June 29, 2021

Challenge yourself with our Phishing quiz!

This week's stories:

- **Canadian Navy Team wins DOD's annual cyber defence exercise**
- **CSE responded to more than 2,000 cyber attacks last year amid heightened concern over Chinese, Russian hacks**
- **The dangers of action bias: Is it always better to act quickly?**
- **Arrested Clop gang members laundered over $500M in ransomware payments**
- **Irish ransomware attack cost estimate: $600M**
- **Should making a ransomware payment be illegal? It's complicated**
- **Bios disconnect: new high-severity bugs affect 128 Dell PC and tablet models**
- **EU wants emergency team for 'nightmare' cyberattacks**
- **Eye clinic cyberattack may have exposed info from 500k patients**
- **COVID, gift cards and phony acquisitions top BEC attack trends**
- **Critical VMWare Carbon Black bug allows authentication bypass**
- **Attacks erase Western Digital network-attached storage devices**
- **Hackers abused Python Package Index (PyPI) that secretly installs cryptominers on affected computers**

Canadian Navy Team wins DOD's annual cyber defence exercise

A team from the Royal Canadian Navy came out on top in the Defense Department's annual Cyber Flag 21-2 training exercise, besting 430 cyber professionals from across the U.S. military's joint services, other agencies and international partners, the commander of U.S. Cyber Command said Friday.

Army Gen. Paul M. Nakasone announced that Team 15 from the Royal Canadian Navy won this year's cyber defense-focused Cyber Flag 21-2 exercise, or "Big Flag," during the event's virtual closing ceremony.

https://www.defense.gov/Explore/News/Article/Article/2673318/canadian-navy-team-wins-dods-annual-cyber-defense-exercise/

Click above link to read more.

Back to top

CSE responded to more than 2,000 cyber attacks last year amid heightened concern over Chinese, Russian hacks

Canada's digital spy agency responded to more than 2,000 attacks on the federal government and its critical infrastructure partners last year, according to a new report, amid heightened concerns over the use of cyber warfare tactics by foreign actors.

In its annual report, the Communications Security Establishment (CSE) said it provided assistance to the Government of Canada or its critical infrastructure partners 2,206 times, including 84 incidents "affecting Canada's health sector." It is the latest in a number of recent reports detailing the higher frequency of cyberattacks being directed toward Canada, including a recent report by the Canadian Security Intelligence Service (CSIS) that found "espionage and foreign interference activity at levels not seen since the Cold War," mostly carried out by Chinese and Russian-backed actors.

https://montrealgazette.com/news/federal-spy-agency-responded-to-more-than-2200-cyber-attacks-last-year-amid-heightened-concern-over-chinese-russian-hacks

Click above link to read more.

Back to top

The dangers of action bias: Is it always better to act quickly?

When a data breach hits, the best response is to act quickly and forcefully … right?

Not necessarily, experts say. The impulse for cybersecurity pros to have control over a situation is common — after all, you don't want to be the CISO who didn't act after learning about an attack — but hastily made decisions may do more harm than good or create a problem where one didn't exist.

https://beta.darkreading.com/careers-and-people/the-danger-of-action-bias-is-it-always-better-to-act-quickly

Click above link to read more.

Back to top

Arrested Clop gang members laundered over $500M in ransomware payments

The members of the Clop ransomware gang that were arrested last week in Ukraine as part of an international law enforcement action also operated money laundering services for multiple cybercrime groups.

According to cryptocurrency exchange portal Binance, the group engaged in both cyber-attacks and "a high-risk exchanger" that laundered funds for the Clop ransomware gang and other criminal groups.

https://therecord.media/arrested-clop-gang-members-laundered-over-500m-in-ransomware-payments/

Click above link to read more.

Back to top

Irish ransomware attack cost estimate: $600M

The recovery costs for the May ransomware attack on Health Service Executive, Ireland's publicly funded healthcare system, is likely to total $600 million, says Paul Reid, HSE's director general.

Reid provided the estimate at a Wednesday hearing of a health committee of the country's legislative body, Oireachtas.

https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931

Click above link to read more.

Back to top

Should making a ransomware payment be illegal? It's complicated

Should ransomware payments be illegal? Policymakers and security professionals have found themselves wrestling with that question after a spree of high-profile ransomware attacks gave criminals multi-million-dollar paydays and crippled organisations in sectors ranging from energy to healthcare. However, despite the simplicity of the question, the answer is complicated.

https://www.verdict.co.uk/ransomware-payment-illegal/

Click above link to read more.

Back to top

BIOS disconnect: New high-severity bugs affect 128 Dell PC and tablet models

Cybersecurity researchers on Thursday disclosed a chain of vulnerabilities affecting the BIOSConnect feature within Dell Client BIOS that could be abused by a privileged network adversary to gain arbitrary code execution at the BIOS/UEFI level of the affected device.

"As the attacker has the ability to remotely execute code in the pre-boot environment, this can be used to subvert the operating system and undermine fundamental trust in the device," researchers from enterprise device security firm Eclypsium said. "The virtually unlimited control over a device that this attack can provide makes the fruit of the labor well worth it for the attacker."

https://thehackernews.com/2021/06/bios-disconnect-new-high-severity-flaws.html

Click above link to read more.

Back to top

EU wants emergency team for 'nightmare' cyberattacks

The European Commission has announced plans to build a Joint Cyber Unit to tackle large scale cyber-attacks.

Recent ransomware incidents on critical services in Ireland and the US has "focused minds", the commission said.

https://www.bbc.com/news/technology-57583158

Click above link to read more.

Back to top

Eye clinic cyberattack may have exposed info from 500k patients

A cybersecurity incident at an Iowa group eye clinic could have exposed the personal information of nearly 500,000 current and former patients.

According to a press release this week, back in February Wolfe Eye Clinic was the target of a deliberate cyberattack.

Because of the complexity and scale of the incident, said the company, the full scope of potentially affected data was not realized until May 28.

https://www.healthcareitnews.com/news/eye-clinic-cyberattack-may-have-exposed-info-500k-patients

Click above link to read more.

Back to top

COVID, gift cards and phony acquisitions top BEC attack trends

New research from Cisco Talos shows cybercriminals are still using the COVID-19 pandemic for BEC attacks to steal millions, but in slightly different ways.

Business email compromise scams are becoming more common, with numerous tricks, including preying on confusion around the COVID-19 pandemic, used as popular lures by cybercriminals.

https://searchsecurity.techtarget.com/news/252502877/COVID-gift-cards-and-phony-acquisitions-top-BEC-attack-trends

Click above link to read more.

Back to top

Critical VMWare Carbon Black bug allows authentication bypass

VMware has fixed an uber-severe bug in its Carbon Black App Control (AppC) management server: A server whose job is to lock down critical systems and servers so they don’t get changed willy-nilly.

AppC also ensures that organizations stay in continuous compliance with regulatory mandates.

https://threatpost.com/vmware-carbon-black-authentication-bypass/167226/

Click above link to read more.

Back to top

Attacks erase Western Digital network-attached storage devices

Companies and individuals using older models of Western Digital network-attached storage (NAS) drives suffered what appears to be an attack that possibly exploited a 2018 vulnerability to reset the drives to the factory defaults and deleting data, according to customer comments and company statements.

Western Digital has confirmed that many customers owning its WD My Book Live and My Book Live Duo storage appliances have suffered compromises through a remote code execution vulnerability. From log files posted to the company's support forum, the attack appeared to happen on June 23 and 24, when drives were reset to factory defaults.

https://www.darkreading.com/attacks-breaches/attacks-erase-western-digital-network-attached-storage-drives/d/d-id/1341419

Click above link to read more.

Back to top

Hackers abused Python Package Index (PyPI) that secretly installs cryptominers on affected computers

Sonatype catches a new PyPI cryptomining malware where the malicious typosquatting packages infiltrating the PyPI repository that secretly pulls in cryptominers on the affected machines.

https://cybersecuritynews.com/pypi-cryptomining-malware/

Click above link to read more.

Back to top