

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 Monday September 28, 2026
(Reported on Tuesday September 29, 2026)**

Local Government

U.S. CISA adds Citrix NetScaler flaws to its Known Exploited Vulnerabilities catalog | Zero-Day/Remote Code Execution | [Security Affairs](#)

CISA added two actively exploited Citrix NetScaler zero-days to its KEV catalog after confirming the flaws could allow unauthenticated remote code execution or denial of service.

FBI job portals remain offline after ShinyHunters claims breach via PeopleSoft zero-day | Data Breach/Zero-Day | [Help Net Security](#)

FBI recruiting portals remain offline while the agency investigates ShinyHunters' claim that an Oracle PeopleSoft vulnerability enabled access to sensitive employee and applicant information.

Healthcare

California Critical Access Hospital Announces Cybersecurity Incident | Data Breach | [HIPAA Journal](#)

California critical access hospital Modoc Medical Center disclosed a cybersecurity incident involving unauthorized access to patient data.

Nearly 400,000 Medicaid Beneficiaries Caught in Medicaid and DC Healthcare Alliance Data Exposure | Data Exposure | [Security Affairs](#)

The DC Department of Health Care Finance is notifying 399,086 beneficiaries after hidden personal information in publicly posted reports was potentially accessible without authorization.

Astrana Health Tells SEC Hack Exposed Sensitive Data | Social Engineering/Data Breach | [HealthcareInfoSecurity](#)

Astrana Health disclosed that attackers used employee impersonation and caller-ID spoofing to access company systems and potentially steal sensitive patient, employee, provider, and corporate information.



Other

JadePuffer agentic AI attacks target Azure, destroy cloud resources | Ransomware | [Bleeping Computer](#)

A ransomware group called JadePuffer uses AI-driven agents to automate reconnaissance, credential theft, and destruction of Azure cloud resources.

Apple Patches CoreGraphics Flaw Possibly Exploited in Targeted Attacks | Zero-Day | [The Hacker News](#)

Apple issued patches for a CoreGraphics out-of-bounds write flaw in older iOS, iPadOS, and macOS versions possibly exploited in targeted attacks.

Chrome Store Hosts 'Poper Blocker' Spyware Downloaded by Millions | Malware/Spyware | [Dark Reading](#)

A widely-installed Chrome extension disguised as an ad blocker was found secretly harvesting user data despite passing Google's store review.

Carbonato Botnet Compromises Docker Hosts to Deploy Telegram-Controlled Hermes AI Agent | Malware/Botnet | [The Hacker News](#)

New Carbonato botnet exploits exposed Docker daemons to install a hijacked open-source AI agent framework controlled remotely via Telegram.

Over 16,000 Supabase databases expose PII, passwords, auth tokens | Data Breach | [Bleeping Computer](#)

Security researchers identified over 16,000 misconfigured Supabase-backed databases publicly exposing PII, credentials, and authentication tokens.

NeedyMantis: Unpacking a post-compromise malware family used in targeted operations | Malware | [Microsoft Security Blog](#)

Microsoft researchers detail NeedyMantis, a modular post-compromise malware framework using custom loaders and encrypted archives to sustain long-term access in targeted intrusions.

