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 Friday November 14, 2025, through Sunday November 16, 2025 (Reported on Monday November 17, 2025)

Government

DOJ Continues Crackdown on North Korea's Cyber Schemes
Read more at GovInfoSecurity

Ed. Dept. Layoffs Are Reversed, But Staff Fear Things Won't Return to Normal
Read more at Edweek.org

Financial Institutions

Hackers Exploited Cisco ISE Zero-Day
Read more at BankInfoSecurity

Bankers Reportedly Launch New Salvo In Bid To Undermine CUs, Push Treasury On Form 990 Rule
Read more at CUtoday.info

Healthcare

Warning Issued About Akira Ransomware as Attacks on Critical Infrastructure Accelerate
Read more at TheHIPAAJournal

Document Tech Firm Hit as New Cyber Gang Expands Reach
Read more at HealthcareInfoSecurity

Other

Microsoft: Windows 10 KB5068781 ESU update may fail with 0x800f0922 errors
Read more at Bleeping Computer

Honeypot: FortiWeb CVE-2025-64446 Exploits, (Sat, Nov 15th)
Read more at SANS

Decades-old 'Finger' protocol abused in ClickFix malware attacks
Read more at Bleeping Computer

Jaguar Land Rover cyberattack cost the company over $220 million
Read more at Bleeping Computer

RondoDox Exploits Unpatched XWiki Servers to Pull More Devices Into Its Botnet

News from Friday November 14, 2025, through Sunday November 16, 2025 (Reported on Monday November 17, 2025)

Read more at TheHackerNews

Five Plead Guilty in U.S. for Helping North Korean IT Workers Infiltrate 136 Companies
Read more at TheHackerNews