May 11, 2021

Challenge yourself with our Spotting a Fake quiz!

This week's stories:

Ottawa invests $80 million to support cybersecurity R&D and commercialization

This week, Canadian Minister of Innovation, Science and Industry François-Philippe Champagne announced the launch of the new Cyber Security Innovation Network program with an investment of $80 million over four years.

In a May 6 news release, The Innovation, Science and Economic Development Canada (ISED) says it is currently seeking to enter into the four-year, non-repayable contribution agreement with a selected applicant who will form the national network with the goal to enhance research and development, and increase commercialization of cybersecurity products, services and/or processes across Canada.

The program was first announced in the 2019 federal budget.

In addition, the network will support the development of skilled cybersecurity talent across the country, including the recruitment and retention of faculty, trainers, and instructors. It will also provide more

resources to curriculum development, training, reskilling and upskilling of the cybersecurity workforce through initiatives designed and delivered in collaboration with industry partners.

https://www.itworldcanada.com/article/ottawa-invests-80-million-to-support-cybersecurity-rd-and-commercialization/447084

Click link above to read more

Major U.S. Pipeline Crippled in Ransomware Attack

A ransomware attack has halted pipeline activities for the Colonial Pipeline Co., which supplies the East Coast with roughly 45 percent of its liquid fuels.

In a statement released on Saturday, Colonial Pipeline said it has temporarily halted pipeline operations in response to a cyberattack impacting the company starting Friday.

“On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware,” the company wrote in the Saturday statement.

As a precaution, the company took key systems offline to avoid further infections, it said.

“In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems,” the company stated. “Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing.”

https://threatpost.com/pipeline-crippled-ransomware/165963/

Click link above to read more

City of Tulsa hit by ransomware over the weekend

The city of Tulsa, Oklahoma, one of the 50 largest cities in the US, has been hit by a ransomware attack over the weekend that affected the city government’s network and brought down official websites.

The attack, which took place on the night between Friday and Saturday, is currently being handled by the city’s IT team, which have managed to restore the city’s websites, a spokesperson told The Record.

IT teams are still working to recover impacted systems from backups.

The attack is believed to have impacted only a small portion of the city’s network. The intrusion could have had much more severe consequences if it had hit the city during a working day when most computers would have been turned on.

https://therecord.media/city-of-tulsa-hit-by-ransomware-over-the-weekend/

Click link above to read more

Is it still a good idea to require users to change their passwords?

For as long as corporate IT has been in existence, users have been required to change their passwords periodically. In fact, the need for scheduled password changes may be one of the most long-standing of all IT best practices.

Recently, however, things have started to change. Microsoft has reversed course on the best practices that it has had in place for decades and no longer recommends that organizations require users to change passwords periodically. Organizations are being forced to consider, perhaps for the first time, whether or not requiring periodic password changes is a good idea.

According to Microsoft, requiring users to change their passwords frequently does more harm than good.

Humans are notoriously resistant to change. When a user is forced to change their password, they will often come up with a new password that is based on their previous password. A user might, for example, append a number to the end of their password and then increment that number each time that a password is required. Similarly, if monthly password changes are required, a user might incorporate the

name of a month into the password and then change the month every time a password change is required (for example, MyM@rchP@ssw0rd).

https://thehackernews.com/2021/05/is-it-still-good-idea-to-require-users.html

Click link above to read more

Over 25% Of Tor Exit Relays Spied On Users' Dark Web Activities

An unknown threat actor managed to control more than 27% of the entire Tor network exit capacity in early February 2021, a new study on the dark web infrastructure revealed.

"The entity attacking Tor users is actively exploiting tor users since over a year and expanded the scale of their attacks to a new record level," an independent security researcher who goes by the name nusenu said in a write-up published on Sunday. "The average exit fraction this entity controlled was above 14% throughout the past 12 months."

It's the latest in a series of efforts undertaken to bring to light malicious Tor activity since December 2019. The attacks, which are said to have begun in January 2020, were first documented and exposed by the same researcher in August 2020.

Tor is open-source software for enabling anonymous communication on the Internet. It obfuscates the source and destination of a web request by directing network traffic through a series of relays in order to mask a user's IP address and location and usage from surveillance or traffic analysis. While middle relays typically take care of receiving traffic on the Tor network and pass it along, an exit relay is the final node that Tor traffic passes through before it reaches its destination.

https://thehackernews.com/2021/05/over-25-of-tor-exit-relays-are-spying.html

Click link above to read more

US physics lab Fermilab exposes proprietary data for all to see

Multiple unsecured entry points allowed researchers to access data belonging to Fermilab, a national particle physics and accelerator lab supported by the Department of Energy.

This week, security researchers Robert Willis, John Jackson, and Jackson Henry of the Sakura Samurai ethical hacking group have shared details on how they were able to get their hands on sensitive systems and data hosted at Fermilab.

After enumerating and peeking inside the fnal.gov subdomains using commonly available tools like amass, dirsearch, and nmap, the researchers discovered open directories, open ports, and unsecured services that attackers could have used to extract proprietary data.

https://arstechnica.com/gadgets/2021/05/researchers-peek-into-proprietary-data-of-us-particle-physics-lab-fermilab/

Click link above to read more

New Spectre Flaws in Intel and AMD CPUs Affect Billions of Computers

When Spectre, a class of critical vulnerabilities impacting modern processors, was publicly revealed in January 2018, the researchers behind the discovery said, "As it is not easy to fix, it will haunt us for quite some time," explaining the inspiration behind naming the speculative execution attacks.

Indeed, it's been more than three years, and there is no end to Spectre in sight.

A team of academics from the University of Virginia and University of California, San Diego, have discovered a new line of attack that bypasses all current Spectre protections built into the chips, potentially putting almost every system — desktops, laptops, cloud servers, and smartphones — once again at risk just as they were three years ago.

https://thehackernews.com/2021/05/new-spectre-flaws-in-intel-and-amd-cpus.html

Click link above to read more

---

12 Security Flaws Russian Spy Hackers Are Exploiting in the Wild

Cyber operatives affiliated with the Russian Foreign Intelligence Service (SVR) have switched up their tactics in response to previous public disclosures of their attack methods, according to a new advisory jointly published by intelligence agencies from the U.K. and U.S. Friday.

"SVR cyber operators appear to have reacted [...] by changing their TTPs in an attempt to avoid further detection and remediation efforts by network defenders," the National Cyber Security Centre (NCSC) said.

These include the deployment of an open-source tool called Sliver to maintain their access to compromised victims as well as leveraging the ProxyLogon flaws in Microsoft Exchange servers to conduct post-exploitation activities.

https://thehackernews.com/2021/05/top-11-security-flaws-russian-spy.html

Click link above to read more

How Patched Android Chip Flaw Could Have Enabled Spying

A severe vulnerability in a system on certain Qualcomm chips, which has been patched, potentially could have enabled attackers to remotely control Android smartphones, access users' text messages and call histories and listen in on conversations, according to a new report from researchers at security company Check Point Software Technologies.

A spokesperson from Qualcomm tells Information Security Media Group that it provided a patch to device manufacturers in December 2020 (see: Snapdragon Chip Flaws Could Facilitate Mass Android Spying).

"We have no evidence the vulnerability is being exploited," the spokesperson says. "For this vulnerability to even begin to work, a device would need to be severely compromised to start with, which would be a bigger problem."

https://www.bankinfosecurity.com/how-patched-android-chip-flaw-could-have-enabled-spying-a-16545

Click link above to read more

'BadAlloc' vulnerabilities spell trouble for IoT, OT devices

Microsoft disclosed several potentially dangerous vulnerabilities in IoT and operational technology products last week, but it's still unclear what mitigations and patches are available.

In a blog post, Microsoft's Security Response Center detailed its discovery of 25 memory allocation vulnerabilities, which its security research group refers to as "BadAlloc." Exploitation of the vulnerabilities, many of which are critical, could lead to remote code execution (RCE), allowing adversaries to bypass security controls in order to execute malicious code or cause a system to crash. The BadAlloc vulnerabilities cover a wide range of technology, including consumer and medical IoT, industrial IoT, operational technology (OT) and industrial control systems (ICSes).

Microsoft said given the pervasiveness of IoT and OT devices, these vulnerabilities, if successfully exploited, represent a significant risk for organizations of all kinds.

"The vulnerabilities exist in standard memory allocation functions spanning widely used real-time operating systems (RTOS), embedded software development kits (SDKs) and C standard library (libc) implementations," the report said.

https://searchsecurity.techtarget.com/news/252500375/BadAlloc-vulnerabilities-spell-trouble-for-IoT-OT-devices

Click link above to read more

---

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