

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 Tuesday October 06, 2026
(Reported on Wednesday October 07, 2026)

Local Government

Coast Guard Boardings of Hacked Vessels: New Details | Vulnerability Exploitation | [BankInfoSecurity](#)

Federal officials reveal hackers exploited known, unpatched vulnerabilities in onboard systems of two US-bound oil tankers, prompting Coast Guard and FBI boardings.

Financial Institutions

ZachXBT Posed as Client to Map Chinese Money Laundering Network that Allegedly Laundered \$1B+ for North Korea's Lazarus Group | Money Laundering / Cryptocurrency Theft | [Crowdfund Insider](#)

A crypto investigator infiltrated a Chinese money-laundering network allegedly used to launder over \$1 billion in crypto stolen by North Korea's Lazarus Group.

Healthcare

Critical Medical Devices Unable to Support PQC Transition | Vulnerability | [Infosecurity Magazine](#)

Research finds nearly all internet-connected medical devices lack cryptographic capability to adopt post-quantum encryption standards.

Other

Welcome to the Jungle: What We Found Inside 15,465 Public MCP Servers | Vulnerability/Supply Chain | [The Hacker News](#)

Security researchers analyzed thousands of public MCP servers and found widespread misconfigurations and critical vulnerabilities exposing AI agent integrations.



Asos hit by extortion hack that may have compromised some customer data | Extortion/Data Breach | [Engadget](#)

Online fashion retailer Asos disclosed a breach after attackers sent customers a push notification announcing an extortion attempt and possible data theft.

Ninja Forms plugin flaw exploited to hack WordPress sites | Vulnerability | [Bleeping Computer](#)

Attackers are actively exploiting stored XSS flaws in the Ninja Forms and WPC Product Bundles WordPress plugins to plant backdoors and create rogue admin accounts.

ClickFix Smuggles Payloads Through Browser Cache to Bypass Windows Run Limits | Social Engineering | [The Hacker News](#)

Microsoft identifies new ClickFix variant that hides malicious scripts as PNG files in browser cache to evade Windows execution restrictions.

Fake ChatGPT, Gemini Sites steal advertising accounts, MFA codes | Phishing | [Bleeping Computer](#)

Attackers use fake ChatGPT, Gemini, Claude, and Perplexity websites with browser-in-browser phishing to steal advertising account credentials and MFA codes.

AI accelerates n-day attacks, as flaw disclosures and exploits double | Vulnerability | [CSO Online](#)

Google threat researchers find AI tools are speeding attackers' ability to weaponize disclosed vulnerabilities, as n-day exploitation surges past last year's total.

