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 09, 2026
(Reported on Thursday September 10, 2026)

Local Government

ShinyHunters claims Florida DMV breach, puts data on the clock | Data Breach | CSO Online

Extortion group ShinyHunters claims to have stolen over 200,000 driver records from Florida's DMV database, including Jeffrey Epstein's data.

Watchdog Finds Critical Access Control Gaps at CBP | Vulnerability/Access Control Weakness | BankInfoSecurity

DHS Inspector General report reveals CBP left a privileged service account exposed to its entire 76,000-user network, creating over 100 potential attack paths.

Financial Institutions

Hilltop National Bank closes Wyoming branches after cybersecurity incident | Cybersecurity Incident / Network Disruption | DysruptionHub

Wyoming-based Hilltop National Bank shut down branches and IT systems after a cyber incident, limiting customers to $1,000 daily card and ATM withdrawals.

Alby Hub Critical Flaw Could Let Attackers Take Over Internet-Exposed Bitcoin Wallets | Vulnerability | The Hacker News

A critical vulnerability in Alby Hub's self-hosted Bitcoin Lightning wallet could allow remote attackers to hijack and drain internet-exposed wallets.

Healthcare

Electronic health record company says customer data stolen in breach | Data Breach | The Record

Electronic health record vendor Veradigm confirmed attackers accessed a specific interface and stole customer data, though core systems were unaffected.

Other

US says Chinese firms extracted billions of tokens from frontier AI models | Data Exfiltration/Model Distillation | Bleeping Computer

US intelligence agencies report six Chinese AI firms systematically siphoned billions of tokens from American frontier AI models to train competing systems.

Four Spy Groups Used the Same Chrome and Windows Exploit Kit Within a Week | Zero-Day/Exploit Kit | The Hacker News

Researchers found four separate state-linked espionage groups, including China's APT31, using a newly identified exploit kit chaining Chrome and Windows flaws.

New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access | Zero-Day/Privilege Escalation | Bleeping Computer

Researcher publicly disclosed a Microsoft Defender zero-day, dubbed ShieldCrash, that can escalate privileges to SYSTEM access on Windows machines.

Infostealer Logs Expose Replayable AI Tokens That Can Bypass MFA | Credential Theft/Session Hijacking | The Hacker News

Researchers found infostealer malware logs containing reusable AI service session tokens that let attackers bypass MFA and hijack accounts on platforms like Google and Anthropic.

AI Is Giving Lesser-Resourced Attackers Nation-State-Level Reach, Google Warns | AI-Enabled Attacks | Security Week

Google's threat intelligence group reports that criminal and state-backed hackers are using AI tools to scale attacks once reserved for well-funded nation-state actors.