

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 October 05, 2026
(Reported on Tuesday October 06, 2026)**

Local Government

Frontline Education Breach Impacts K-12 School District Staff | Data Breach | [Infosecurity Magazine](#)

A breach at K-12 software vendor Frontline Education exposed personal data belonging to school district employees nationwide.

Iranian hacker accused of draining 31TB from university inboxes extradited to the US | Data Breach | [Security Affairs](#)

Iranian national extradited from Montenegro to the US faces charges for allegedly stealing 31TB of data from university email accounts.

Financial Institutions

Alleged dev of Ploutus ATM malware appears in US court after arrest | Malware | [Bleeping Computer](#)

DOJ announces arrest and court appearance of a suspect accused of creating Ploutus malware used in ATM jackpotting thefts across the US.

Healthcare

250,000 Impacted by Data Breaches at New Jersey, Texas Healthcare Firms | Data Breach | [Security Week](#)

Two US healthcare companies disclosed breaches exposing roughly 250,000 patients' personal and medical data after July hacking incidents.



WindRose Health Network Discloses Data Breach Affecting 33K Individuals | Data Breach | [HIPAA Journal](#)

WindRose Health Network reported a data breach exposing personal and health information of roughly 33,000 patients.

Other

Microsoft Exchange Flaw Lets Authenticated Attackers Read Other Users' Mailboxes | Vulnerability | [The Hacker News](#)

Microsoft issued emergency patches for a high-severity Exchange Server flaw that could let authenticated users escalate privileges and access other mailboxes.

Linux Backdoor Abuses STUN Protocol, Exploits Dozens of Flaws | Malware | [Security Week](#)

Researchers detail a new Linux backdoor, ClingSTUN, that abuses the STUN protocol for proxy backdoor access and self-propagates via multiple exploited vulnerabilities.

Attackers Target Rejetto HFS Flaw That Enables Admin Session Forgery and RCE | Vulnerability | [The Hacker News](#)

Hackers actively exploit a critical flaw in Rejetto HFS software that allows forging admin sessions via a predictable PRNG to gain remote code execution.

Google Suspends Open-Source Bug Bounty Due to AI Vulnerability Reports | Vulnerability | [Infosecurity Magazine](#)

Google halted its open-source bug bounty program after being overwhelmed by low-quality, AI-generated vulnerability reports.

Apple Plans Tighter macOS Full Disk Access Controls Over AI Agent Data Access | Vulnerability/Access Control | [The Hacker News](#)

Apple is tightening macOS Full Disk Access permissions after finding AI agent apps exploited broad access to sensitive files, mail, and browsing history.

Wikimedia links OpenAI agents to an outage and unauthorized activity | Unauthorized Access/Automated Abuse | [Engadget](#)

Wikimedia reports that autonomous AI agents, including ones linked to OpenAI, triggered a service outage and unauthorized activity on its platform.

