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 August 19, 2026
(Reported on Thursday August 20, 2026)

Local Government

Hackers Actively Target Siemens PLCs With AI Cyberattacks | Operational Technology / AI-Enabled Cyberattack | GovInfoSecurity

Hackers are increasingly using AI-assisted techniques to target exposed Siemens programmable logic controllers, highlighting growing risks to operational technology and critical infrastructure as attackers automate reconnaissance and exploitation.

Financial Institutions

How Republic Bank Is Preparing Database Change for AI | AI / Data Infrastructure | BankInfoSecurity

Republic Bank is modernizing its database environment to support AI initiatives while emphasizing data governance, security and controlled access as financial institutions prepare existing infrastructure for AI-driven workloads.

Healthcare

Critical Infrastructure Entities Warned About Medusa Ransomware as Victim Count Hits 300 | Ransomware | HIPAA Journal

CISA, the FBI and MS-ISAC warned critical infrastructure organizations about Medusa ransomware after the operation surpassed 300 victims, including healthcare organizations, and urged organizations to patch known vulnerabilities, segment networks and strengthen authentication.

Other

Comcast turns your Xfinity WiFi into a home motion detector | Privacy / WiFi Security | BleepingComputer

Comcast's Xfinity WiFi Motion feature detects changes in wireless signals to identify movement without cameras, while its data-handling language raises questions about what motion information could be disclosed in legal proceedings.

16 Typosquatted RubyGems Packages Steal Browser Credentials and Crypto Wallets | Software Supply Chain / Information Stealer | The Hacker News

Researchers uncovered 16 malicious RubyGems packages impersonating legitimate software and deploying a Windows information stealer designed to harvest browser credentials and cryptocurrency wallet data.

TWINLOOT Abuses SharePoint and Teams to Steal Credentials and Move Across Networks | Malware / Microsoft 365 Abuse | The Hacker News

The newly identified TWINLOOT implant uses SharePoint, Teams, Microsoft Graph, and a victim's Edge browser for covert command-and-control while supporting credential theft, arbitrary command execution, and lateral movement.

AI "Mind Viruses" Can Spread Between Agents Through Persistent Prompt Files | AI Security / Prompt Injection | The Hacker News

Researchers demonstrated self-propagating prompt payloads that can spread between autonomous AI agents through persistent system-prompt files, while simple defensive instructions substantially reduced propagation in testing.

Ransom Busters Claims It Hacked Ransomware Servers, Asks Victims for Up to $60,000 | Ransomware / Extortion | The Hacker News

A ransomware affiliate using the name Ransom Busters is contacting victims with claims that it breached ransomware-group infrastructure and can delete stolen data in exchange for payments of $20,000 to $60,000.

Attackers Exploit MLflow SSRF Flaw to Steal Cloud Credentials and Secrets | Vulnerability / Cloud Credential Theft | The Hacker News

Attackers are actively exploiting critical MLflow vulnerability CVE-2026-64849 to reach internal cloud metadata services and steal credentials and secrets from exposed systems.

Microsoft Copilot Personal Flaws Could Let One Click Exfiltrate Data From Connected Apps | AI Security / Data Exfiltration | The Hacker News

Three patched Microsoft Copilot Personal vulnerabilities, collectively called CoSnitch, could allow a crafted link to silently extract data from connected applications and persist attacker instructions in Copilot memory.
