April 5, 2022

Challenge yourself with our Spring Cleaning quiz!

This past week's stories:

- 19-year-old Ontario woman charged in several 'grandparent scams'
- Five universities supporting Canada's cyber security strategy
- Ronin Network: What a $600m hack says about the state of crypto
- Russian government hackers linked to cyber attack on first day of Ukraine invasion
- Spring4Shell: Spring users face new, zero-day vulnerability
- Automaker cybersecurity lagging behind tech adoption, experts warn
- Cisco software update blocks exploit chain in network management software
- Warning over Covid text scam which could take your bank details
- Public Safety and Security Market worth $707.2 billion by 2027 - Exclusive report by MarketsandMarkets™
- War, fear, 'hacktivist' zeal are upending energy cybersecurity
- Nearly two-thirds of ransomware victims paid ransoms last year, finds "2022 Cyberthreat Defense Report"
- Nordex hit by cyber security incident, shuts IT systems

19-year-old Ontario woman charged in several 'grandparent scams'

Toronto police say they have charged a 19-year-old Ajax, Ont., woman in three "grandparent" scams over a two-day period.

Investigators said that on March 24, a 78-year-old woman was contacted by a person claiming to be her grandson who said he had been arrested and was calling from a police station.

https://globalnews.ca/news/8724451/toronto-grandparent-scam-ajax-woman-charged/

Click above link to read more.

Back to top

Five universities supporting Canada's cyber security strategy

The federal government is moving to strengthen Canada's national cybersecurity ecosystem with the help of five universities, amid rising digital crimes perpetrated by hackers, companies and governments.

The Cyber Security Innovation Network (CSIN) aims to enhance research and development, increase the commercialization of IT security, and expand the country's talent pool. The network was unveiled last month by the Ministry of Innovation, Science and Economic Development Canada (ISED) as part of the government's roughly $500 million National Cyber Security Strategy. This pan-Canadian initiative is being led by the National Cybersecurity Consortium (NCC), a federally incorporated non-profit consisting of Concordia University, Ryerson University, the University of Calgary, the University of New Brunswick and the University of Waterloo.

www.universityaffairs.ca/news/news-article/five-universities-supporting-canadas-cybersecurity-strategy/

Click above link to read more.

Back to top

Ronin Network: What a $600m hack says about the state of crypto

Ronin Network, a key platform powering the popular mobile game Axie Infinity, has had $615m (£467m) stolen.

A 20-year-old from Wiltshire, Dan Rean, is one of those affected. He told the BBC: "I have lost 0.15 Ethereum, about $500. It's bad but I have friends in a worse position."

https://www.bbc.com/news/technology-60933174

Click above link to read more.

Back to top

Russian government hackers linked to cyber attack on first day of Ukraine invasion

Russian government hackers have been linked to an attack on a satellite communications company at the start of the invasion of Ukraine.

Businesses and individuals using routers made by Viasat, an American business that provides broadband-speed satellite internet connections, were knocked offline on 24 February.

https://news.sky.com/story/russian-government-hackers-linked-to-cyber-attack-on-first-day-of-ukraine-invasion-12579396

Click above link to read more.

Back to top

Spring4Shell: Spring users face new, zero-day vulnerability

Spring users are facing a new, zero-day vulnerability which was discovered in the same week as an earlier critical bug.

The first security issue, CVE-2022-22963, is a SpEL expression injection bug in Spring Cloud Function, disclosed on March 28 by NSFOCUS, as previously reported by The Daily Swig.

A second RCE bug, dubbed “Spring4Shell/Springshell”, has now also been discovered in Spring Framework’s Java-based Core module.

https://portswigger.net/daily-swig/spring4shell-spring-users-face-new-zero-day-vulnerability

Click above link to read more.

Back to top

Automaker cybersecurity lagging behind tech adoption, experts warn

A bug in Honda is indicative of the sprawling car-attack surface that could give cyberattackers easy access to victims, as global use of ‘smart car tech’ and EVs surges.

A pair of recent vulnerabilities found in the automaker ecosystem might not seem like a real danger taken separately. But experts warn a lack of attention on cybersecurity could plague “smart” car and electric vehicle systems — and users — in years to come, as the use of automotive technology continues to explode.

https://threatpost.com/automaker-cybersecurity-lagging-tech-adoption/179204/

Click above link to read more.

Back to top

Cisco software update blocks exploit chain in network management software

The researcher, Pedro Ribeiro, was able to put together a damaging exploit against the enterprise-grade network and storage management technology by chaining together a combination of vulnerabilities in the system.

The exploit chain allowed Ribeiro to escalate a web-based flaw to achieve a root shell, or complete compromise.

https://portswigger.net/daily-swig/cisco-software-update-blocks-exploit-chain-in-network-management-software

Click above link to read more.

Back to top

Warning over Covid text scam which could take your bank details

Warnings have been issued about a Covid text scam that could take your bank details. The scam is a text which says you're been in close contact with a Covid case and redirects you to a website to order a PCR test where you input your bank details.

Since April 1, Covid tests are no longer available for free in England (with some exceptions for vulnerable people), which has led to some people being caught out by the scam.

https://www.mylondon.news/news/uk-world-news/warning-over-covid-text-scam-23587254

Click above link to read more.

Back to top

Public Safety and Security Market worth $707.2 billion by 2027 - Exclusive report by MarketsandMarkets™

According to a new market research report "Public Safety and Security Market by Component, Solution (Critical Communication Network, Biometric & Authentication System, Surveillance System, Emergency & Disaster Management, Cyber Security), Service, Vertical and Region - Global Forecast to 2027", published by MarketsandMarkets™, the global Public Safety and Security Market size is expected to grow from USD 433.6 billion in 2022 to USD 707.2 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 10.3% from 2022 to 2027.

https://www.prnewswire.com/news-releases/public-safety-and-security-market-worth-707-2-billion-by-2027--exclusive-report-by-marketsandmarkets-301516532.html

Click above link to read more.

Back to top

War, fear, ‘hacktivist’ zeal are upending energy cybersecurity

After news broke that hackers had forced the biggest U.S. petroleum pipeline to stop shipping fuel to the East Coast, drivers started hoarding gasoline.

Fear took root within a few days of Colonial Pipeline Co.’s announcement last spring. Images of panic-buying went viral on social media. And in response, the U.S. Consumer Product Safety Commission took to Twitter.

https://www.eenews.net/articles/war-fear-hacktivist-zeal-are-upending-energy-cybersecurity/

Click above link to read more.

Back to top

Nearly two-thirds of ransomware victims paid ransoms last year, finds “2022 Cyberthreat Defense Report”

CyberEdge Group, a leading research and marketing firm serving the cybersecurity industry’s top vendors, today announced the launch of its ninth annual Cyberthreat Defense Report (CDR). The award-winning CDR is the standard for assessing organizations’ security posture, gauging

perceptions of information technology (IT) security professionals, and ascertaining current and planned investments in IT security infrastructure – across all industries and geographic regions.

https://www.businesswire.com/news/home/20220404005094/en/Nearly-Two-thirds-of-Ransomware-Victims-Paid-Ransoms-Last-Year-Finds-%E2%80%9C2022-Cyberthreat-Defense-Report%E2%80%9D

Click above link to read more.

Back to top

Nordex hit by cyber security incident, shuts IT systems

Germany's Nordex Group, which along with its subsidiaries, develops, manufactures and distributes wind power systems, has been hit by a cyber security incident since Thursday and has shut down its IT systems across multiple locations and business units to contain the issue, the company said on Saturday.

It said the intrusion had been noticed at an early stage, and that customers, employees and other stakeholders might be affected by the shutdown of IT systems.

https://www.reuters.com/technology/nordex-hit-by-cyber-security-incident-shuts-it-systems-2022-04-02/

Click above link to read more.

Back to top


Security News Digest
Information Security Branch
BRITISH COLUMBIA
OCIO
Office of the Chief Information Officer