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 August 31, 2026
(Reported on Tuesday September 01, 2026)

Local Government

State-linked actor targets Cisco routers for espionage | Espionage/Network Intrusion | Cybersecurity Dive

China-linked espionage group Fire Ant used custom tooling to stealthily compromise Cisco routers in trusted network environments for long-term access.

Iran Cyber Risk Climbs as US Resumes Strikes | Reconnaissance/Probing (ICS/OT) | BankInfoSecurity

Analysts warn that renewed US-Iran military strikes historically precede fresh Iranian probing of US water and energy control systems.

DoJ Corrects China Hacking Claim, Says U.S. Agencies Were Targets, Not Victims | Cyber Espionage | The Hacker News

DoJ revised its earlier statement, clarifying that NASA, the Federal Reserve, DOE, and DOJ were targeted—not breached—by Chinese state-linked hackers.

Financial Institutions

Five plead guilty in latest federal ATM jackpotting case | Malware | The Record

Five Venezuelan nationals pleaded guilty in a federal ATM jackpotting scheme using malware to force cash dispensing.

Healthcare

Healthcare cyberattacks hit pacemakers and millions of patient records | Data Breach | The Register

McKesson confirmed a data breach as extortion group ShinyHunters demanded $55.2 million, part of a wider wave of healthcare-sector cyberattacks affecting patient records and connected medical devices.

Other

Aurora Ransomware Operators Use Cursor AI in Attacks Against 10 Targets | Ransomware | The Hacker News

Researchers found Aurora ransomware affiliates leveraging the Cursor AI coding assistant to develop intrusion tools across ten targeted organizations.

Spring Ring: An Inside Look at Voice Phishing Campaigns in Microsoft Teams | Social Engineering | Palo Alto Networks Unit 42

Researchers detail a vishing campaign called Spring Ring that abuses Microsoft Teams calls to trick employees into installing malware targeting corporate domain controllers.

Cronos blockchain restarts after $74 million Tectonic exploit | Price Manipulation/Exploit | Bleeping Computer

Attacker exploited a price-manipulation flaw in Tectonic's lending protocol to borrow $74 million, prompting Cronos blockchain to halt and restart.

Microsoft warns of TerminalFix attacks deploying reverse tunnels | Social Engineering | Bleeping Computer

Microsoft details a new ClickFix variant using fake Cloudflare CAPTCHAs to trick users into running PowerShell commands that install reverse tunnels.
