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 November 09, 2026
(Reported on Tuesday November 10, 2026)

Local Government

CISA updates cyber reporting form as broader incident mandate awaits approval | Regulatory Guidance | NextGov

CISA revised its voluntary cyber incident reporting form to collect more detailed attack data ahead of final CIRCIA mandatory reporting rules.

Financial Institutions

Financially motivated threat cluster uses AI-enabled tools against banking sector | Malware/AI-enabled automated attack tools | Cybersecurity Dive

A financially motivated hacking group is reportedly using AI-enhanced penetration-testing tools like Artex to automate attacks on banks.

LNbits Urges All Operators to Shut Down Their Bitcoin Lightning Wallet Servers Amid Attacks | Vulnerability/Exploit | The Hacker News

Open-source Bitcoin Lightning wallet platform LNbits told all operators to shut down servers after attackers exploited a flaw to drain funds from at least one deployment.

Healthcare

13.3 million people's medical data exposed; companies pay $300,000 | Data Breach | Malwarebytes Labs

Medical transcription vendor and affiliates settle with New York AG for $300,000 after a 2023 breach exposed health data of 13.3 million people.

Data breach at hearing aid giant Amplifon impacts thousands | Data Breach | The Record

Amplifon's US division notified thousands of customers that a breach exposed personal and medical information earlier this year.

States, IT Services Firms Reach $10M Settlement in Data Hack | Data Breach | BankInfoSecurity

Healthcare IT vendor Perry Johnson & Associates settles with four states for $10M over a 2023 breach exposing 13.3 million patients' data.

Healthcare Providers Discover Unauthorized PHI Disclosures to AI Tools | Data Breach | HIPAA Journal

Healthcare organizations found employees had uploaded patient health information to AI tools without authorization, risking HIPAA violations.

Other

N-able takes cloud platform offline after 30+ "zero-days" published | Vulnerability/Zero-Day | Bleeping Computer

N-able shut down its N-central RMM cloud platform and urged on-prem customers to halt servers after 30+ unpatched vulnerabilities were publicly disclosed.

Default 'admin:admin' Server Password Helps Researchers Hack Two Automakers, Unlock and Start Cars | Vulnerability | The Hacker News

Researchers found default admin:admin credentials on ForgeRock identity servers used by two car brands' apps, enabling account takeover and remote unlock/start of vehicles.

Hackers exploit SSHole OpenSSH flaw to breach Linux systems | Vulnerability | Bleeping Computer

Attackers are actively exploiting a newly disclosed OpenSSH vulnerability, dubbed SSHole, to run commands, steal credentials, and maintain persistent access on Linux hosts.

New Supply Chain Attack Compromises Tens of Thousands of GitHub Repositories | Supply Chain | Infosecurity Magazine

Malicious GitHub Actions workflow infected tens of thousands of repositories, including some owned by Uber, in a widespread supply chain attack.