Week of April 28, 2025

Cybersecurity Headlines

Cybercrimes, Scams & Incidents

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

Industry News

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

Cyber Security Company CEO Arrested for Installing Malware Onto Hospital Computers

cybersecuritynews.com

Jeffrey Bowie, CEO of cybersecurity firm Veritaco, was arrested on April 14, 2025, facing two counts of violating Oklahoma's Computer Crimes Act for allegedly installing malware on computers at St. Anthony Hospital in Oklahoma City.

DHS Secretary Noem: CISA needs to get back to 'core mission'

cyberscoop.com

SAN FRANCISCO — Homeland Security Secretary Kristi Noem outlined her plans Tuesday to refocus the Cybersecurity and Infrastructure Security Agency (CISA) on protecting critical infrastructure from increasingly sophisticated threats — particularly fro...

Malicious PyPI packages abuse Gmail, websockets to hijack systems - BleepingComputer

www.bleepingcomputer.com

Seven malicious PyPi packages were found using Gmail's SMTP servers and WebSockets for data exfiltration and remote command execution. The packages were discovered by Socket's threat research team ...

House passes legislation to criminalize nonconsensual deepfakes

cyberscoop.com

The House passed a bill Monday evening that would criminalize using a person's likeness to create nonconsensual deepfake pornography. The Take It Down Act sailed through the chamber on a vote of 402-2, marking one of the first major pieces of legisla...

Hackers abuse IPv6 networking feature to hijack software updates - BleepingComputer

www.bleepingcomputer.com

A China-aligned APT threat actor named "TheWizards" abuses an IPv6 networking feature to launch adversary-in-the-middle (AitM) attacks that hijack software updates to install Windows malware.

US wants to cut off key player in Southeast Asian cybercrime industry

therecord.media

The Treasury Department issued the proposed rulemaking Thursday, stating that Huione Group has helped launder funds from North Korean state-backed cybercrime operations and investment scams originating in Southeast Asia.

Salt Typhoon telecom hacks one of the most consequential campaigns against US ever, expert says

www.cybersecuritydive.com

A prominent former member of a recently shuttered cyber-incident review panel said the board should be reconstituted with independent authority.

China's Salt Typhoon cyber espionage campaign was one of the most damaging series of cyberattacks ever undertaken against the United States, with profound impacts on national security...

New Reports Uncover Jailbreaks, Unsafe Code, and Data Theft Risks in Leading AI Systems - The Hacker News

thehackernews.com

"Even when prompting for secure code, it really depends on the prompt's level of detail, languages, potential CWE, and specificity of instructions," Backslash Security said. "Ergo – having built-in guardrails in the form of policies and prompt rules ...

TikTok fined €530 million for sending European user data to China - BleepingComputer

www.bleepingcomputer.com

The Irish Data Protection Commission (DPC) has fined TikTok €530 million (over $601 million) for illegally transferring the personal data of users in the European Economic Area (EEA) to China ...
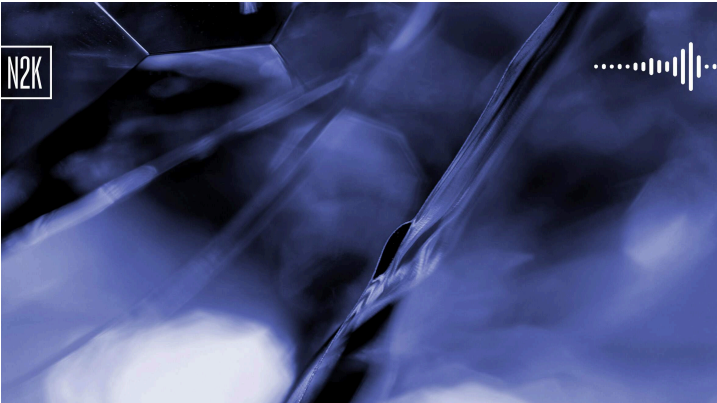
AI on the offensive.

www.thecyberwire.com

Updates from RSAC 2025. Former NSA cyber chief Rob Joyce warns that AI is rapidly approaching the ability to develop high-level software exploits. An FBI official warns that China is the top threat to U.S. critical infrastructure. Mandiant and Google...

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
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record