June 8, 2021

Challenge yourself with our Phishing quiz!

Register for Security Day: June 23, 2021

This week's stories:

VMware releases report detailing surge in cyberattacks

VMware, Inc. released the findings from the fourth installment of the Global Security Insights Report. The Canada report is based on an online survey of 251 Canadian CIOs, CTOs and CISOs in December 2020. The report explores the impact of cyberattacks and breaches on organizations and details how security teams are adapting to these challenges.

Accelerated digital transformation has caused security teams to face evolving threats as cybercriminals seize the opportunity to execute targeted attacks exploiting fast-tracked innovation and the anywhere workforce. Close to 86 percent of organizations surveyed experienced cyberattacks due to more employees working from home, highlighting the vulnerabilities in legacy security technology and postures.

https://www.canadiansecuritymag.com/vmware-releases-report-detailing-surge-in-cyberattacks/

Click above link to read more.

Back to top

ANOM: Hundreds arrested in massive global crime sting using messaging app

More than 800 suspected criminals have been arrested worldwide after being tricked into using an FBI-run encrypted messaging app, officials say.

The operation, jointly conceived by Australia and the FBI, saw devices with the ANOM app secretly distributed among criminals, allowing police to monitor their chats about drug smuggling, money laundering and even murder plots.

Officials called it a watershed moment.

Targets included drug gangs and people with links to the mafia.

https://www.bbc.com/news/world-57394831?utm_term=OZY&utm_campaign=pdb&utm_content=Tuesday_06.08.21&utm_source=Campaigner&utm_medium=email

Click above link to read more.

Back to top

The true cost of a ransomware attack

Companies need to prepare for the costs of an attack now, before they get attacked. Here's a checklist to help.

If anyone needed further proof that ransomware is one of the most important digital threats organizations currently face, the recent attacks on Colonial Pipeline; the Washington, DC, police department; Apple; and Ireland's national health service are all glaringly emblematic of the problem.

According to a recent Sophos survey, 51% of responding organizations were hit with ransomware last year, and the increasingly brazen attacks being carried out through ransomware-as-a-service (RaaS) syndicates suggest that the trend is likely to continue — even amid recent government efforts to shut down RaaS infrastructure.

https://beta.darkreading.com/vulnerabilities-threats/the-true-cost-of-a-ransomware-attack

Click above link to read more.

Back to top

Microsoft 365: Most Common Threat Vectors & Defensive Tips

Security pros discuss the most typical ways attackers leverage Microsoft 365 and share their guidance for defenders.

As more organizations have grown reliant on Microsoft 365, Google Cloud, and Amazon Web Services, cybercriminals have begun to realize that the shift benefits them and are consequently tailoring their attacks to take advantage of the major cloud platforms in use by organizations.

https://www.darkreading.com/theedge/microsoft-365-most-common-threat-vectors-and-defensive-tips/b/d-id/1341179

Click above link to read more.

Back to top

Encrypted EncroChat network: police arrest more suspects

More customers of the now defunct encrypted communications service EncroChat are getting busted by police.

EncroChat previously sold smartphones for about $1,000, with a six-month service plan costing $1,700.

https://www.bankinfosecurity.com/blogs/encrypted-encrochat-network-police-arrest-more-suspects-p-3049

Click above link to read more.

Back to top

Attack on meat supplier came from REvil, ransomware's most cut-throat gang

The cyberattack that halted some operations at the world's biggest meat processor this week was the work of REvil, a ransomware franchise that's known for its ever-escalating series of cut-throat tactics designed to extort the highest price.

https://arstechnica.com/gadgets/2021/06/attack-on-meat-supplier-came-from-revil-ransomwares-most-cut-throat-gang/

Click above link to read more.

Back to top

Ransomware attack disrupts Massachusetts Ferries

A ransomware attack has caused delays and disruptions at Steamship Authority, the largest ferry service in Massachusetts, and has disrupted ferry transports between mainland US and the Martha's Vineyard and Nantucket islands.

The attack took place earlier today, according to a series of tweets posted on the company's official Twitter account.

https://therecord.media/ransomware-attack-disrupts-massachusetts-ferries/

Click above link to read more.

Back to top

Interpol has Intercepted $83 Million in Illicit Funds Transferred from Victims to Cybercriminals

Interpol had coordinated an operation that was codenamed HAECHI-I. The purpose of this operation was to curb the increase in online fraud and intercept the transfer of illicit funds from the victims to the perpetrators of the crime.

The HAECHI-I team comprised of more than 40 law enforcement officers across the Asia Pacific region. This operation is the first in a three-year project to tackle cyber financial crime.

https://cybersecuritynews.com/interpol-has-intercepted-83-million/

Click above link to read more.

Back to top

Hackers use Colonial pipeline ransomware news for phishing attack

Cyberattackers are now using the notoriety of the Colonial Pipeline ransomware attack to leverage further phishing attacks, according to the findings of a cybersecurity company.

It is common for attackers to use widely-covered news events to get people to click on malicious emails and links, and cybersecurity firm INKY said it recently received multiple helpdesk emails about curious emails their customers were receiving.

INKY customers reported receiving emails that discuss the ransomware attack on Colonial Pipeline and ask them to download "ransomware system updates" in order to protect their organization from a similar fate.

https://www.zdnet.com/article/hackers-use-colonial-pipeline-ransomware-news-for-phishing-attack/

Click above link to read more.

Back to top

Data breaches drive higher loan interest rates

Companies that experience a data breach may not suffer a long-term drop in stock price, but will often have to pay higher loan interest rates and grant other concessions, according to a study published this week.

The academic study, conducted by researchers at Yeshiva University in New York City and Hong Kong Polytechnic University, found the average company paid almost $3.7 million more in interest every year. Businesses with a strong reputation for IT security, which often have more favorable loan terms compared to their peers, suffered more following a breach.

https://therecord.media/ransomware-attack-disrupts-massachusetts-ferries/

Click above link to read more.

Back to top

Cybercriminals hold $115,000-prize contest to find new cryptocurrency hacks

A top Russian-language underground forum has been running a "contest" for the past month, calling on its community to submit "unorthodox" ways to conduct cryptocurrency attacks.

The forum's administrator, in an announcement made on April 20, 2021, invited members to submit papers that assess the possibility of targeting cryptocurrency-related technology, including the theft of private keys and wallets, in addition to covering unusual cryptocurrency mining software, smart contracts, and non-fungible tokens (NFTs).

https://thehackernews.com/2021/06/cybercriminals-hold-115000-prize.html

Click above link to read more.

Back to top

Privacy fears over NHS plans to share GP medical records with third parties

Privacy fears have been raised over controversial plans to share NHS medical records from every GP patient in England with third parties.

According to NHS Digital, the medical histories of more than 55 million patients will be made available on a database to "support the planning and commissioning of health and care services, the development of health and care policy, public health monitoring and interventions (including COVID-19) and enable many different areas of research."

https://www.healthcareitnews.com/news/emea/privacy-fears-over-nhs-plans-share-gp-medical-records-third-parties

Click above link to read more.

Back to top

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca