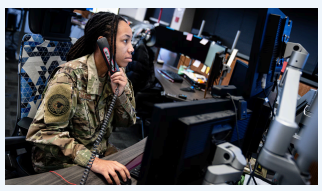
Week of March, 17, 2025

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources



U.S. Cyber Command Wraps Up Largest-Ever Cyber Guard Exercise

www.cybercom.mil

U.S. Cyber Command personnel conduct cyber operations during the Cyber Guard 25-1 exercise, held from March 12-18, 2025. The exercise is part of a larger joint force series designed to simulate real-world scenarios and enable participants to practice...

Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks

Cybersecurity officials warn against potentially costly Medusa ransomware attacks | AP News - Associated Press News

apnews.com

LOS ANGELES (AP) — The FBI and the U.S. Cybersecurity and Infrastructure Security Agency are warning against a dangerous ransomware scheme. In an advisory posted earlier this week, government officials warned that a ransomware-as-a-service software c...

UAT-5918 Targets Taiwan's Critical Infrastructure Using Web Shells and Open-Source Tools - The Hacker News

thehackernews.com

Threat hunters have uncovered a new threat actor named UAT-5918 that has been attacking critical infrastructure entities in Taiwan since at least 2023. "UAT-5918, a threat actor believed to be motivated by establishing long-term access for informatio...

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech

Zero-Trust Architecture in Government: Spring 2025 Roundup

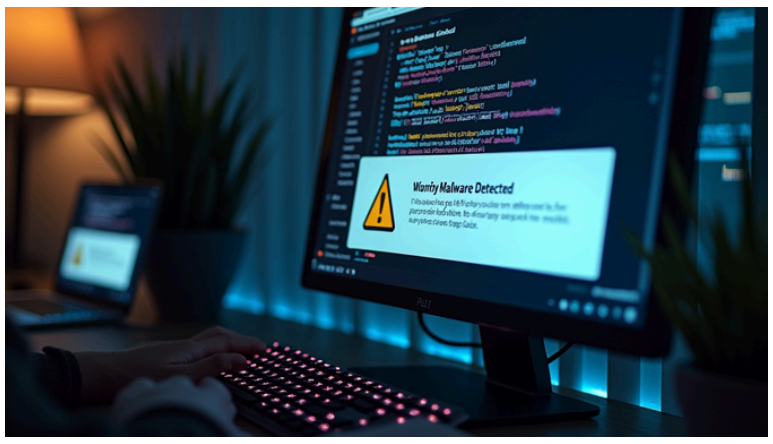
www.govtech.com

Next, we have a March 2025 article explaining why zero-trust architecture is the next big thing in security. Here's how that ends: "Heading into 2025, the conversation is no longer about ...

Cybersecurity experts say it's necessary to maintain U.S. cyberoperations against Russia

www.wbur.org

To bring Russia to the negotiating table to discuss the war in Ukraine, and as Trump warms up to Putin, it's been reported that the Trump administration ordered U.S. Cyber Command to stop ...



Hackers Exploit Severe PHP Flaw to Deploy Quasar RAT and XMRig Miners

thehackernews.com

Threat actors are exploiting a severe security flaw in PHP to deliver cryptocurrency miners and remote access trojans (RATs) like Quasar RAT. The vulnerability, assigned the CVE identifier CVE-2024-4577, refers to an argument injection vulnerability ...

School's out for cyber - POLITICO

www.politico.com

Today's Agenda. After a busy week on Capitol Hill, capped by the Senate voting to pass the CR and avert a government shutdown, Congress is out this week.. At the Agencies. ADDED RISKS — As ...

Microsoft identifies new RAT targeting cryptocurrency wallets and more

therecord.media

A previously unreported remote access trojan that Microsoft researchers dubbed StilachiRAT is designed to steal a wide range of data, including information about cryptocurrency wallet extensions for Google's Chrome browser.

DOGE to Fired CISA Staff: Email Us Your Personal Data

krebsonsecurity.com

A message posted on Monday to the homepage of the U.S. Cybersecurity & Infrastructure Security Agency (CISA) is the latest exhibit in the Trump administration's continued disregard for basic cybersecurity protections. The message instructed recently-fired CISA employees to get in touch so they can be rehired and then immediately placed on leave, asking employees to send their Social Security numbe