August 29, 2023

Challenge yourself with our Cryptocons Quiz!

Cybersecurity Issue of the Week: **CRYPTOCONS**
✪ Read our Cryptocons Infosheet to learn more.

This past week's stories:

- **Canadian Cyber Threat Exchange and Rogers Cybersecure Catalyst announce new $10 million program to fuel cybersecurity excellence and innovation in Ontario**
- **Moscow helping cybercriminals operate with 'near impunity': Canadian Cyber Centre**
- **Protecting Canada's energy infrastructure and supply chain from cyber attacks**
- **77% of Canadian energy companies lack cybersecurity protection, study finds**
- **Cybersecurity companies report surge in ransomware attacks**
- ✪ **Crypto scams push deeper into the American heartland**
- **Unrealistic expectations exacerbate the cybersecurity talent shortage**
- **Raccoon malware resurfaces in dark web with new stealing capabilities**
- **Flax Typhoon group abusing built-in operating system tools to deploy malware**
- **Juice jacking: Is it a real issue or media hype?**
- **Urgent FBI warning: Barracuda email gateways vulnerable despite recent patches**
- **Virtual patching: what is it? Your defense against exploits and threats**

Canadian Cyber Threat Exchange and Rogers Cybersecure Catalyst announce new $10 million program to fuel cybersecurity excellence and innovation in Ontario

Canadian Cyber Threat Exchange ("CCTX") and Rogers Cybersecure Catalyst at Toronto Metropolitan University ("the Catalyst") are proud to announce the Ontario Cybersecurity Excellence Initiative (OCEI) – a first-of-its-kind effort to drive Ontario's cyber competitiveness and resilience in six key sectors: advanced manufacturing, automotive, life sciences, mining, law enforcement and smart infrastructure.

https://www.newswire.ca/news-releases/canadian-cyber-threat-exchange-and-rogers-cybersecure-catalyst-announce-new-10-million-program-to-fuel-cybersecurity-excellence-and-innovation-in-ontario-899205965.html

Click above link to read more.

Back to top

Moscow helping cybercriminals operate with 'near impunity': Canadian Cyber Centre

A new federal report predicts Russian intelligence services and police will help cybercriminals operate with "near impunity" against their targets -- including Canadians -- in coming months.

https://www.ctvnews.ca/politics/moscow-helping-cybercriminals-operate-with-near-impunity-canadian-cyber-centre-1.6537728

Click above link to read more.

Back to top

Protecting Canada’s energy infrastructure and supply chain from cyber attacks

An engineering professor from the University of Waterloo was awarded $1.2 million in federal funding to protect Canada’s critical energy infrastructure and energy sector supply chains from cyber threats.

https://uwaterloo.ca/news/protecting-canadas-energy-infrastructure-and-supply-chain

Click above link to read more.

Back to top

77% of Canadian energy companies lack cybersecurity protection, study finds

More than three-quarters of Canadian energy companies fail to have basic cybersecurity measures in place, a security lag that puts the country's energy infrastructure at risk, a new study has found.

https://www.nsnews.com/highlights/77-of-canadian-energy-companies-lack-cybersecurity-protection-study-finds-7448187

Click above link to read more.

Back to top

Cybersecurity companies report surge in ransomware attacks

Ransomware attacks continue to be highly profitable for cybercrime groups and the recent reports released by various cybersecurity firms show that they are increasing both in terms of volume and sophistication.

https://www.securityweek.com/cybersecurity-companies-report-surge-in-ransomware-attacks/

Click above link to read more.

Back to top

Crypto scams push deeper into the American heartland

American seniors are increasingly vulnerable to so-called “pig butchering” crypto scams, partly on account of chronic loneliness. So much so that The American Association of Retired Persons (AARP) has published an explicit warning telling Americans over 50 to watch out for criminals trying to trick them out of their hard-earned savings.

https://beincrypto.com/elderly-americans-risk-pig-butchering-aarp/

Click above link to read more.

Back to top

Unrealistic expectations exacerbate the cybersecurity talent shortage

Consumers believe today’s cybersecurity talent shortage is in large part due to limited exposure to the profession and a lack of cybersecurity education and training at a younger age within school systems, according to ThreatX.

https://www.helpnetsecurity.com/2023/08/25/cybersecurity-talent-shortage-expectations/

Click above link to read more.

Back to top

Raccoon malware resurfaces in dark web with new stealing capabilities

It has recently come to light that the individuals responsible for the development and distribution of the infamous Raccoon Stealer malware have returned to online hacker forums.

https://cybersecuritynews.com/raccoon-malware-resurface/

Click above link to read more.

Back to top

Flax Typhoon group abusing built-in operating system tools to deploy malware

With the rapid evolution of technology, the threat actors, along with their attacks, are also getting more sophisticated and evolving at an increasing pace, posing a growing threat to vital infrastructure and sensitive data.

https://cybersecuritynews.com/flax-typhoon-abusing-operating-system/

Click above link to read more.

Back to top

Juice jacking: Is it a real issue or media hype?

You get off a flight and realize your phone is almost out of battery, which will make getting an Uber at your destination a bit challenging. Then you see it — a public charging station at the next gate like a pot of gold at the end of the rainbow. As you run rom-com style to the USB port, you may briefly wonder if it's actually safe from a cybersecurity perspective to plug in your phone.

https://securityintelligence.com/articles/juice-jacking-is-it-real-or-media-hype/

Click above link to read more.

Back to top

Urgent FBI warning: Barracuda email gateways vulnerable despite recent patches

The U.S. Federal Bureau of Investigation (FBI) is warning that Barracuda Networks Email Security Gateway (ESG) appliances patched against a recently disclosed critical flaw continue to be at risk of potential compromise from suspected Chinese hacking groups.

https://thehackernews.com/2023/08/urgent-fbi-warning-barracuda-email.html

Click above link to read more.

Back to top

Virtual patching: what is it? Your defense against exploits and threats

You might discover hundreds of open doors if you scan your website for security vulnerabilities. Our AppSec research across 1400 websites protected by AppTrana uncovered 33,000 critical, medium, and high vulnerabilities in Q2, 2023.

What's more alarming is that 31% of these vulnerabilities remained open for over 180 days, with 1729 classified as critical or high.

https://cybersecuritynews.com/virtual-patching/

Click above link to read more.

Back to top