April 9, 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
It's never a bad idea to be cautious online. If you find an ad that appeals to you on a third-party website, do a web search and go directly to the seller's site, instead of clicking the ad on the webpage.	To recover from data corruption from malware, keep offline backups and ensure you are following your company's guidance on how regularly you create those backups. Be sure to test recovery from backup.	Ensure your organization implements enterprise level anti-virus software onto your organization's devices. Ask teams about your incident recovery plans and hold tabletop exercises to validate them.

This past week's stories:

Trudeau announces $2.4 billion for AI-related investments
University of Winnipeg says cyberattack stole employee, student financial info
New phishing campaign targets oil & gas with evolved data-stealing malware
Researchers unveil the attackers behind the Agent Tesla campaign
✪ **Hackers hijacking YouTube channels to steal your data**
Alarming gaps in mobile cybersecurity in 2024: Expert analysis
Ukrainian cybersecurity official reveals structure of Russian hacker groups
EU drops sovereignty requirements in cybersecurity certification scheme, document shows
Indian government's cloud spilled citizens' personal data online for years
Ivanti CEO vows cybersecurity makeover after zero-day blitz
Why a near-miss cyberattack put US officials and the tech industry on edge
Software-defined vehicle fleets face a twisty road on cybersecurity

Trudeau announces $2.4 billion for AI-related investments

The Liberal government is setting aside $2.4 billion in its upcoming budget to build capacity in artificial intelligence, Prime Minister Justin Trudeau announced Sunday.

https://www.cbc.ca/news/politics/federal-government-ai-investment-1.7166234

Click above link to read more.

Back to top

University of Winnipeg says cyberattack stole employee, student financial info

The University of Winnipeg said Thursday the individuals behind a cyberattack discovered last week likely “stole information” from current and former students and employees dating back more than 20 years.

https://globalnews.ca/news/10403728/university-winnipeg-cyberattack-stole-information-employees-students/

Click above link to read more.

Back to top

New phishing campaign targets oil & gas with evolved data-stealing malware

An updated version of an information-stealing malware called Rhadamanthys is being used in phishing campaigns targeting the oil and gas sector.

https://thehackernews.com/2024/04/new-phishing-campaign-targets-oil-gas.html

Click above link to read more.

Back to top

Researchers unveil the attackers behind the Agent Tesla campaign

Check Point Research has exposed a recent wave of cyberattacks utilizing the infamous Agent Tesla malware. This campaign targeted organizations in the United States and Australia.

https://cybersecuritynews.com/agent-tesla-attackers-revealed/

Click above link to read more.

Back to top

Hackers hijacking YouTube channels to steal your data

Cybercriminals are increasingly exploiting YouTube, a platform beloved by millions, to produce sophisticated malware attacks.

https://cybersecuritynews.com/hackers-hijacking-youtube/

Click above link to read more.

Back to top

Alarming gaps in mobile cybersecurity in 2024: Expert analysis

As social engineering tactics become the most popular attack vectors, consumers' security awareness is seen as the ultimate line of defense. Users who build a strong security culture fortify their defenses against cyberattacks, better adapt to innovation, and understand digital challenges and issues while avoiding risks and building confidence.

https://www.techopedia.com/news/alarming-gaps-in-mobile-cybersecurity-expert-analysis

Click above link to read more.

Back to top

Ukrainian cybersecurity official reveals structure of Russian hacker groups

Russian hacker groups are military units with code names that are part of the Main Intelligence Directorate of the General Staff and the Federal Security Service of the Russian Federation.

https://www.ukrinform.net/rubric-ato/3848343-ukrainian-cybersecurity-official-reveals-structure-of-russian-hacker-groups.html

Click above link to read more.

Back to top

EU drops sovereignty requirements in cybersecurity certification scheme, document shows

Amazon (AMZN.O), opens new tab, Alphabet's (GOOGL.O), opens new tab Google and Microsoft (MSFT.O), opens new tab may find it easier to bid for EU cloud computing contracts after draft cybersecurity labelling rules scrapped a requirement that vendors should be independent from non-EU laws, according to the document seen by Reuters.

https://www.reuters.com/technology/eu-drops-sovereignty-requirements-cybersecurity-certification-scheme-document-2024-04-03/

Click above link to read more.

Back to top

Indian government's cloud spilled citizens' personal data online for years

The Indian government has finally resolved a years-long cybersecurity issue that exposed reams of sensitive data about its citizens. A security researcher exclusively told TechCrunch he found at least hundreds of documents containing citizens' personal information — including Aadhaar numbers, COVID-19 vaccination data, and passport details — spilling online for anyone to access.

https://techcrunch.com/2024/04/02/indian-government-cloud-spilled-citizens-personal-data-online-for-years/

Click above link to read more.

Back to top

Ivanti CEO vows cybersecurity makeover after zero-day blitz

Reeling from a spate of zero-day attacks that threw its security response teams into disarray and forced the US government to issue disconnection instructions, Ivanti says it has found security enlightenment with a CEO-led media campaign vowing to fix the entire cybersecurity organization.

https://www.securityweek.com/ivanti-ceo-vows-cybersecurity-makeover-after-zero-day-blitz/

Click above link to read more.

Back to top

Why a near-miss cyberattack put US officials and the tech industry on edge

German software developer Andres Freund was running some detailed performance tests last month when he noticed odd behavior in a little known program. What he found when he investigated has sent shudders across the software world and drawn attention from tech executives and government officials.

https://www.reuters.com/technology/cybersecurity/why-near-miss-cyberattack-put-us-officials-tech-industry-edge-2024-04-05/

Click above link to read more.

Back to top

Software-defined vehicle fleets face a twisty road on cybersecurity

When Israel-based REE Automotive designed its P7 electric vehicle chassis, it worked from the software out: The flat vehicle chassis is totally configurable with four independent modules near each tire for steering, braking, suspension, and power train, each driven by an electronic control unit (ECU) customizable through software.

https://www.darkreading.com/ics-ot-security/software-defined-vehicle-fleets-twisty-road-cybersecurity

Click above link to read more.

Back to top


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