

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 September 25, 2026 through Sunday September 27, 2026
(Reported on Monday September 28, 2026)**

Local Government

CISA and FBI Warn OT Operators About Third-Party Hacking | Supply Chain | [BankInfoSecurity](#)

CISA and FBI alert operational technology operators that foreign hackers are exploiting third-party integrator remote access to compromise critical infrastructure systems.

Microsoft SharePoint Flaw CVE-2026-65660 Now Exploited in Attacks | Vulnerability/Zero-Day | [Security Week](#)

CISA confirms active exploitation of a Microsoft SharePoint vulnerability, mandating federal agencies patch by September 28.

OpenAI agents accessed Census, SEC data and tried to hack Education website | Unauthorized Access/AI-driven Intrusion Attempt | [NextGov](#)

OpenAI disclosed that its AI agents accessed Census Bureau and SEC data and attempted unauthorized access to a US Education Department website.

Financial Institutions

CISA issues urgent alert about vulnerabilities in remote access technology used by businesses | Vulnerability | [ABA Banking Journal](#)

CISA warns of active exploitation of critical flaws in Citrix NetScaler ADC and Gateway, urging banks to patch remote access systems immediately.

Bitget Says Suspected North Korean Hackers Stole \$351.6M After Backend Compromise | Data Breach / Theft | [The Hacker News](#)

Crypto exchange Bitget disclosed a \$351.6 million theft from hot and warm wallets by suspected North Korean-linked hackers after a backend compromise.



Healthcare

Threat groups ramp up social-engineering attacks against healthcare sector | Social Engineering | [Cybersecurity Dive](#)

Cybercriminal groups are using voice-phishing calls to trick healthcare employees into revealing login credentials, enabling network access.

Labcorp Settles Multistate Data Breach Investigation for \$2.3 Million | Data Breach | [HIPAA Journal](#)

Labcorp will pay \$2.3 million to settle a 44-state probe into the AMCA data breach that exposed patient billing information.

Other

GitHub Actions re-enabled with Mini Shai-Hulud payload still active | Supply Chain | [Bleeping Computer](#)

Maintainer re-enabled two compromised GitHub Actions still linked to Mini Shai-Hulud malware, leaving malicious code live for over a week.

U.S. Soldier Gets 70 Months in Prison for AT&T, Verizon Extortions | Data Breach/Extortion | [Krebs on Security](#)

A U.S. Army soldier was sentenced to nearly six years in prison for hacking telecom carriers and extorting AT&T and Verizon using stolen customer call/text metadata.

Kiteworks urges 6-hour server shutdown over potential zero-day attacks | Zero-Day/Vulnerability | [Bleeping Computer](#)

Secure file-sharing vendor Kiteworks told global customers to power down servers for six hours amid credible threat intel on an imminent zero-day exploit.

Storm-3168: Agentic-driven cloud attacks using compromised service principals | Cloud Account Compromise / Credential Access | [Microsoft Security Blog](#)

Microsoft reports Storm-3168 threat actor using compromised Azure service principals for cloud reconnaissance, resource deletion, and credential theft.

