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 November 12, 2026
(Reported on Friday November 13, 2026)

Local Government

Attackers Use Autonomous AI to Target Semiconductor, Defense and Civil Society Sectors | Autonomous AI-driven Intrusion | Palo Alto Networks Unit 42

Unit 42 details how threat actors weaponized the open-source Cairn AI agent framework to autonomously breach semiconductor, defense and civil society organizations.

AI found widespread IoT vulnerabilities more quickly and cheaply than humans could | Vulnerability | Cybersecurity Dive

Researchers used AI tools to rapidly uncover numerous security flaws in widely deployed IoT and embedded systems tied to critical infrastructure.

Financial Institutions

FBI disrupts intricate North Korean fake-call scheme tied to $400M in crypto theft | Social Engineering | NextGov

FBI dismantled a North Korean social-engineering operation using spoofed voice calls to steal $400M in cryptocurrency from targeted holders and developers.

Healthcare

Minnesota Epilepsy Group Falls Victim to Second 2026 Cyberattack | Data Breach | HIPAA Journal

Minnesota Epilepsy Group, a specialty medical practice, disclosed its second cyberattack and patient data breach within 2026.

Other

US seizes North Korean hacking infrastructure, $1.2 billion in cryptocurrency stolen from Binance | Social Engineering/Cryptocurrency Theft | CyberScoop

US authorities seized North Korean APT38 hacking infrastructure, including deepfake video tools, tied to the $1.2 billion Binance cryptocurrency theft.

Police dismantle Gootloader, CastleRAT, StealC malware infrastructure | Malware | Bleeping Computer

International law enforcement coalition seized servers and domains tied to Gootloader, CastleRAT, and StealC malware operations.

Critical Red Hat Quay Flaw Lets Attackers Read and Overwrite All Private Container Images in a Registry | Vulnerability | The Hacker News

Red Hat Quay registry had a critical flaw letting attackers read and overwrite private container images across repositories, with patches now released.

Apache HTTP Server patches critical HTTP/2 remote code execution flaw | Vulnerability | Bleeping Computer

Apache patched a critical HTTP/2 module flaw in its HTTP Server that could let unauthenticated attackers achieve remote code execution.

Node.js Fixes 16 Flaws, Including HTTP/2 Bugs That Crash Servers and Leak Other Connections' Data | Vulnerability | The Hacker News

Node.js patched 16 vulnerabilities, including HTTP/2 flaws letting attackers crash servers or leak other users' data across connections.

New Windows SignDrop zero-day gives hackers SYSTEM privileges | Zero-Day | Bleeping Computer

Researcher publicly discloses an unpatched Windows zero-day flaw named SignDrop that allows attackers to escalate privileges to SYSTEM level.

Trained to betray: How post-training supply chain attacks hijack coding agents | Supply Chain | Microsoft Security Blog

Microsoft researchers detail how poisoned training data or model checkpoints can backdoor AI coding agents to enable remote code execution.
