January 10, 2023

Challenge yourself with our Cyber Security Resolutions Quiz!

This past week's stories:

- **Toronto hospital network issues 'code grey' as digital systems go down**
- **SickKids attack – and apology – pulls ransomware's 'Robin Hood' into spotlight**
- **Five Guys data breach puts HR data under a heat lamp**
- **Email addresses linked to 235M Twitter accounts leaked in hack**
- **Ongoing Flipper Zero phishing attacks target infosec community**
- **The cybersecurity talent shortage: The outlook for 2023**
- **Schools hit by cyber attack and documents leaked**
- **Exclusive: Russian hackers targeted U.S. nuclear scientists**
- **Critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche expose owners' personal information**
- **The dark web's criminal minds see Internet of Things as next big hacking prize**
- **Hackers using CAPTCHA bypass tactics in freejacking campaign on GitHub**
- **Russian Turla hackers hijack decade-old malware infrastructure to deploy new backdoors**
- **Iowa's largest city cancels classes due to cyber attack**

Toronto hospital network issues 'code grey' as digital systems go down

A major Toronto hospital network said its digital systems went down on Monday and it was working to investigate what was causing the outage.

The University Health Network issued a "code grey" — a hospital code for system failure — but released few other details about what happened.

https://www.cbc.ca/news/canada/toronto/ont-uhn-1.6708319

Click above link to read more.

Back to top

SickKids attack – and apology – pulls ransomware's 'Robin Hood' into spotlight

The CEO was losing their patience.

Their company had been hacked, their data stolen, and they were now deep into a heated negotiation with a representative of the organization that was holding their files for ransom.

https://www.thestar.com/news/canada/2023/01/05/sickkids-attack-and-apology-pulls-ransomwares-robin-hood-into-spotlight.html?rf

Click above link to read more.

Back to top

Five Guys data breach puts HR data under a heat lamp

The Five Guys burger empire has been hit with what appears to be a "smash-and-grab" operation: Cyberattackers busted into a file server and made off with the personally identifiable information (PII) of people who applied to work at the chain.

Details are scant, but in a form letter to the impacted sent out on Dec. 29, Five Guys chief operating officer Sam Chamberlain noted that an "unauthorized access to files" was discovered on Sept. 17 and was blocked the same day.

https://www.darkreading.com/attacks-breaches/five-guys-data-breach-hr-data

Click above link to read more.

Back to top

Email addresses linked to 235M Twitter accounts leaked in hack

More than 200 million Twitter accounts, including email addresses, were leaked this week, raising privacy and security concerns.

Alan Gal, the co-founder of Israeli security firm Hudson Rock, reportedly first uncovered the leak and took to social media to alert the public.

https://thehill.com/policy/cybersecurity/3800607-email-addresses-linked-to-235m-twitter-accounts-leaked-in-hack/

Click above link to read more.

Back to top

Ongoing Flipper Zero phishing attacks target infosec community

A new phishing campaign is exploiting the increasing interest of security community members towards Flipper Zero to steal their personal information and cryptocurrency.

Flipper Zero is a portable multi-functional cybersecurity tool for pen-testers and hacking enthusiasts. The tool allows researchers to tinker with a wide range of hardware by supporting RFID emulation, digital access key cloning, radio communications, NFC, infrared, Bluetooth, and more.

https://www.bleepingcomputer.com/news/security/ongoing-flipper-zero-phishing-attacks-target-infosec-community/

Click above link to read more.

Back to top

The cybersecurity talent shortage: The outlook for 2023

The global cybersecurity workforce grew to encompass 4.7 million people, reaching its highest-ever levels, according to (ISC)2 2022 workforce study. That's the encouraging news.

However, the same study found that there is still a need for more than 3.4 million security professionals, an increase of over 26% from 2021's numbers. This reverses a trend seen in (ISC)2's 2021 study, where the number of open cybersecurity jobs actually dropped over a two-year period.

https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/

Click above link to read more.

Back to top

Schools hit by cyber attack and documents leaked

Highly confidential documents from 14 schools have been leaked online by hackers, the BBC can reveal.

One of those was Pates Grammar School in Gloucestershire, targeted by a hacking group called Vice Society.

https://www.bbc.com/news/uk-england-gloucestershire-63637883

Click above link to read more.

Back to top

Exclusive: Russian hackers targeted U.S. nuclear scientists

Russian hacking team known as Cold River targeted three nuclear research laboratories in the United States this past summer, according to internet records reviewed by Reuters and five cyber security experts.

Between August and September, as President Vladimir Putin indicated Russia would be willing to use nuclear weapons to defend its territory, Cold River targeted the Brookhaven (BNL), Argonne (ANL) and Lawrence Livermore National Laboratories (LLNL), according to internet records that showed the hackers creating fake login pages for each institution and emailing nuclear scientists in a bid to make them reveal their passwords.

https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06/

Click above link to read more.

Back to top

Critical vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche expose owners' personal information

Hackers could have performed malicious activities through API security vulnerabilities in nearly twenty car manufacturers and services. As a result of these vulnerabilities, hackers could be able to perform the following activities:

- Unlocking cars,
- Starting cars,
- Tracking cars, and
- Exposing customers' personal information.

https://cybersecuritynews.com/api-vulnerabilities-auto-industry/

Click above link to read more.

Back to top

The dark web's criminal minds see Internet of Things as next big hacking prize

John Hultquist, vice president of intelligence analysis at Google-owned cybersecurity firm Mandiant, likens his job to studying criminal minds through a soda straw. He monitors cyberthreat groups in real time on the dark web, watching what amounts to a free market of criminal innovation ebb and flow.

Groups buy and sell services, and one hot idea — a business model for a crime — can take off quickly when people realize that it works to do damage or to get people to pay. Last year, it was ransomware, as criminal hacking groups figured out how to shut down servers through what's called directed denial of service attacks. But 2022, say experts, may have marked an inflection point due to the rapid proliferation of IoT (Internet of Things) devices.

https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html

Click above link to read more.

Back to top

Hackers using CAPTCHA bypass tactics in freejacking campaign on GitHub

A South Africa-based threat actor known as Automated Libra has been observed employing CAPTCHA bypass techniques to create GitHub accounts in a programmatic fashion as part of a freejacking campaign dubbed PURPLEURCHIN.

The group "primarily targets cloud platforms offering limited-time trials of cloud resources in order to perform their crypto mining operations," Palo Alto Networks Unit 42 researchers William Gamazo and Nathaniel Quist said.

https://thehackernews.com/2023/01/hackers-using-captcha-bypass-tactics-in.html

Click above link to read more.

Back to top

Russian Turla hackers hijack decade-old malware infrastructure to deploy new backdoors

The Russian cyberespionage group known as Turla has been observed piggybacking on attack infrastructure used by a decade-old malware to deliver its own reconnaissance and backdoor tools to targets in Ukraine.

Google-owned Mandiant, which is tracking the operation under the uncategorized cluster moniker UNC4210, said the hijacked servers correspond to a variant of a commodity malware called ANDROMEDA (aka Gamarue) that was uploaded to VirusTotal in 2013.

https://thehackernews.com/2023/01/russian-turla-hackers-hijack-decade-old.html

Click above link to read more.

Back to top

Iowa's largest city cancels classes due to cyber attack

Iowa's largest school district cancelled classes for Tuesday after determining there was a cyber attack on its technology network.

Des Moines Public Schools announced Monday that classes would be cancelled for its 33,000 students after being "alerted to a cyber security incident on its technology network."

https://www.thestar.com/news/world/us/2023/01/09/iowas-largest-city-cancels-classes-due-to-cyber-attack.html?rf

Click above link to read more.

Back to top

OCIOSecurity@gov.bc.ca