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 September 18, 2026 through Sunday September 20, 2026 (Reported on Monday September 21, 2026)

Local Government

CISA Flags Three Linux Kernel Vulnerabilities Exploited in the Wild | Vulnerability/Active Exploitation | The Hacker News

CISA added three actively exploited Linux kernel vulnerabilities to its Known Exploited Vulnerabilities catalog that could enable memory disclosure, denial of service, privilege escalation, or data-integrity impacts.

Financial Institutions

YouLend US network disruption in Georgia exposes sensitive data | Data Breach | DysruptionHub

Fintech lender YouLend suffered a US network disruption in Georgia that exposed sensitive data, with scope of impacted services still undisclosed.

Healthcare

McKesson Cyberattack: Stolen Data Includes 6.4 Million Unique Email Addresses | Data Breach | HIPAA Journal

McKesson data breach investigation reveals 6.4 million unique email addresses were exposed among stolen records.

Ambry Genetics Pays $700,000 Penalty to Settle HIPAA Violations | Data Breach | HIPAA Journal

Genetic testing firm Ambry Genetics paid $700,000 to settle HHS OCR findings tied to a data breach exposing patient health information.

Other

Cisco Zero-Day Highlights API Endpoint Authentication Issues | Zero-Day/Authentication Bypass | Dark Reading

A maximum-severity authentication bypass zero-day in Cisco's Identity Services Engine exposes API endpoints to unauthorized access risk.

Gyazo server flaw exploited to steal 23.6 million user records | Data Breach | Bleeping Computer

Image-hosting service Gyazo confirmed attackers exploited a server vulnerability to steal 23.6 million user account records.

CrowdSec Says TanStack npm Attack Led to Copy of 170 Private GitHub Repositories | Supply Chain / Data Breach | The Hacker News

CrowdSec disclosed that attackers exploited a former employee's still-active credentials, compromised via the TanStack npm supply-chain attack, to exfiltrate roughly 170 private GitHub repositories.

GhostCode attackers abuse device codes to take over Microsoft 365 accounts | Phishing/Social Engineering | CSO Online

New GhostCode phishing kit tricks Microsoft 365 users via OAuth device-authorization flow abuse, letting attackers hijack accounts without stealing passwords.

North Korea's fake job interviews infected 30,000 devices | Social Engineering | The Register

North Korea-linked group WaterPlum used fake job interview coding tests to plant backdoors on 30,000 devices and steal from over 7,000 crypto wallets.

Researchers use AI to find widespread software decoder flaw | Vulnerability | CyberScoop

AI-assisted research uncovered a widespread HEIF/HEIC image decoder flaw enabling remote code execution, impacting systems at Meta and OpenAI before being patched.