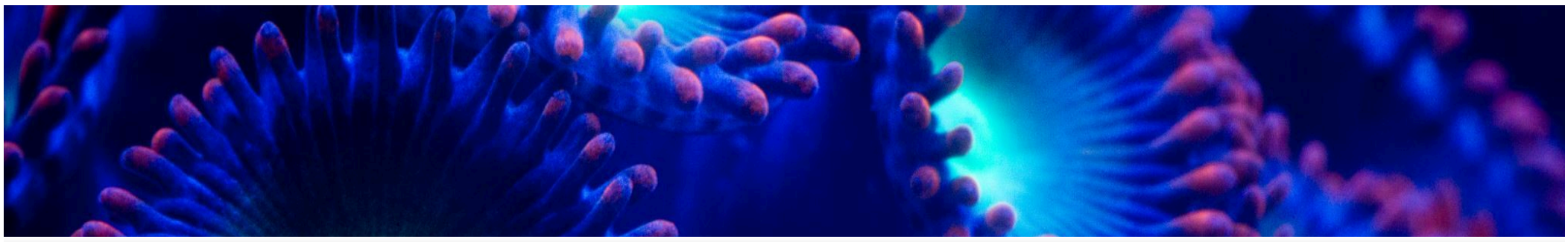


Week of June 9, 2025

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

Center for Internet Security Awards Nearly $250,000 to Purdue University's Technical Assistance Program

www.cisecurity.org

The Center for Internet Security, Inc. (CIS®) is proud to announce that Purdue University's Cyber Technical Assistance Program (cyberTAP) has been selected as the 2025 recipient of the Alan Paller Laureate Program grant. The nearly $250,000 award will support Purdue cyberTAP's mission to enhance cybersecurity resilience among rural electric cooperatives and other underserved critical infrastructur

Center for Internet Security Awards Nearly $250,000 to Purdue University's Technical Assistance Program

www.cisecurity.org

EAST GREENBUSH, N.Y., June 9, 2025 — The Center for Internet Security, Inc. (CIS ®) is proud to announce that Purdue University's Cyber Technical Assistance Program (cyberTAP) has been selected as the 2025 recipient of the Alan Paller Laureate Progra…

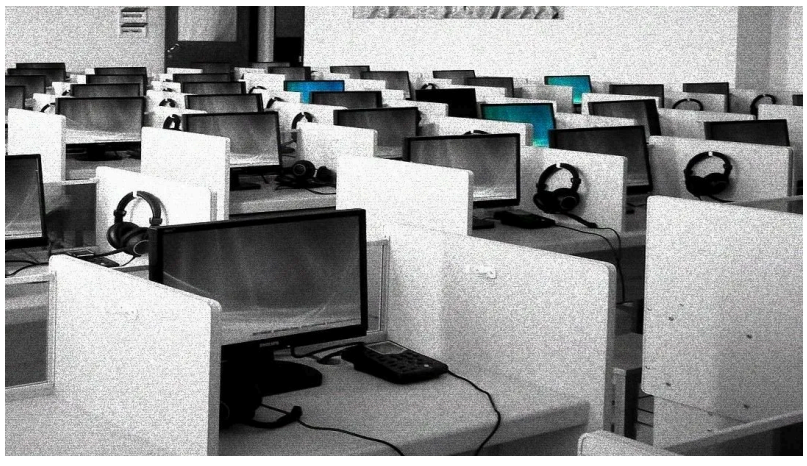
Cybercrimes, Scams & Incidents

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

Inside a Dark Adtech Empire Fed by Fake CAPTCHAs

krebsonsecurity.com

Late last year, security researchers made a startling discovery: Kremlin-backed disinformation campaigns were bypassing moderation on social media platforms by leveraging the same malicious advertising technology that powers a sprawling ecosystem of online hucksters and website hackers. A new report on the fallout from that investigation finds this dark ad tech industry is far more resilient and i



FIN6 cybercriminals pose as job seekers on LinkedIn to hack recruiters

therecord.media

Cybercriminals from the long-running FIN6 group are posing as job seekers on platforms like LinkedIn to infect recruiters with malware delivered through fake resumes, according to a new report.

Zero-Click AI Vulnerability Exposes Microsoft 365 Copilot Data Without User Interaction

thehackernews.com

A novel attack technique named EchoLeak has been characterized as a "zero-click" artificial intelligence (AI) vulnerability that allows bad actors to exfiltrate sensitive data from Microsoft 365 (M365) Copilot's context sans any user interaction.

Industry News

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

Patch Tuesday, June 2025 Edition – Krebs on Security

krebsonsecurity.com

2 thoughts on " Patch Tuesday, June 2025 Edition " Secret Squirrel June 10, 2025. Thanks Brian. KB5060842 failed to install on one of my PCs. According to windowslatest.com, there is an issue ...

CISA warns of SimpleHelp ransomware compromises after string of retail attacks

therecord.media

Ransomware gangs have been exploiting a vulnerability in remote device control software SimpleHelp during a recent string of attacks, according to federal cybersecurity officials.

ConnectWise to Rotate ScreenConnect Code Signing Certificates Due to Security Risks

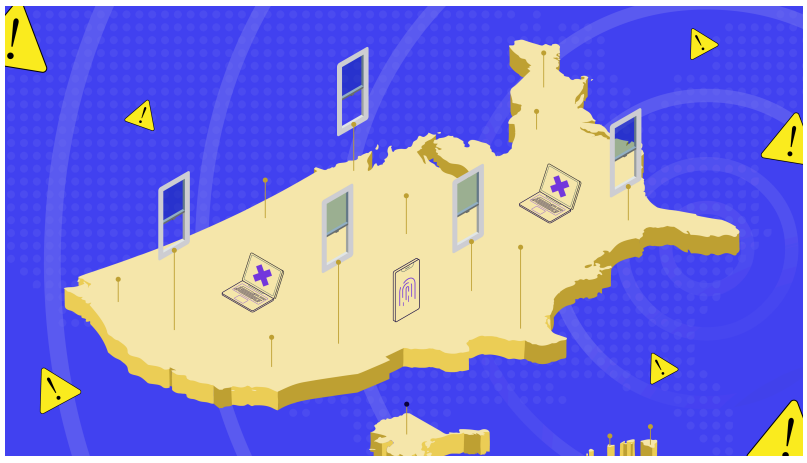
thehackernews.com

ConnectWise has disclosed that it's planning to rotate the digital code signing certificates used to sign ScreenConnect, ConnectWise Automate, and ConnectWise remote monitoring and management (RMM) executables due to security concerns.

The Hidden Threat in Your Stack: Why Non-Human Identity Management is the Next Cybersecurity Frontier

thehackernews.com

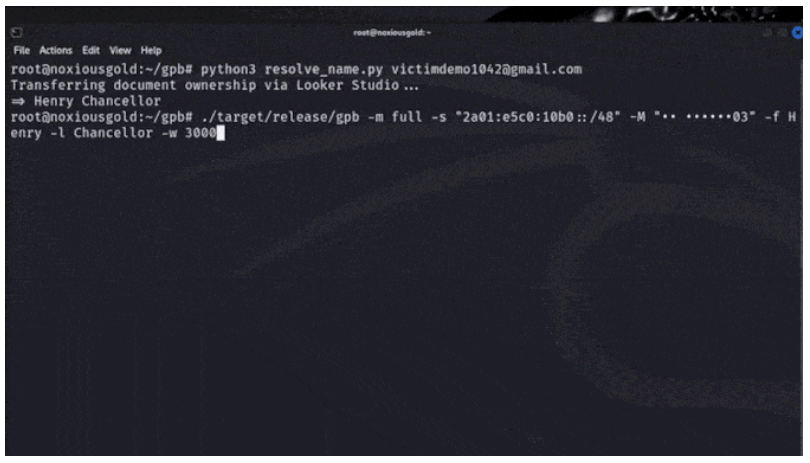
Modern enterprise networks are highly complex environments that rely on hundreds of apps and infrastructure services. These systems need to interact securely and efficiently without constant human oversight, which is where non-human identities (NHIs) come in. NHIs — including application secrets, API keys, service accounts, and OAuth tokens — have exploded in recent years, thanks to...



A house full of open windows: Why telecoms may never purge their networks of Salt Typhoon | CyberScoop

cyberscoop.com

When the news broke that a Chinese hacking group known as Salt Typhoon had penetrated multiple U.S. telecommunications networks, gained access to the phones of a presidential campaign, and collected geolocation data on high-value targets around Washi...



Researcher Found Flaw to Discover Phone Numbers Linked to Any Google Account

thehackernews.com

Google has stepped in to address a security flaw that could have made it possible to brute-force an account's recovery phone number, potentially exposing them to privacy and security risks.

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