural telecommunications carriers pay to rip and replace technology from the Chinese firms Huawei and ZTE.

In June 2020, the FCC designated Huawei and ZTE as threats to U.S. national security, noting that if the companies' gear is used on U.S. telecom networks, the firms could spy on communications on behalf of the Chinese government.

https://www.bankinfosecurity.com/fcc-finalizes-plan-to-rip-replace-chinese-telecom-gear-a-17075

Click above link to read more.

Back to top

Windows Hello bypassed using infrared image

Researchers from security firm CyberArk bypassed Windows Hello, the biometrics authentication system included with all Windows 10 versions, using just an infrared image of the device's owner.

Discovered by CyberArk security researcher Omer Tsarfati, the vulnerability resided in Windows Hello's facial recognition feature, and more specifically, in how Windows Hello processed data from USB-connected webcams.

https://therecord.media/windows-hello-bypassed-using-infrared-image/

Click above link to read more.

Back to top

Protect your smartphone from radio-based attacks

By now, most of us are aware that smartphones are powerful computers and should be treated as such. It's not a coincidence that most of the security tips given to smartphone users – such as refraining from opening suspicious links or downloading untrusted apps – also apply to PCs.

But unlike PCs, smartphones contain a plethora of radios – typically cellular, Wi-Fi, Bluetooth and Near Field Communication (NFC) – that enable wireless communication in a variety of circumstances, and these radios are designed to remain turned on as the user moves through the world. It's important for all smartphone users to understand the security implications of these wireless interfaces.

https://www.helpnetsecurity.com/2021/07/19/smartphone-radio-based-attacks/

Click above link to read more.

Back to top

Banks now rely on a few cloud computing giants. That's creating some unexpected new risks

Banks' growing reliance on cloud computing could pose a risk to financial stability and will require stricter oversight, according to top executives from the UK's central bank.

In a report focusing on financial stability in the UK over the past few months, the Bank of England drew attention to the increasing adoption of public cloud services, and voiced concerns about those services being provided by only a handful of huge companies that dominate the market.

https://www.zdnet.com/article/banks-now-rely-on-a-few-cloud-computing-giants-thats-creating-some-unexpected-new-risks/

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

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