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, June 30, 2026
(Reported on Wednesday, July 1, 2026)

Government

CISA: Windows BlueHammer flaw now exploited by ransomware gangs
Read more at Bleeping Computer

Financial Institutions

Silent Swap Crypto Clipper Uses Fake Google Notes Extension to Replace Wallet Addresses
Read more at TheHackerNews

Healthcare

Data Breaches Reported by Amicus Solutions: Huntsville Hospital Health System
Read more at HIPAAJournal

Insurance giant Aflac discloses data breach after subsidiary hack
Read more at Bleeping Computer

Washington Dept. Health & Social Services Insider Breach Affects 8,600 Individuals
Read more at HIPAAJournal

Other

Fake Perplexity extension on Chrome Web Store tracked searches
Read more at Bleeping Computer

Microsoft Warns Poisoned MCP Tool Descriptions Can Make AI Agents Leak Data
Read more at TheHackerNews

Blackfield ransomware asks Nidec Corporation for $2 million ransom
Read more at Bleeping Computer

New BioShocking Attack Tricks AI Browsers Into Leaking User Credentials
Read more at TheHackerNews

News from Tuesday, June 30, 2026
(Reported on Wednesday, July 1, 2026)

Attackers actively exploit the Oracle E-Business Suite flaw CVE-2026-46817
Read more at Security Affairs

AirDrop and Quick Share Flaws Let Nearby Attackers Trigger Crashes and Bypass Checks
Read more at TheHackerNews

Attackers Hijack Exposed AI Endpoints to Power Offensive Ops
Read more at DarkReading

RustDuck Botnet Rebuilds in Rust to Hijack Routers and Servers for DDoS
Read more at TheHackerNews