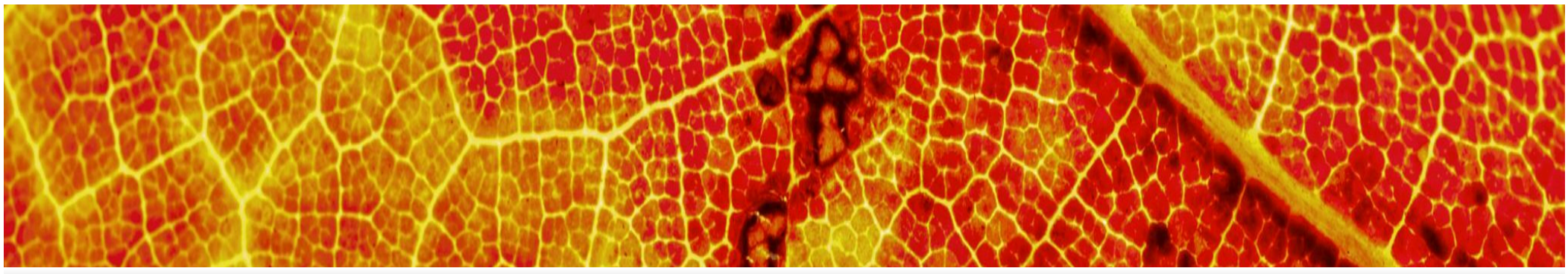
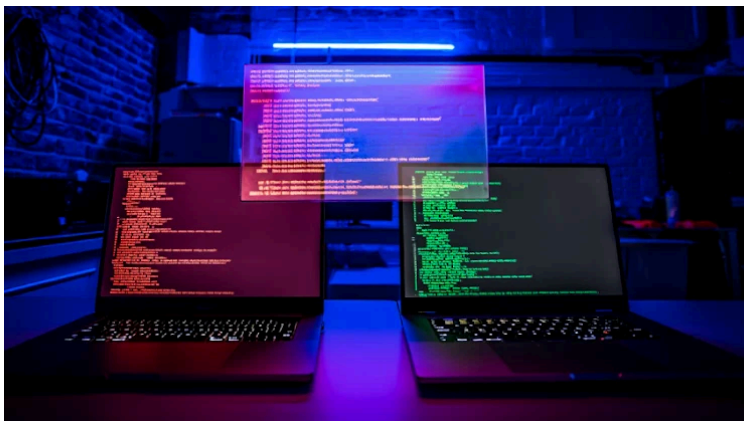


Week of October 14, 2025

Cybersecurity Headlines

Digital Threat Landscape

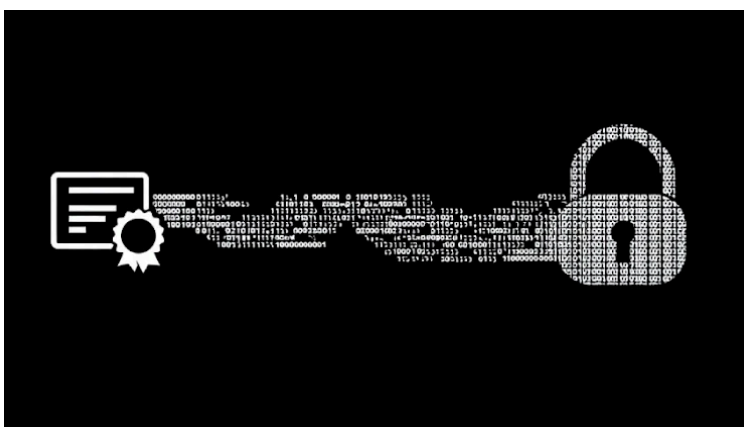
Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



North Korean Hackers Combine BeaverTail and OtterCookie into Advanced JS Malware - The Hacker News

thehackernews.com

OtterCookie v5 merges BeaverTail features with new keylogging and blockchain-based C2 tactics.



Microsoft Revokes 200 Fraudulent Certificates Used in Rhysida Ransomware Campaign - The Hacker News

thehackernews.com

Microsoft on Thursday disclosed that it revoked more than 200 certificates used by a threat actor it tracks as Vanilla Tempest to fraudulently sign malicious binaries in ransomware attacks. The certificates were "used in fake Teams setup files to del...

New Pixnapping Android Flaw Lets Rogue Apps Steal 2FA Codes Without Permissions - The Hacker News

thehackernews.com

Pixnapping side-channel can steal 2FA codes pixel-by-pixel on Android 13–16; CVE-2025-48561 patched Sept 2025 but workaround exists.

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Layoffs, reassignments further deplete CISA - Cybersecurity Dive

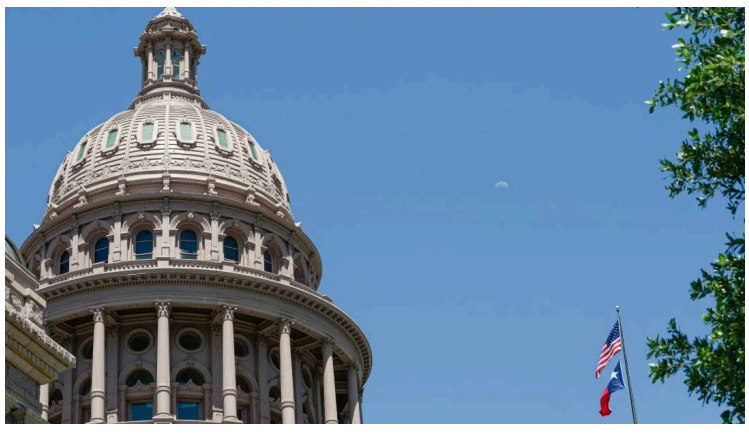
www.cybersecuritydive.com

Layoffs, reassignments further deplete CISA Some CISA staffers have been pushed out, while others are being told to move across the country for jobs outside their skill sets.

Florida sues Roku for illegally selling children's data, including precise geolocation

therecord.media

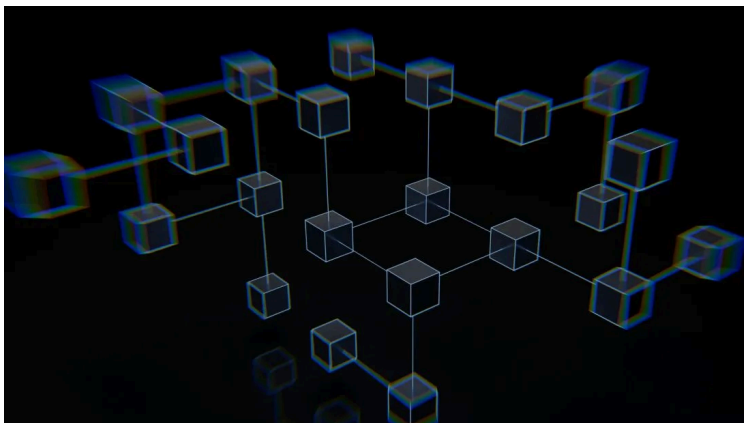
Florida on Tuesday sued the smart television company Roku for collecting and selling children's sensitive data, including information showing precise geolocation, without notice and parental consent.



Tech industry association sues to block Texas 'censorship' law age-gating access to apps

therecord.media

A leading technology industry association has sued Texas, seeking to block a state law that requires app stores to verify user ages to purchase and download apps.



North Korean hackers seen using blockchain to hide crypto-stealing malware

therecord.media

Google security researchers said they observed a Pyongyang-backed hacking group, tracked as UNC5342, deploying a method known as EtherHiding — a way of embedding malicious code inside smart contracts on decentralized networks such as Ethereum and BNB...

CISA warns of 'significant' threat to federal networks after nation-state hackers stole F5 source code, undisclosed bug info

therecord.media

The emergency directive orders all agencies to apply the latest updates for all at-risk F5 virtual and physical devices and downloaded software by October 22.

Email Bombs Exploit Lax Authentication in Zendesk – Krebs on Security

krebsonsecurity.com

Cybercriminals are abusing a widespread lack of authentication in the customer service platform Zendesk to flood targeted email inboxes with menacing messages that come from hundreds of Zendesk corporate customers simultaneously.

Patch Tuesday, October 2025 'End of 10' Edition – Krebs on Security

krebsonsecurity.com

Microsoft today released software updates to plug a whopping 172 security holes in its Windows operating systems, including at least two vulnerabilities that are already being actively exploited ...

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