



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...

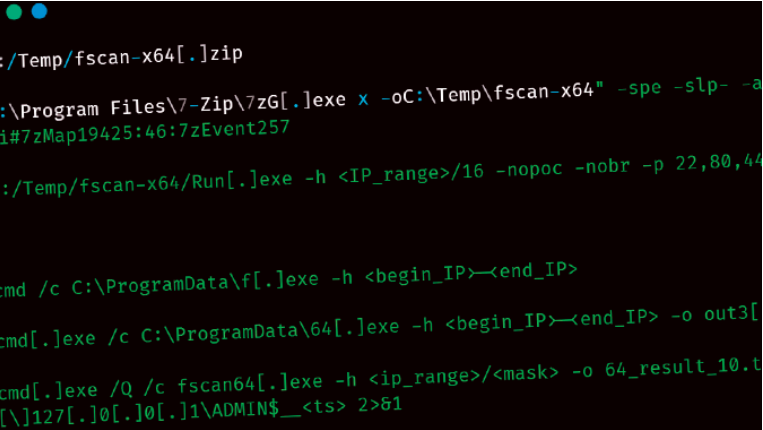
Cybercrimes, Scams & Incidents

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



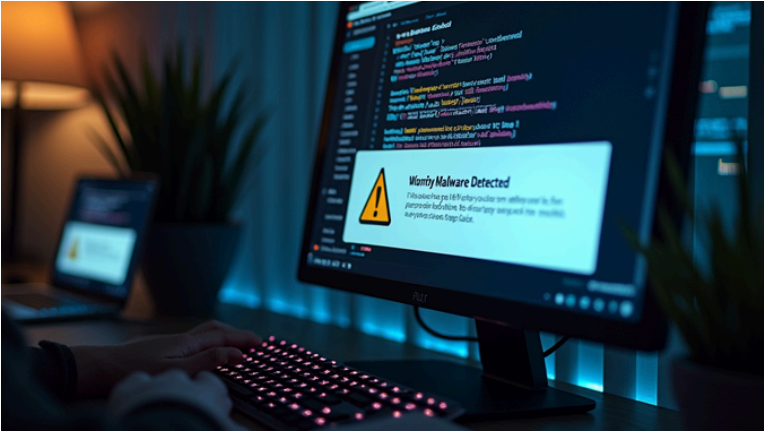
Zero-Trust Architecture in Government: Spring 2025 Roundup
www.govtech.com

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 ...



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.



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 ...



Probationary Reinstatements

CISA issued a Temporary Restraining Order in *Maryland, et al. v. United States Dep't of Agriculture, et al.*, No. 25-cv-00748, Docket No. 43 (D. Md.) (March 13, 2025). CISA's very effort to individually contact all impacted individuals. However, to the extent that you have been terminated by CISA since January 20, 2025, were in a probationary period at the time of your termination, you have not already been contacted by CISA in relation to this matter, and believe that you fall within the Court's order please reach out to hr@cisa.dhs.gov. Please provide a password protected attachment that provides your full name, your dates of employment (including date of termination), and on the date of your termination, such as date of birth or social security number. Please, to the extent that it is available, attach any termination notice. To the extent that you are identified as a probationary employee whose termination falls within the Court's order, your employment will be reinstated effective March 17, 2025. Upon your reinstatement, you will be placed on administrative leave, which is a paid non-duty status. Administrative leave is a management authorized leave category and does not count against your annual or sick leave. Upon reinstatement, your pay and benefits will restart, and all requirements of federal employment will be applicable including your ethical obligations. If you do not wish to be reinstated, please provide a written statement declining to be reinstated as quickly as possible. Nothing in this process implicates your ability to voluntarily resign.

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 number.

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

Official Quick Links

- [CISA](#)
- [CIS/MS-ISAC](#)
- [CyberCom](#)
- [DHS](#)
- [DOJ](#)
- [FBI](#)
- [NIST](#)
- [NSA](#)

External Quick links

- [AIScoop](#)
- [BleepingComputer](#)
- [Cisco Talos Intelligence Group](#)
- [CSO Online](#)
- [CyberScoop](#)
- [Cybersecurity Dive](#)
- [Cyware](#)
- [CyberWire](#)
- [Government Executive](#)
- [ISACA](#)
- [ISSA International](#)
- [FedScoop](#)
- [MITRE ATT&CK®](#)
- [Government Technology](#)
- [NASCIO](#)
- [Krebs on Security](#)
- [SC Media](#)
- [StateScoop](#)
- [The Hacker News](#)
- [The Record](#)
- [Schneier on Security](#)