

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 29, 2026
(Reported on Wednesday September 30, 2026)

Local Government

Three Million Affected in Pentagon Personnel Agency Data Breach | Data Breach | [Security Affairs](#)

Hackers accessed a Pentagon personnel agency's file-sharing server for nine months, exposing personal data of three million people.

Healthcare

WPM Pathology Laboratory; Salina Regional Health Center Settle Class Action Litigation | Data Breach | [HIPAA Journal](#)

Pathology lab and Kansas health center reach class action settlement over a 2024 cyberattack that exposed patient data.

Other

Russia's Star Blizzard Targets 100+ Organizations With Fake Event Invites to Deliver Backdoor | Phishing/Social Engineering (Backdoor Malware) | [The Hacker News](#)

Microsoft reports Russian state-linked group Star Blizzard used fake event invitations to deploy Windows backdoors against over 100 Ukraine-linked organizations, mostly in the US and UK.

New Spectre v2 attack variant leaks Linux root password hash in minutes | Vulnerability (Spectre v2 side-channel/speculative execution) | [Bleeping Computer](#)

Researchers unveiled a new Spectre v2 side-channel technique that extracts Linux root password hashes from Intel CPUs within minutes.



Custom ChatGPTs push ClickFix attacks to deploy RAT malware | Social Engineering | [Bleeping Computer](#)

Malicious ads for fake custom ChatGPT tools lure users into ClickFix-style prompts that install remote-access trojan malware.

101 Malicious npm Packages Add Developers' WhatsApp Accounts to Groups Without Consent | Supply Chain | [The Hacker News](#)

Researchers found 101 malicious npm packages that exploit an open-source WhatsApp library to covertly enroll developers into subscriber groups.

Amazon Bedrock AgentCore Flaws Could Expose AWS Credentials | Vulnerability | [Infosecurity Magazine](#)

Researchers found flaws in AWS Bedrock AgentCore SDK that could let attackers execute code in AI sandboxes and steal AWS credentials.

Official MCP Python SDK Flaw Can Let Malicious Servers Steal OAuth Credentials | Vulnerability | [The Hacker News](#)

Security flaw in the official MCP Python SDK could let a rogue server intercept OAuth secrets, codes, and PKCE keys meant for a legitimate service, now patched.

