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 Monday October 13, 2025 (Reported on Tuesday October 14, 2025)

Government

Pro-Russian TwoNet Hacktivists Target Water Utility Honeypot
Read more at GovInfoSecurity

Financial Institutions

Salesforce Extortion Group Leaks Data After FBI Disruption
Read more at BankInfoSecurity

Mass Federal Firings Begin: Thousands Laid Off As Treasury Reportedly Shuts Down CDFI Fund
Read more at CUtoday.info

Healthcare

SimonMed says 1.2 million patients impacted in January data breach
Read more at Bleeping Computer

ALN Medical Management to Pay $4 Million to Settle Class Action Data Breach Lawsuit
Read more at The HIPAA Journal

Other

Microsoft restricts IE mode access in Edge after zero-day attacks
Read more at Bleeping Computer

SonicWall VPN accounts breached using stolen creds in widespread attacks
Read more at Bleeping Computer

Microsoft investigates outage affecting Microsoft 365 apps
Read more at Bleeping Computer

Microsoft: Windows 11 Media Creation Tool broken on Windows 10 PCs
Read more at Bleeping Computer

Hackers can steal 2FA codes and private messages from Android phones
Read more at Arstechnica

Researchers Warn RondoDox Botnet is Weaponizing Over 50 Flaws Across 30+ Vendors

News from Monday October 13, 2025
(Reported on Tuesday October 14, 2025)

Read more at TheHackerNews

Microsoft Locks Down IE Mode After Hackers Turned Legacy Feature Into Backdoor
Read more at TheHackerNews

Oracle releases emergency patch for new E-Business Suite flaw
Read more at Bleeping Computer

Harvard investigating breach linked to Oracle zero-day exploit
Read more at Bleeping Computer

Why Unmonitored JavaScript Is Your Biggest Holiday Security Risk
Read more at TheHackerNews

Astaroth Banking Trojan Abuses GitHub to Remain Operational After Takedowns
Read more at TheHackerNews

New Rust-Based Malware "ChaosBot" Uses Discord Channels to Control Victims' PCs
Read more at TheHackerNews

Critical infrastructure CISOs Can't Ignore 'Back-Office Clutter' Data
Read more at DarkReading