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 Friday September 04, 2026, through Monday September 07, 2026 (Reported on Tuesday September 08, 2026)

Local Government

OpenAI, MS-ISAC Launch AI Cyber Defense Pilot | AI Cybersecurity | GovTech

OpenAI and MS-ISAC launched a pilot providing state and local governments and critical infrastructure organizations with AI-powered cyber defense tools, training, and hands-on support.

Financial

Ransomware Group Claims 50GB Stolen In Gale Credit Union Data Breach | Ransomware/Data Breach | CU Today

Gale Credit Union is notifying individuals after an Akira ransomware attack exposed sensitive personal and financial information, with the group claiming it stole approximately 50GB of data.

Healthcare

Luminis Health Working to Restore Systems After Cyberattack | Cyberattack/Operational Disruption | HIPAA Journal

Luminis Health is restoring systems after a cyberattack disrupted phones and MyChart across two Maryland hospitals while investigators assess whether patient data was compromised.

Resource Center of Dallas Notifies 12,500 Patients About Cyber Incident | Data Breach | HIPAA Journal

A Dallas healthcare nonprofit disclosed a cyber incident exposing personal and medical information of roughly 12,500 patients.

Other

Magento StyleSmuggler zero-day exploited to deploy Linux backdoor | Zero-Day | Bleeping Computer

Attackers exploit a new unpatched Magento/Adobe Commerce flaw dubbed StyleSmuggler to install a Linux backdoor on e-commerce servers.

New Ransomware Gang Claims Boeing and Airbus Supplier Breach | Ransomware | Cybernews

The Storm ransomware group claims it breached aerospace supplier Star Aviation and stole internal documents, with leaked samples reportedly including aircraft wiring schematics and employee identification cards.

Hackers exploit new MikroTik RouterOS flaws to hijack routers | Vulnerability Exploitation | Bleeping Computer

Attackers are chaining two newly disclosed MikroTik RouterOS vulnerabilities to compromise routers with internet-exposed SSH services.

Rogue ScreenConnect Clients Spread Four-Stage VBScript Chain to Newly Connected Hosts | Malware | The Hacker News

Researchers found attackers abusing compromised ScreenConnect RMM clients to self-propagate a multi-stage VBScript malware chain to newly connected endpoints.

New CrowdStrike 'FalconFlank' Zero-Day Grants SYSTEM Privileges | Zero-Day/Privilege Escalation | Bleeping Computer

A newly disclosed CrowdStrike Falcon zero-day can allow attackers to escalate privileges to SYSTEM on fully updated Windows devices by abusing the platform's Office macro-remediation feature.

JSCeal Malware Can Bypass Google Authentication Using Stolen Session Cookies | Malware | The Hacker News

Researchers detail JSCeal, a compiled JavaScript malware that steals credentials and session cookies to bypass Google authentication and intercept traffic.

Condé Nast Data of 32.8 Million Users Offered for Sale After WIRED Leak | Data Breach | Security Affairs

Hackers advertise a 32.8 million-record Condé Nast user database, reportedly stolen following a breach linked to WIRED, on a cybercrime forum for $15,000.

Attackers Exploit PaperCut Flaws to Steal Credentials From Schools and Universities | Vulnerability/Credential Theft | The Hacker News

Attackers are chaining two PaperCut vulnerabilities to execute commands, create privileged accounts, and steal credentials from schools and universities in the United States and Europe.