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 November 16, 2026
(Reported on Tuesday November 17, 2026)

Financial Institutions

JPMorgan Software Bug Disrupts US Banking Services | Software Outage/IT Failure | BankInfoSecurity

A software bug in JPMorgan Chase's on-premises systems caused widespread online banking outages and delayed interbank transactions, with no evidence of cyberattack.

Other

Optimizely hack infected CNN, Fox News, BBC, Salesforce sites with malware | Supply Chain | Bleeping Computer

Compromised Optimizely CMS platform injected malicious JavaScript into CNN, Fox News, BBC, Salesforce, and other major sites to steal crypto and payment data.

Amazon Uncovers AI Agent Campaign Targeting LiteLLM, Dify, and Other Apps for API Keys | Vulnerability/Credential Theft | The Hacker News

Amazon's threat intelligence team detected autonomous AI agents scanning exposed LiteLLM, Dify, and similar AI platforms to harvest API keys for further attacks.

Fandango says hackers stole payment card details from checkout pages | Data Breach | Bleeping Computer

Fandango Media disclosed that attackers compromised its checkout pages to steal customers' payment card information.

Weekly Recap: N-able 0-Days, Windows 0-Days, Chrome 0-Days, Fridge 0-Days, and More Bad Days | Vulnerability | The Hacker News

Weekly roundup covers multiple zero-day flaws in N-able, Windows, and Chrome, plus supply-chain and default-password incidents affecting various organizations.

Google Project Zero cuts bug disclosures to 30 days amid AI threats | Vulnerability Disclosure Policy | Bleeping Computer

Google's Project Zero shortens its vulnerability disclosure window to a fixed 30 days, citing faster AI-assisted exploit development.

Retadup Worm Resurfaces 7 Years After Takedown to Spread CoffeeLoader Malware | Malware | The Hacker News

Researchers found a new CoffeeLoader malware variant using a patched legitimate tool to load malicious payloads, linked to the resurfaced Retadup worm technique.

SilentAir and LIMINAL PANDA Target Telecom Networks to Spy on Subscribers | Espionage/Telecom Network Intrusion | Security Affairs

Security researchers identified two threat actors, SilentAir and LIMINAL PANDA, infiltrating mobile carrier networks to intercept calls and texts and surveil subscribers.

Ransomware Attacks Increase Behind AI, But Payments Decline | Ransomware | Dark Reading

Report finds AI tools are helping ransomware gangs craft phishing lures and locate valuable data, even as victim ransom payments fall.

Infoblox customer and staff data exposed in Sharepoint breach | Data Breach | The Register

Networking security vendor Infoblox is probing a breach exposing customer and employee data via a compromised SharePoint instance.

NoisyTCP bug gives Linux servers a remote crash problem 11 years in the making | Vulnerability | The Register

A long-standing Linux kernel TCP flaw lets remote attackers crash entire host systems, even affecting containerized services.
