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 August 07, 2026 through Sunday August 09, 2026 (Reported on Monday August 10, 2026)

Local Government

New 'Water Watch Center' launched to help small utilities stop cyberattacks | Vulnerability/Intrusion | NextGov

New national coordination center aims to help small water utilities detect and respond to intrusions, amid suspected Iran-linked attacks on multiple state water systems.

Progress Kemp LoadMaster Flaw Hits CISA KEV After 792 Reported Exploit Attempts | Vulnerability | The Hacker News

CISA added a critical Progress Kemp LoadMaster command injection flaw to its exploited vulnerabilities list after hundreds of attack attempts were observed.

Financial Institutions

Sawyer Savings Bank of New York keeps branches closed amid possible data security incident | Vulnerability | DysruptionHub

A New York community bank closed branches after a third-party vendor vulnerability triggered a suspected data security incident, though online banking stayed operational.

Ransomware Surges in July After Q2 Lull | Ransomware | Infosecurity Magazine

Ransomware attacks spiked in July after a Q2 slowdown, with financial services, technology, and healthcare organizations among the top targets.

Healthcare

Experts say healthcare faces cybersecurity crisis: 'These are patient safety issues' | Vulnerability | Cybersecurity Dive

Security researchers warn that weak regulation, underfunding, and hospital-system consolidation are leaving US healthcare providers highly exposed to cyberattacks that threaten patient safety.

Other

Levi Strauss & Co. says hackers stole corporate data in cyberattack | Social Engineering | Bleeping Computer

Levi Strauss confirms attackers used social engineering to compromise three employees and steal internal corporate data.

New CSS Attacks Can Break Webmail Defenses to Steal Passwords and Tokens | Vulnerability | The Hacker News

New CSS-based attack techniques let malicious emails break out of message boundaries to steal credentials and tokens across major webmail providers.

Critical One-Click Vulnerability in Atlassian's Rovo AI Exposed Enterprise Data | Vulnerability | Security Week

Researchers found a one-click flaw in Atlassian's Rovo AI, dubbed RovoBlast, that could let attackers exfiltrate Confluence, Jira, and SharePoint data.

Metabase Zero-Day Exploited in Wild Allows Admin Access Without Authentication | Zero-Day/Vulnerability (SQL Injection) | The Hacker News

Attackers actively exploit a maximum-severity, unauthenticated SQL injection flaw in Metabase to gain admin access to BI platform databases.