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 September 08, 2026
(Reported on Wednesday September 09, 2026)

Local Government

CISA tells operators to harden Siemens S7 PLCs. Here's how to do it without disrupting production | Vulnerability/Hardening Guidance | CSO Online

CISA and NSA issued a joint advisory urging operators to harden Siemens S7 industrial controllers, with practical guidance on avoiding production disruptions.

Financial Institutions

DoppelCart fraud network uses 119,000 fake shops to steal credit cards | Fraud/Phishing (Fake E-commerce Card Skimming) | Bleeping Computer

Researchers uncover a large-scale scheme running over 119,000 fraudulent online storefronts designed to harvest shoppers' payment card information.

Liquid Hackers Return 3,400 Bitcoin Taken via Elements Bug, Still Holding $47M in BTC | Vulnerability/Exploit | The Hacker News

Attacker who exploited a bug in Bitcoin sidechain Liquid Network returned most stolen funds, but roughly $47M in bitcoin remains unrecovered.

Russian national extradited to US for alleged involvement in bank-account takeover scheme | Account Takeover / Credential Theft | CyberScoop

Russian national extradited to the US faces charges for allegedly harvesting over 5,000 stolen bank login credentials in an account takeover scheme.

Healthcare

OneTouchPoint Agrees to Multi-Million Dollar Data Breach Settlement | Ransomware | HIPAA Journal

Printing and mailing vendor serving health plans reaches multi-million dollar settlement over 2022 ransomware breach exposing patient data.

NFI North Data Breach Affects Almost 50,000 Individuals | Data Breach | HIPAA Journal

Healthcare-related organization NFI North disclosed a data breach exposing personal information of nearly 50,000 individuals.

Other

Microsoft September 2026 Patch Tuesday fixes 966 flaws, 2 zero-days | Zero-Day | Bleeping Computer

Microsoft's September 2026 Patch Tuesday addresses nearly a thousand vulnerabilities, including two zero-days already under active exploitation.

ChatGPT Flaw Let a Planted Prompt Send a Victim's Gmail Data to Another Account | Prompt Injection | The Hacker News

Researchers demonstrated a ChatGPT prompt-injection flaw that secretly exfiltrated a connected Gmail account's data to an attacker-controlled account.

Hackers breach F5 BIG-IP APM devices to deploy Linux rootkit | Malware/Rootkit | Bleeping Computer

Attackers exploit F5 BIG-IP APM devices to install a stealthy Linux rootkit that injects a fileless web shell via PHP hooking.

Autonomous AI Agents Compromise Thousands of Credentials in Under Six Hours | Credential Theft / AI-Powered Attack Automation | The Hacker News

Google researchers report a financially motivated hacking group used a self-directed, multi-agent AI framework to harvest thousands of credentials within six hours.