

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 09, 2026 through Sunday October 11, 2026
(Reported on Monday October 12, 2026)**

Local Government

FBI Arrests Executive at Ransomware Negotiation Firm | Data Breach | [Krebs on Security](#)

FBI arrests a ransomware-negotiation firm co-founder tied to the ShinyHunters group's theft of sensitive FBI agent data.

UK and Allies Warn of Cyber Threat from China's Integrity Technology Group | Cyber Espionage | [Infosecurity Magazine](#)

UK, US and allied cyber agencies issued a joint advisory exposing a China-linked contractor's hacking operations against government and critical infrastructure networks.

White House Says All AI Companies Must Report Security Incidents | Data Breach | [PYMNTS](#)

White House orders AI companies to disclose and remediate security incidents following reported breaches at Anthropic.

Healthcare

Hundreds of thousands impacted by data breach at biosensor firm iRhythm | Data Breach | [The Record](#)

Wearable cardiac monitor maker iRhythm disclosed a summer data breach affecting hundreds of thousands of patients, now reported to state regulators.

Valley Oaks Health Data Breach Settlement Gets First Nod from Court | Data Breach | [HIPAA Journal](#)

Court granted preliminary approval of a class action settlement over a 2023 Valley Oaks Health data breach affecting over 50,000 patients.



Other

Citrix warns admins to patch new NetScaler RCE flaw immediately | Vulnerability | [Bleeping Computer](#)

Citrix issued an urgent advisory urging immediate patching of a critical remote code execution flaw in NetScaler ADC and Gateway appliances.

Researchers Publish Working Exploit for Pre-Auth AnyDesk Linux Flaw That Gives Root Access | Vulnerability | [The Hacker News](#)

Researchers released a working pre-authentication exploit for an AnyDesk Linux flaw that grants root access without connection approval.

Q3 2026 Sets New Record for Ransomware Attacks | Ransomware | [Infosecurity Magazine](#)

Research firm reports ransomware attacks hit a quarterly record, with sharp increases targeting finance, tech, education and healthcare organizations.

Silent Ransom Group Allegedly Extorted \$207 Million Without Encrypting Files | Social Engineering | [Security Affairs](#)

Threat group used phone-based social engineering rather than encryption to extort roughly \$207 million from dozens of law firms.

AI systems are fully capable of carrying out nightmare attacks against infrastructure and nobody's ready | AI-Enabled OT/ICS Attack | [The Register](#)

Researchers demonstrate AI agents can manipulate industrial control systems, spoofing operator screens and controlling robotic arms in critical infrastructure.

U.S. CISA adds ProFTPD, ONLYOFFICE Docs, Strapi, Apache Struts, and ISC BIND flaws to its Known Exploited Vulnerabilities catalog | Vulnerability | [Security Affairs](#)

CISA added actively exploited flaws in ProFTPD, ONLYOFFICE Docs, Strapi, Apache Struts, and ISC BIND to its Known Exploited Vulnerabilities catalog, urging urgent patching.

