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 Wednesday August 12, 2026
(Reported on Thursday August 13, 2026)

Local Government

Lazarus hackers exploited Windows zero-day to target defense firms | Zero-Day | Bleeping Computer

North Korea-linked Lazarus Group exploited a Windows zero-day vulnerability to breach defense contractors via fake job recruitment lures.

Financial Institutions

Android malware combo takes out loans and relays victims' credit cards | Malware | Bleeping Computer

New Android malware pairing, WindRelay and SpyNote RAT, relays stolen NFC card data to attackers in real time and enables fraudulent loans.

WindRelay Malware Pairs With SpyNote RAT in Live-Call Scam | Malware | Infosecurity Magazine

New WindRelay NFC-relay malware combined with SpyNote Android RAT enables fraudsters to clone bank cards during live phone-call scams.

Healthcare

Data Breaches Announced by Five Small Healthcare Organizations | Data Breach | HIPAA Journal

Five small US healthcare providers disclosed separate data breaches compromising patient information, per HIPAA Journal roundup.

Critical Vulnerabilities Identified in Popular Consumer Fertility Device | Vulnerability | HIPAA Journal

Researchers found critical security flaws in a consumer fertility hormone tracker and a vagus nerve stimulator device.

Other

Hackers exploit critical Adobe Commerce flaw to hijack customer accounts | Vulnerability | Bleeping Computer

Attackers are actively exploiting a critical Adobe Commerce and Magento vulnerability to take over customer accounts on e-commerce sites.

OpenAI, Anthropic, Google API Flaw Let Weaker AI Models Decode Stronger Models' Reasoning | Vulnerability | The Hacker News

Researchers found a flaw letting encrypted reasoning tokens from major AI providers' APIs be replayed across sessions, exposing internal reasoning and leaked secrets like API keys.

Hundreds of fake Chrome VPN extensions route traffic through a proxy | Malicious Browser Extension / Supply Chain | Bleeping Computer

Researchers found over 737 Chrome Web Store extensions posing as popular VPN/proxy tools that secretly funneled user traffic through a single SOCKS5 proxy operator.

Malicious LiteLLM Releases Tied to Trivy Hack May Have Exposed 2,100+ Organizations | Supply Chain | The Hacker News

Malicious LiteLLM PyPI packages briefly live in March stole credentials from thousands of systems, with new data suggesting over 2,100 organizations were exposed.