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 Wednesday September 16, 2026
(Reported on Thursday September 17, 2026)

Local Government

Coast Guard, FBI board US-bound foreign ships in order to probe for cyberattacks | Network Compromise | CyberScoop

US Coast Guard and FBI conducted joint security boardings of foreign vessels after detecting signs their shipboard networks had been compromised.

New CISA Guidance Helps Critical Infrastructure Detect, Observe and Impede Malicious Cyber Activity | Critical Infrastructure Security | CISA
CISA released guidance on using cyber decoys, including lures, tripwires, honeytokens, and honeypots, to help critical infrastructure organizations detect, observe, and disrupt malicious activity earlier.

Financial Institutions

Malware bypasses browser checks to force install Chrome, Edge extensions | Malware | Bleeping Computer

A banking-focused malware toolkit called KREMLIN forcibly installs malicious Chrome and Edge extensions to steal credentials and session tokens.

Healthcare

CVS, Criteo Settle Web Tracker Data Privacy Suit for $20.5M | Data Breach | BankInfoSecurity

CVS Health and ad-tech firm Criteo will pay $20.5 million to settle claims that website trackers leaked patients' health data without consent.

Other

Google Pixel phones pwned in zero-click attacks | Zero-Day/Zero-Click Exploit | The Register

Attackers exploited zero-click vulnerabilities in Google Pixel phones, prompting CISA to order federal agencies to patch within three days.

Attackers Exploit Issabel Framework Flaw Enabling Unauthenticated OS Command Execution | Vulnerability Exploitation | The Hacker News

Hackers actively exploit a critical hard-coded credential flaw in Issabel PBX framework allowing unauthenticated remote OS command execution.

Iranian hackers use CHOSEN BRICK Windows malware to spy on targets | Malware | Bleeping Computer

Government agencies warn that Iranian state-linked hackers deploy new Windows malware called CHOSEN BRICK to surveil dissidents, activists, and journalists globally.

Active Exploitation Attempts Target WSO2 API Manager JWT Bypass With Forged Admin Tokens | Vulnerability/Authentication Bypass | The Hacker News

Attackers are actively exploiting a critical WSO2 API Manager flaw that allows forged JWT tokens to bypass authentication and seize admin accounts.

Atomic macOS (AMOS) Stealer Activity | Malware | Palo Alto Networks Unit 42

Unit 42 details fake setup guides luring macOS users into installing the Atomic Stealer malware that harvests credentials and sensitive data.

One Extension Could Hijack AI Assistants Across Chrome, Comet, Edge, Opera Neon and Claude | Vulnerability | The Hacker News

Researchers found a malicious browser extension could hijack AI assistants embedded in Chrome, Edge, Comet, Opera Neon and Claude with one click.

Zero-Day Flaw in TP-Link Cameras Enables Eavesdropping | Zero-Day/Vulnerability | Infosecurity Magazine

Security researchers disclosed two unpatched vulnerabilities in TP-Link cameras that could allow attackers to spy on video feeds.