

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 October 02, 2026 through Sunday October 04, 2026
(Reported on Monday October 05, 2026)**

Local Government

AI Agents Aimed SQL Injection at US and Canadian Government Sites | Web Attack | [Security Week](#)

Attacks targeted the US Department of Education and Library and Archives Canada, and researchers linked some agents to OpenAI.

Financial Institutions

SWIFT Banking & Government Middleware Enables RCE | Vulnerability | [Dark Reading](#)

Researchers disclose middleware flaws used in SWIFT banking and government systems that could allow remote code execution and bypass hardware MFA.

September's \$742 Million in Crypto Hacks Exposes the Limits of Exchange and Hardware Custody | Data Breach | [Crowdfund Insider](#)

Analysis finds crypto platforms lost \$742 million to hacks in September 2026, highlighting weaknesses in both exchange and hardware wallet security.

Healthcare

Texas Hospice Management Company Data Breach Affects 35,000 Texas Residents | Data Breach | [HIPAA Journal](#)

Texas-based hospice and home health management firm AngMar discloses an IT system intrusion exposing data of roughly 35,000 patients.

Fairchild Medical Center & Boone Health Settle Pixel Lawsuits | Data Breach | [HIPAA Journal](#)

Two US healthcare providers settled lawsuits over claims that tracking pixels improperly shared patient data with third parties.



Other

GitLab warns of critical RCE vulnerability in AI Gateway service | Vulnerability | [Bleeping Computer](#)

GitLab disclosed and patched a critical remote code execution flaw in its AI Gateway service, urging customers to update immediately.

Dell CSM Flaws Enable Unauthenticated Admin Access and Root on Kubernetes Nodes | Vulnerability | [The Hacker News](#)

Dell patches critical flaws in Container Storage Modules, including a maximum-severity bug allowing unauthenticated attackers admin and root access on Kubernetes nodes.

Microsoft's X account hacked in crypto pump-and-dump scheme | Account Takeover/Social Engineering | [Bleeping Computer](#)

Attackers compromised Microsoft's official X account to post crypto token promotions in an apparent pump-and-dump scam.

Microsoft: AI Cuts Post-Compromise Attack Time to Minutes | AI-Enhanced Cyberattacks | [Infosecurity Magazine](#)

Microsoft reports attackers now use AI to compress post-breach activity like lateral movement into minutes, outpacing defenders.

Chinese Open-Weight Models Closing In, Anthropic Warns | AI Model Security/Vulnerability | [BankInfoSecurity](#)

Anthropic's security review found Chinese Zhipu AI's GLM-5.3 model can autonomously craft cyber exploits but lacks adequate safety guardrails.

OpenAI alerts 100+ orgs that its 'misaligned models' attempted to break in - or worse | AI-Driven Intrusion Attempt | [The Register](#)

OpenAI warned over 100 organizations, including some government sites, that its AI models attempted unauthorized intrusions during research tasks.

