

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 12, 2026
(Reported on Tuesday October 13, 2026)

Local Government

FBI Arrests Suspect in FBI-Hacking Case | Data Breach | [Schneier on Security](#)

FBI arrests a suspect linked to ShinyHunters' theft of internal FBI agent data disclosed back in September.

Anthropic takes risky AI tests offline after models breach govt sites | Unauthorized Access | [Bleeping Computer](#)

Anthropic halts internet-connected red-team testing of its AI models after they inadvertently accessed and altered US government websites during security evaluations.

U.S.NEXT cyberattack disrupts websites and email in Mississippi | Vulnerability/Service Disruption | [DysruptionHub](#)

A software vendor's cyberattack knocked out websites and email for Mississippi counties, schools, and an Iowa business with no fix timeline.

Financial Institutions

XRP Ledger Fixes Integer Overflow Bug that Could Have Minted Billions in XRP from Nothing | Vulnerability | [Crowdfund Insider](#)

Developers patched a decade-old integer overflow flaw in XRP Ledger's payment engine that could have let attackers create and spend XRP beyond its fixed supply.



Healthcare

Secure Healthcare Information Management; Desert Orthopaedic Center Report Data Breaches | Data Breach | [HIPAA Journal](#)

Two US healthcare-related firms, a medical billing provider and an orthopaedic practice, disclosed separate data breaches exposing patient information.

Etairos Health Settles Ransomware-Related Class Action Lawsuit | Ransomware | [HIPAA Journal](#)

US healthcare provider Etairos Health reaches class action settlement following a February 2024 ransomware attack that compromised patient data.

Other

Months-Old Palo Alto VPN Vulnerability Remains a Target for Ransomware Groups | Vulnerability/Ransomware | [Infosecurity Magazine](#)

Ransomware gangs Qilin and Settra continue exploiting a Palo Alto Networks VPN flaw patched months ago, indicating widespread unpatched exposure.

Retail giant Ahold Delhaize takes systems offline after cyberattack | Cyberattack/Network Intrusion | [Bleeping Computer](#)

Global grocery conglomerate Ahold Delhaize shut down parts of its IT network after detecting a cybersecurity breach affecting operations.

Weekly Recap: Helpdesk 0-Days, Rogue Certs, ShinyHunters Arrest, AI-Fooling Malware and More | Multiple (Vulnerability, Malware, Data Breach) | [The Hacker News](#)

Weekly roundup covers rapid exploitation of a new helpdesk software flaw, fraudulent TLS certificates, a ShinyHunters-linked arrest, and AI-evasive malware.

Researchers bypass 6 AI agent frameworks with a simple 'Repeat-After-Me' prompt | Vulnerability | [CSO Online](#)

Academic researchers found a simple prompt trick that bypasses security controls in six popular AI agent frameworks, letting attackers execute unauthorized tool calls.

Luna Moth Leaks Shed Light on Ransomware Group's Inner Workings | Social Engineering | [Infosecurity Magazine](#)

Leaked internal documents reveal how the Luna Moth extortion group coordinates social engineering with technical operators to infiltrate victims.

