# 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 August 10, 2026
## (Reported on Tuesday August 11, 2026)

---

## Local Government

**FBI, South Korea warn of Gunra ransomware gang targeting critical infrastructure** | Ransomware | The Record

*FBI and South Korean authorities warn that Gunra ransomware operators are exploiting firewall vulnerabilities to breach critical infrastructure organizations.*

**Kimsuky Builds Offline AI Stack to Boost Phishing and Automate Malware Development** | Malware | The Hacker News

*Researchers found North Korea's Kimsuky group running offline AI tools to sharpen phishing lures and speed up malware coding.*

## Financial Institutions

**LexisNexis shuts down services after suspicious activity on servers** | Data Breach | Bleeping Computer

*Data broker LexisNexis took several services offline after detecting suspicious activity on servers managed by a third-party vendor.*

## Healthcare

**Data Breaches Announced by Loma Linda University Health & UCLA Health** | Data Breach | HIPAA Journal

*Two US healthcare systems, Loma Linda University Health and UCLA Health, disclosed separate data breach incidents affecting patient information.*

## Other

**Weekly Recap: AI Goes Rogue, Metabase 0-Day, MCP Supply-Chain Attacks, and Router Backdoors** | Vulnerability | The Hacker News

*Weekly roundup covers a Metabase zero-day, MCP supply-chain compromises, router backdoors, and AI-related security risks.*

**OpenAI says Astra could reach 'critical' cyber capability, tightens safeguards** | AI-Enabled Cyber Capability | CSO Online

*OpenAI warns its upcoming Astra model may approach autonomous exploit-development capability, prompting tightened AI safety controls.*

**Coruna, DarkSword iOS Exploits Proliferate Globally** | Zero-Day/Exploit Chain | Dark Reading

*Advanced iPhone spyware exploit chains once exclusive to nation-state actors are now being adopted by organized cybercrime groups worldwide.*

**Cisco Warns of High-Severity ClamAV Vulnerabilities With Public PoC** | Vulnerability | Security Week

*Cisco disclosed high-severity ClamAV flaws with public proof-of-concept code that could let unauthenticated attackers trigger denial-of-service conditions.*