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 Thursday May 14, 2026
(Reported on Friday May 15, 2026)

Government

US charges suspected Dream Market admin arrested in Germany
Read more at Bleeping Computer

US CISA adds a flaw in Cisco Catalyst SD-WAN to its Known Exploited Vulnerabilities catalog
Read more at Security Affairs

Financial Institutions

Cryptohack Roundup: Banking Trojan Targets Crypto Firms
Read more at BankInfoSecurity

ECB: AI Means European Banks Must Hasten Cybersecurity Pace
Read more at HealthCareInfoSecurity

Healthcare

Atrium Health & Interim HealthCare Affected by Business Associate Data Breaches
Read more at TheHIPAAJournal

Other

FlowerStorm phishing gang adopts virtual-machine obfuscation to evade email defenses
Read more at CSO Online

KongTuke hackers now use Microsoft Teams for corporate breaches
Read more at Bleeping Computer

Linux Kernel bug Fragnesia allows local root access attacks
Read more at Security Affairs

OpenAI confirms security breach in TanStack supply chain attack
Read more at Bleeping Computer

Zero-day exploit completely defeats default Windows 11 BitLocker protections
Read more at Arstechnica

News from Thursday May 14, 2026
(Reported on Friday May 15, 2026)

Broadcom releases VMware Fusion security update for root access bug
Read more at Security Affairs

PraisonAI vulnerability gets scanned within 4 hours of disclosure
Read more at CSO Online

'FrostyNeighbor' APT Carefully Targets Govt Orgs in Poland, Ukraine
Read more at DarkReading

18-Year-Old NGINX Rewrite Module Flaw Enables Unauthenticated RCE
Read more at TheHackerNews