Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

News from Tuesday, July 14, 2026
(Reported on Wednesday, July 15, 2026)

Government

US Government Launches AI Vulnerability Clearinghouse
Read more at Gov Info Security

U.S. Sanctions First VPN Service and Malware Cryptor Seller Over Ransomware Support
Read more at The Hacker News

Illinois Enacts First US Law Mandating AI Safety Audits
Read more at Gov Info Security

Financial Institutions

Big Banks Accelerate Rollout Of AI 'Digital Employees'
Read more at CUtoday.info

Healthcare

Lucent Health Solutions to Pay Up to 1.95M to Settle Data Breach Litigation
Read more at HIPAA Journal

Other

Microsoft Patches Record 622 Flaws, Including Two Zero-Days Under Active Attack
Read more at The Hacker News

SAP warns of critical flaws in NetWeaver and Commerce Cloud
Read more at Bleeping Computer

Cursor IDE Auto-Executes Malicious Code in Poisoned Repos
Read more at Dark Reading

New phishing kits target Microsoft 365 accounts, evade MFA
Read more at Bleeping Computer

LabubaRAT Masquerades as NVIDIA Software to Control Windows Hosts
Read more at The Hacker News

News from Tuesday, July 14, 2026
(Reported on Wednesday, July 15, 2026)

Nearly 300 GitHub repos pose as legit software to push malware
Read more at Bleeping Computer

6 GHz Wi-Fi Flaws Could Disrupt Critical Systems
Read more at Dark Reading

SonicWall SMA appliances targeted in zero-day attacks (CVE-2026-15409, CVE-2026-15410)
Read more at Help Net Security

Microsoft's Secure Boot has been broken for a decade and no one noticed until now
Read more at Arstechnica