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 Thursday September 03, 2026
(Reported on Friday September 04, 2026)

Local Government

US and Canadian court data exposed in Thomson Reuters breach | Data Breach | The Record

A breach of a Thomson Reuters legal records platform exposed sealed court filings and personal data linked to courts in over a dozen US states and Canada.

Government, industry partner to shut down long-running Sality botnet | Malware/Botnet Takedown | Cybersecurity Dive

US law enforcement and CrowdStrike coordinated a takedown of the long-running Sality malware botnet, with victim notification now underway.

Financial Institutions

'Breeze Comet' Tears Into Brazilian & Global Financial Systems | Malware/Financial Fraud | Dark Reading

Sophisticated Brazilian threat group 'Breeze Comet' is compromising financial institutions in Brazil and abroad to siphon funds directly into its own accounts.

Healthcare

Five Healthcare Providers Report Ransomware-Related Data Breaches | Ransomware | HIPAA Journal

Five US healthcare organizations across multiple states disclosed patient data breaches stemming from separate ransomware attacks.

Multi-Million Settlement Resolves Managed Care of North America Data Breach Litigation | Data Breach | HIPAA Journal

Dental benefits manager MCNA reaches multi-million dollar settlement over a 2023 breach that exposed patients' personal and health data.

Other

Shai-Hulud's Reach Just Grew to 469 Credential Locations. Here's What That Means | Supply Chain | The Hacker News

Researchers found a Shai-Hulud npm supply-chain worm variant now scans 469 credential locations, including CI/CD, cloud, and AI tool configs.

Decade-old PostgreSQL flaw turns backup account into a backdoor | Vulnerability | CSO Online

Researchers uncover decade-old PostgreSQL flaw letting low-privilege replication accounts execute arbitrary code for full server takeover.

Chaotic Eclipse Releases Crowdstrike Falcon ZeroDay FalconFlank | Zero-Day/Privilege Escalation | Security Affairs

Researcher publicly released FalconFlank, a proof-of-concept exploit for an unpatched privilege-escalation flaw in CrowdStrike Falcon's endpoint agent.

Counterfeit installers turn routine software downloads into enterprise breaches | Malware/Supply Chain (Trojanized Installers) | CSO Online

Microsoft warns fake download sites for Edge, Kaspersky, and Razer are distributing trojanized installers to gain persistent enterprise access.