

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 Thursday October 08, 2026
(Reported on Friday October 09, 2026)**

Local Government

FBI Seizes Domains Used in Flax Typhoon Attacks | Nation-State Cyber Espionage / Infrastructure Takedown | [BankInfoSecurity](#)

FBI seized seven domains linked to China-backed Flax Typhoon hackers used for scanning, phishing, and data theft against critical infrastructure.

Watchdog to examine summertime hack of DHS information network, other incidents | Data Breach | [NextGov](#)

GAO review finds DHS delayed informing Congress about a summer cyber intrusion into its information network and related incidents.

Financial Institutions

Wazza Phishkit Targets Banking, Government, and Manufacturing Across the US, EU, and Australia | Phishing | [The Hacker News](#)

Researchers uncover Wazza, a sophisticated phishing kit with built-in traffic filtering and session controls targeting banks, manufacturers, and government bodies in the US, EU, and Australia.

Healthcare

Almost 20 Million Individuals Affected by 2025 Data Breach at Oracle Health/Cerner | Data Breach | [HIPAA Journal](#)

Oracle Health disclosed that a 2025 breach of legacy Cerner servers exposed protected health information of nearly 20 million patients.



Reported cyberattack disrupts care at Green Clinic in Louisiana | Unknown/Suspected Cyberattack | [DysruptionHub](#)

A Louisiana medical clinic suffered a suspected cyberattack that knocked out access to patient records and scheduling systems.

Laboratory Services Cooperative Agrees to Pay \$6.1 Million to Settle Data Breach Litigation | Data Breach | [HIPAA Journal](#)

A Planned Parenthood-affiliated lab testing provider will pay \$6.1 million to settle litigation over a patient data breach.

Other

'AgentCorruption' Puts AWS Environments At Risk With Single Prompt | Vulnerability | [Dark Reading](#)

Researchers disclosed a patched AWS Bedrock AgentCore flaw letting a single malicious prompt hijack an AI agent to compromise an entire cloud fleet.

OpenAI says Iran, Russia used AI journalists, think tanks to influence Western media | Disinformation/Influence Operation | [CyberScoop](#)

OpenAI disrupted Iranian and Russian AI-driven influence campaigns using fake journalist and think-tank personas to sway Western media narratives.

Low-cost Android phones ship with residential proxy malware | Supply Chain / Malware | [Bleeping Computer](#)

Researchers found budget Android phones preloaded with firmware malware that silently installs apps, commits ad fraud, and converts devices into residential proxies.

FakeGit malware campaign returns with 17,610 malicious GitHub repos | Malware/Supply Chain | [Bleeping Computer](#)

A large-scale GitHub campaign using over 17,000 fake repositories is distributing SmartLoader malware and the StealIC infostealer to unsuspecting developers.

