

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 Wednesday September 30, 2026
(Reported on Thursday October 01, 2026)

Local Government

Russian state hackers use new RedFlick technique to push malware | Malware | [Bleeping Computer](#)

Russian state-linked group Star Blizzard adopts a new 'RedFlick' delivery method to install its CosmicPulse backdoor in espionage campaigns.

WaterISAC reckons with range of threats after summer of cyberattacks | Vulnerability | [CyberScoop](#)

Water sector ISAC outlines ongoing risks from exposed PLCs, third-party integrators, and internet-facing systems after a wave of utility cyberattacks.

Financial Institutions

US sanctions 10 over ATM malware scheme tied to Tren de Aragua | Malware (ATM Jackpotting) | [The Record](#)

Treasury sanctioned ten Venezuelan nationals and affiliated firms linked to Tren de Aragua for an ATM jackpotting malware scheme and laundering stolen cash.

Healthcare

H1 2026 Healthcare Data Breach Report | Data Breach | [HIPAA Journal](#)

Aggregate report shows US healthcare data breaches dropped nearly 6% in the first half of 2026 compared to the prior year.

The Mental Health Association Data Breach Settlement Agreed | Data Breach | [HIPAA Journal](#)

Massachusetts behavioral health nonprofit reaches settlement over a data breach that exposed clients' protected health information.



Other

DIVD says Zammad zero-days enabled AI-driven network breach | Zero-Day Exploitation | [Bleeping Computer](#)

Dutch vulnerability disclosure nonprofit DIVD confirms attackers chained two unpatched Zammad ticketing system flaws, aided by AI tools, to breach its network.

Attackers Exploit Zimbra Flaw to Deploy Web Shells and Harvest Authentication Secrets | Vulnerability Exploitation | [The Hacker News](#)

Hackers actively exploit an unauthenticated RCE flaw in Zimbra Collaboration Suite to install web shells and steal mailbox credentials.

OpenAI reveals ‘novel’ encryption bypass used in distillation attack | Vulnerability/Encryption Bypass | [CyberScoop](#)

OpenAI disclosed a novel technique bypassing its encryption that enabled unauthorized model distillation, allegedly tied to individuals linked to China's MoonshotAI.

16-year-old researcher found a Microsoft bug, got admin access to databases with 17.3 trillion rows | Vulnerability | [The Register](#)

Teenage security researcher discovered a Microsoft flaw granting admin-level access to massive internal databases containing trillions of rows of data.

Over 543,000 valid credentials exposed in public GitHub repositories | Data Breach | [Bleeping Computer](#)

Security researchers found over 543,000 still-valid credentials leaked in public GitHub repositories despite platform safeguards.

