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 September 02, 2026
(Reported on Thursday September 03, 2026)

Local Government

How China industrialized the infrastructure behind state hacking | State-Sponsored Hacking Infrastructure | CSO Online

DOJ and FBI seized domains tied to QScan and QTRouter, hacking tools built by a PRC state-sponsored group to target US critical infrastructure networks.

GeoNetwork Fixes Unauthenticated RCE Chain Affecting Government Geoportal Backends | Vulnerability/RCE Chain | The Hacker News

Researchers disclosed a chained pair of flaws in GeoNetwork, open-source metadata software used by many government geoportals, enabling unauthenticated remote code execution.

Senator asks NSA to update Americans about VPN spying risks | Traffic Analysis/Deanonymization | NextGov

A US senator pressed the NSA to inform Americans after a congressional review found foreign actors could deanonymize VPN users via traffic correlation analysis.

Financial Institutions

Core Banking Provider Jack Henry Confirms Limited Cyber Incident After Voice Phishing Campaign | Social Engineering | Crowdfund Insider

Jack Henry contained a ShinyHunters voice-phishing intrusion to a restricted non-production environment, though personally identifiable information tied to fewer than 10 client institutions was affected.

Healthcare

Baylor Genetics: ePHI of 2.8M Patients Exposed in Cybersecurity Incident | Data Breach | HIPAA Journal

Baylor Genetics confirms a cybersecurity incident exposed electronic protected health information of approximately 2.8 million patients.

Cyber incident disrupts Luminis Health systems in Maryland | Data Breach | DysruptionHub

Maryland-based Luminis Health hospital system suffers cyberattack, disabling online patient portals and prompting probe into possible patient data exposure.

Other

BGP Hijack Delivers Malicious Virtualizor Update That Establishes Persistent Root Access | Supply Chain | The Hacker News

Attackers hijacked BGP routes to intercept Softaculous update traffic, pushing a trojanized Virtualizor package that granted persistent root access on affected hypervisors.

Hackers Chain Two New SonicWall Zero-Day Vulnerabilities | Zero-Day/Vulnerability Chaining | Infosecurity Magazine

SonicWall warns attackers are chaining two newly discovered zero-day flaws in its products to compromise networks, urging immediate patching.

Hackers exploit Sangoma Switchvox flaw to deploy reverse shells | Vulnerability (SQL Injection to RCE) | Bleeping Computer

Attackers actively exploit an unauthenticated SQL injection flaw in Sangoma Switchvox VoIP systems to gain remote code execution and install reverse shells.

WordPress backup plugin flaw exposes millions of sites to takeover attacks | Vulnerability | Bleeping Computer

Unauthenticated SQL injection flaw in a popular WordPress backup plugin could let attackers remotely execute code and hijack millions of sites.