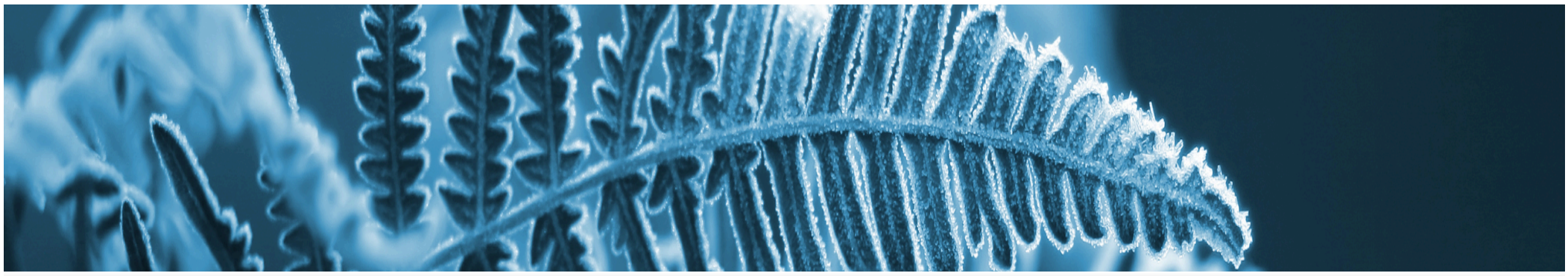


Week of January 26, 2025

Cybersecurity Headlines

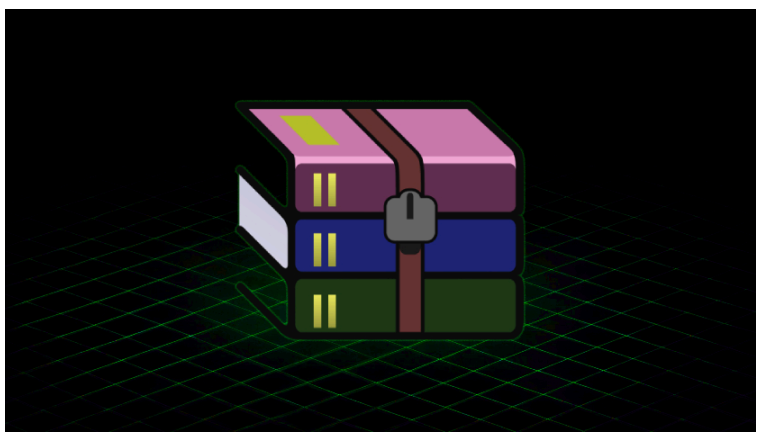
Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

Microsoft Office Zero-Day (CVE-2026-21509) - Emergency Patch Issued for Active Exploitation - The Hacker News

thehackernews.com

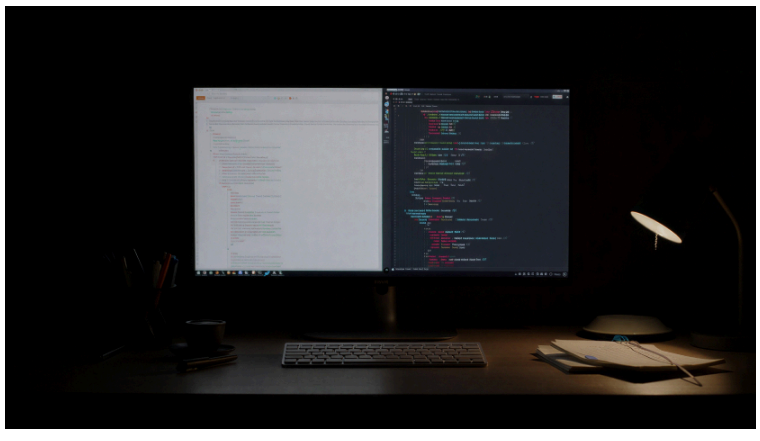
Microsoft released out-of-band patches for an actively exploited Microsoft Office zero-day, CVE-2026-21509, a security feature bypass flaw.



Google Warns of Active Exploitation of WinRAR Vulnerability CVE-2025-8088 - The Hacker News

thehackernews.com

Google confirms nation-state and cybercrime groups exploit a patched WinRAR flaw to gain persistence and deploy malware via Windows Startup folders.



Malicious VS Code AI Extensions with 1.5 Million Installs Steal Developer Source Code - The Hacker News

thehackernews.com

Security researchers found two AI-branded VS Code extensions with 1.5M installs that covertly send source code and files to China-based servers.

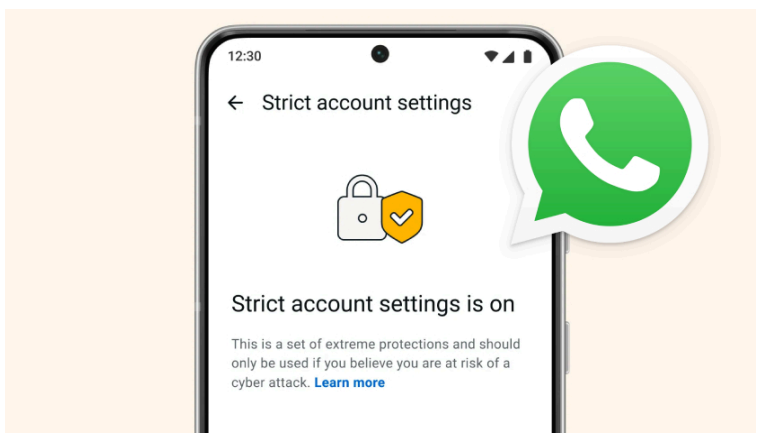
Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Public Outcry Surrounds West Virginia Data Center Tax Break Bill

www.govtech.com

State lawmakers are ramping up data center pursuit a year after passing controversial legislation aimed at drawing data centers to West Virginia at the expense of local government control and funding.



WhatsApp Rolls Out Lockdown-Style Security Mode to Protect Targeted Users From Spyware - The Hacker News

thehackernews.com

Meta is rolling out Strict Account Settings on WhatsApp and using Rust-based media code to protect journalists and high-risk users from spyware attack

Google Disrupts IPIDEA — One of the World's Largest Residential Proxy Networks - The Hacker News

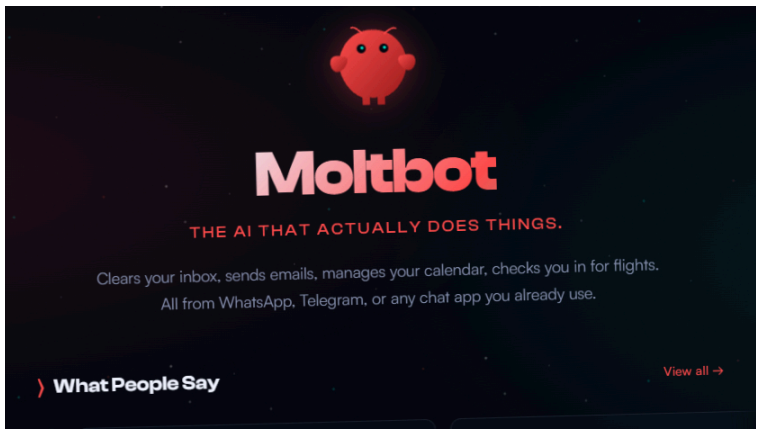
thehackernews.com

Google dismantled IPIDEA, a residential proxy network used by 550+ threat groups to hijack millions of consumer devices for cybercrime and espionage.

Who Operates the Badbox 2.0 Botnet? – Krebs on Security

krebsonsecurity.com

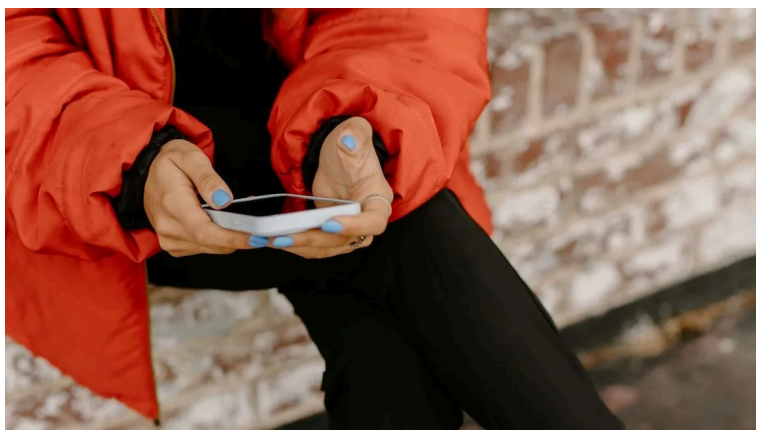
The control panel for the Badbox 2.0 botnet lists seven authorized users and their email addresses. Click to enlarge.



Fake Moltbot AI Coding Assistant on VS Code Marketplace Drops Malware - The Hacker News

thehackernews.com

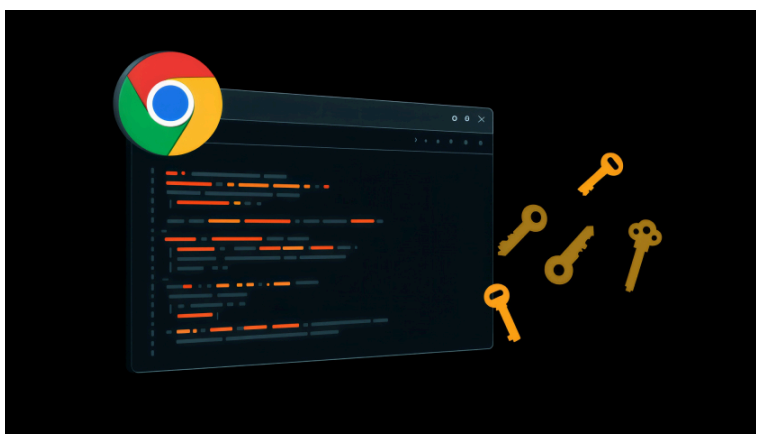
A fake VS Code extension posing as a Moltbot AI assistant installed ScreenConnect malware, giving attackers persistent remote access to developer syst



Dating-app giants investigate incidents after cybercriminals claim to steal data

therecord.media

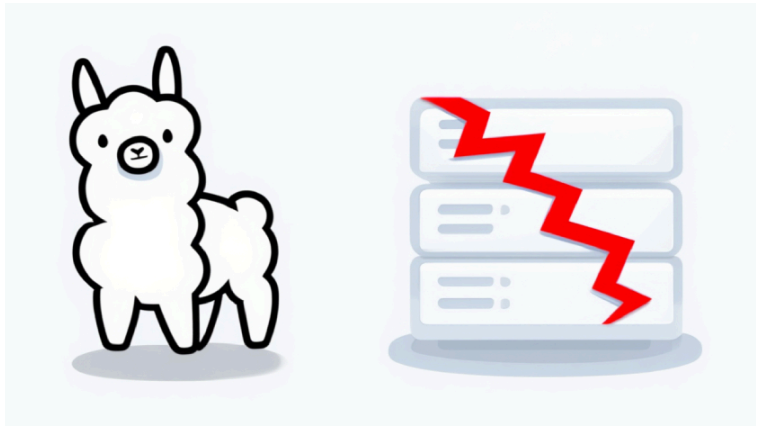
Bumble and Match said they each recently responded to network intrusions. The group ShinyHunters claimed to have stolen data from both.



Researchers Uncover Chrome Extensions Abusing Affiliate Links and Stealing ChatGPT Access - The Hacker News

thehackernews.com

Experts uncovered malicious Chrome extensions that replace affiliate links, exfiltrate data, and steal ChatGPT authentication tokens from users.



Researchers Find 175,000 Publicly Exposed Ollama AI Servers Across 130 Countries - The Hacker News

thehackernews.com

Over 175,000 publicly exposed Ollama AI servers across 130 countries, with many enabling tool calling that allows code execution and LLMjacking abuse.

Ex-Google Engineer Convicted for Stealing 2,000 AI Trade Secrets for China Startup - The Hacker News

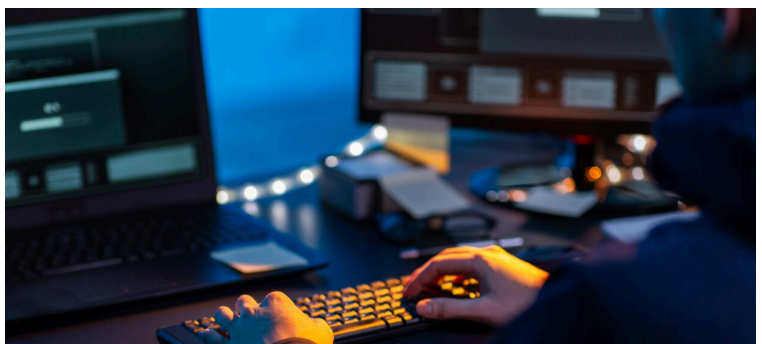
thehackernews.com

A U.S. jury convicted a former Google engineer of stealing over 2,000 AI trade secret documents to benefit China-linked companies, DOJ says.

Michigan Official Renews Call for Immediate Cyber Attack Reporting

www.govtech.com

Attorney General Dana Nessel is renewing her call for Michigan to pass a law requiring companies to immediately report data breaches to her office, which would allow for quickly alerting the public.



Baltimore Officials Clamp Down on Unauthorized Files Access

www.govtech.com

Following an internal audit by the city technology office, leaders said they have removed an unknown account that had gained access to confidential legal files. An IT analysis is underway.

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.*

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