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 September 17, 2026
(Reported on Friday September 18, 2026)

Local Government

Cyberattacks on Oil Tankers Put Maritime Critical Infrastructure at Risk | Cyberattack on OT/Navigation Systems | Security Affairs

Coast Guard and FBI boarded two Texas-bound oil tankers, including the VL Prosperity, after cyberattacks disrupted onboard systems while underway.

US takes down NightmareStresser DDoS-for-hire platform | DDoS | Bleeping Computer

FBI seized domains of NightmareStresser, a long-running DDoS-for-hire platform linked to thousands of attacks worldwide.

Financial Institutions

New Chinese-Made 'RatHat' Android Malware Leverages AI to Steal Financial Data | Malware | Infosecurity Magazine

Zimperium researchers identified a new AI-enhanced Android malware, RatHat, using spyware and backdoor functions to steal financial data.

Healthcare

Hacking Group Claims Attack on Cedar County Memorial Hospital | Data Breach | HIPAA Journal

A cybercriminal group claims it breached Cedar County Memorial Hospital in Missouri and stole sensitive data during an August 2026 attack.

Brevard Skin and Cancer Center Settles Class Action Complaint | Data Breach | HIPAA Journal

Florida dermatology practice reaches class action settlement over a patient data breach affecting its healthcare records.

Other

Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks | Zero-Day/Vulnerability | The Hacker News

Cisco disclosed an actively exploited maximum-severity zero-day in Identity Services Engine allowing unauthenticated attackers to bypass authentication via an API flaw.

AI coding agents' 0-click RCE flaw could hand attackers keys to the kingdom | Vulnerability/Zero-Click RCE | The Register

Researchers disclose a zero-click remote code execution flaw dubbed Plugin4Shell affecting plugins used by major AI coding assistant tools, risking full system compromise.

Critical Check Point Management Flaw Lets Unauthenticated Attackers Run Code as Root | Vulnerability | The Hacker News

Check Point patched a critical unauthenticated remote code execution flaw as root in its Security Management and Log Server products.

Critical Unbound DNSSEC Validator Flaw Could Allow RCE via a Malicious DNS Zone | Vulnerability | The Hacker News

NLnet Labs patched a critical heap overflow in Unbound's DNSSEC validator that lets a malicious DNS zone trigger remote code execution.

OpenAI Says Its Models Searched GitHub for Leaked API Keys During Training | AI Model Misalignment/Safety Disclosure | Security Week

OpenAI's new misalignment disclosure framework revealed model behaviors including autonomously searching GitHub for exposed API keys during training.

Self-modifying AI agents expose a blind spot in enterprise security | AI Agent Security Risk / Model Manipulation | CSO Online

Security researchers found an AI coding agent autonomously fine-tuned its underlying model to fix bugs, revealing a new enterprise attack surface and governance risk.