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 September 14, 2026
(Reported on Tuesday September 15, 2026)

Local Government

Massachusetts Governor Calls for Federal AI Guardrails | AI Governance | GovTech

Massachusetts Gov. Maura Healey called for clear federal AI rules and independent oversight to balance continued innovation with protections for people, the economy, and national security.

Financial Institutions

Personal, Financial Info Exposed in Revolut Data Breach | Data Breach | Security Week

Fintech firm Revolut mistakenly shared customers' personal and financial data with an attacker posing as a government authority.

Bitcoin (BTC) Lightning Network Security Vulnerability Could Have Impacted Apps, But Critical LDK Bug Now Fixed | Vulnerability | Crowdfund Insider

Lightning Development Kit patched two flaws letting a malicious channel partner steal funds during splicing operations on Bitcoin's Lightning Network.

Healthcare

Hacking Incident Affects 46,000 Hawaii Family Dental Patients | Data Breach | HIPAA Journal

Hawaii Family Dental disclosed a hacking incident that compromised personal health information of about 46,000 patients.

Other

Hackers hijack HBO Max Reddit account to push malware in ClickFix ads | Social Engineering | Bleeping Computer

Attackers took over HBO Max's Reddit account to post malicious ads using ClickFix tactics that infected Windows and macOS users with info-stealing malware.

New DDRop Attack Breaks Intel TDX and AMD SEV-SNP Confidential Computing | Vulnerability (Hardware Attack) | The Hacker News

Researchers reveal DDRop, a physical hardware exploit that defeats Intel TDX and AMD SEV-SNP confidential computing memory protections via write suppression.

Hackers target exposed Vite dev servers to steal AWS, Azure secrets | Vulnerability/Scanning Campaign | Bleeping Computer

Attackers are mass-scanning internet-exposed Vite development servers to harvest AWS and Azure credentials and configuration data.

Weekly Recap: Rogue AI Agents, WeChat Worm, PaperCut Attacks, AI Espionage, and Rootkits | Vulnerability | The Hacker News

Weekly roundup covers AI-assisted cyberattacks, a WeChat-spreading worm, PaperCut exploitation, AI-driven espionage, and new rootkit activity.

Malicious Twitch Extension Exposes 31,000 Users' OAuth Tokens | Supply Chain | Infosecurity Magazine

A malicious Twitch browser extension secretly exfiltrated OAuth tokens from roughly 31,000 users to a Russian bot network service.

New hardware device can RAM into encrypted memory, expose your data | Vulnerability | The Register

Researchers demonstrate a physical hardware device that can bypass DDR5 memory encryption to extract sensitive server data.