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 28, 2026 through Sunday August 30, 2026 (Reported on Monday August 31, 2026)

Local Government

US government snitch-finder pleads guilty to leaking state secrets to foreign spies | Espionage/Insider Threat | The Register

A DIA insider-threat analyst pleaded guilty to passing classified US secrets to a foreign intelligence service shortly after his assignment began.

ownCloud Flaw Exploited to Steal Nuclear Records From Philippine Research Body | Vulnerability | The Hacker News

CISA added an actively exploited ownCloud flaw to its KEV catalog after Chinese-speaking hackers used it to steal data from a Philippine nuclear research agency.

Financial Institutions

Treasury Launches Quantum Task Force for Financial Sector | Cryptography | Bank Info Security

Treasury department announced a task force designed to push banks onto quantum resistant encryption.

Healthcare

McKesson discloses breach after ShinyHunters claims patient data theft | Data Breach | Bleeping Computer

McKesson confirmed a breach after ShinyHunters extortion group claimed theft of 284 million patient records via compromised third-party applications.

American Vision Partners Settles Data Breach Litigation for $1.75M | Data Breach | HIPAA Journal

Eye-care provider American Vision Partners agreed to pay $1.75M to settle lawsuits over a patient data breach affecting its network.

Other

Chrome Web Store extensions caught stealing crypto, browser data | Malware/Supply Chain | Bleeping Computer

Researchers found multiple Chrome and Edge extensions distributing a malware framework that steals cryptocurrency, browser data, and injects ClickFix-style social-engineering lures.

Cosmos EVM Flaw Exploited After Cosmos Labs Knew Every Blockchain Running It Was Vulnerable | Vulnerability | The Hacker News

A critical flaw in the shared Cosmos EVM module was actively exploited to drain funds from six blockchains despite prior vendor knowledge of the risk.

GiveWP WordPress donation plugin flaw lets hackers execute server commands | Vulnerability | Bleeping Computer

A critical unauthenticated remote code execution flaw in the widely-used GiveWP WordPress donation plugin could let attackers run arbitrary server commands.

China-Made ZBT Routers Ship With Two Implants Giving Unauthenticated Attackers Root Access | Supply Chain | The Hacker News

Researchers found two hidden backdoors baked into ZBT router firmware that let remote attackers gain unauthenticated root access.