April 23, 2024

Challenge yourself with our Internet of Things (IoT) Quiz!

Cybersecurity theme of the week: **Malware**

✪ Check out our **Malvertising Quiz** to learn more.

Wonder what you can do to protect yourself from malware?

All Users	Technical Users	Business Owners
Make sure your software is up to date on all your devices. For corporate updates, accept the prompts to update your software when they come up, don't delay or postpone. For personal updates, wherever possible choose the automatic update feature. If that is not available, check for updates on a regular basis and review your installed software and apps to see if any are no longer in use.	Take a layered approach to defending against malware. Understand "normal" patterns in your environment, review logs and accounts for any that falls outside of the normal.	Integrate security risks with operational and organizational risks to balance business decisions. Ask your security and other technical leaders their opinions.

This past week's stories:

It's a field that needs more workers — and these Fredericton whiz kids have a head start

Russian APT deploys new 'Kapeka' backdoor in eastern European attacks

Identity in the shadows: Shedding light on cybersecurity's unseen threats

Data center ransomware attacks on rise: Microsoft SQL server is prime target

✪ **R00TK1T claims that they have acquired confidential data from Nestle**

Authorities busted cybercrime platform that steal passwords & card details

✪ **New Android trojan 'SoumniBot' evades detection with clever tricks**

It's a field that needs more workers — and these Fredericton whiz kids have a head start

A cyber attack on the City of Saint John in November 2020 may have been just a headline for many, but for a group of students at Nashwaaksis Middle School, defending such an attack is the stuff career ambitions are made of.

https://www.cbc.ca/news/canada/new-brunswick/cybersecurity-nashwaaksis-middle-school-1.7177678

Click above link to read more.

Back to top

Russian APT deploys new 'Kapeka' backdoor in eastern European attacks

A previously undocumented "flexible" backdoor called Kapeka has been "sporadically" observed in cyber attacks targeting Eastern Europe, including Estonia and Ukraine, since at least mid-2022.

https://thehackernews.com/2024/04/russian-apt-deploys-new-kapeka-backdoor.html

Click above link to read more.

Back to top

Identity in the shadows: Shedding light on cybersecurity's unseen threats

In today's rapidly evolving digital landscape, organizations face an increasingly complex array of cybersecurity threats. The proliferation of cloud services and remote work arrangements has heightened the vulnerability of digital identities to exploitation, making it imperative for businesses to fortify their identity security measures.

https://thehackernews.com/2024/04/identity-in-shadows-shedding-light-on.html

Click above link to read more.

Back to top

Data center ransomware attacks on rise: Microsoft SQL server is prime target

Ransomware threats are increasingly targeting data center servers and workloads as the initial step in the attack chain.

https://cybersecuritynews.com/data-center-ransomware-attacks/

Click above link to read more.

Back to top

R00TK1T claims that they have acquired confidential data from Nestle

The hacker group known as R00TK1T has announced that it has successfully entered the systems of Nestle, the world's largest food and beverage company, and acquired confidential data.

https://cybersecuritynews.com/r00tk1t-claims/

Click above link to read more.

Back to top

Authorities busted cybercrime platform that steal passwords & card details

International law enforcement agencies have successfully dismantled a notorious cybercrime platform, LabHost, which facilitated criminals in conducting phishing attacks to steal sensitive information such as passwords, addresses, and card details from unsuspecting victims worldwide.

https://cybersecuritynews.com/authorities-busted-cybercrime-platform/

Click above link to read more.

Back to top

New Android trojan 'SoumniBot' evades detection with clever tricks

A new Android trojan called SoumniBot has been detected in the wild targeting users in South Korea by leveraging weaknesses in the manifest extraction and parsing procedure.

https://thehackernews.com/2024/04/new-android-trojan-soumnibot-evades.html

Click above link to read more.

Back to top

One tech tip: What to do if your personal info has been exposed in a data breach

Data breaches like the recent one involving millions of AT&T customers are becoming an almost regular occurrence.

https://abcnews.go.com/Business/wireStory/tech-tip-personal-info-exposed-data-breach-109371703

Click above link to read more.

Back to top

Russian hacker group ToddyCat uses advanced tools for industrial-scale data theft

The threat actor known as ToddyCat has been observed using a wide range of tools to retain access to compromised environments and steal valuable data.

https://thehackernews.com/2024/04/russian-hacker-group-toddycat-uses.html

Click above link to read more.

Back to top

GPT-4 is capable of exploiting 87% of one-day vulnerabilities

Large language models (LLMs) have achieved superhuman performance on many benchmarks, leading to a surge of interest in LLM agents capable of taking action, self-reflecting, and reading documents.

https://cybersecuritynews.com/gpt-4-exploits-one-day-vulnerabilities/#google_vignette

Click above link to read more.

Back to top

Hackers mimic road toll collection services to steal your money

The FBI's Internet Crime Complaint Center (IC3) has warned about a sophisticated smishing scam targeting drivers across multiple states.

https://cybersecuritynews.com/hackers-mimic-road-toll-collection/

Click above link to read more.

Back to top

Ransomware double-dip: Re-victimization in cyber extortion

In our dataset of over 11,000 victim organizations that have experienced a Cyber Extortion / Ransomware attack, we noticed that some victims re-occur. Consequently, the question arises why we observe a re-victimization and whether or not this is an actual second attack, an affiliate crossover (meaning an affiliate has gone to another Cyber Extortion operation with the same victim) or stolen data that has been travelling and re-(mis-)used. Either way, for the victims neither is good news.

https://thehackernews.com/2024/04/ransomware-double-dip-re-victimization.html

Click above link to read more.

Back to top

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.