

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 24, 2026
(Reported on Friday September 25, 2026)**

Local Government

CISA Election Security Plan Flags Patching Barriers, Voter Database Attacks | Election Security | [SecurityWeek](#)

CISA's 2026 election security plan warns that certification requirements can delay critical software patches while voter registration databases and interconnected government networks remain targets for cyberattacks.

CISA Promises OT Recovery Guidance Through CI-Fortify | Vulnerability | [BankInfoSecurity](#)

CISA and Five Eyes partners plan to release guidance urging OT operators to test end-to-end cyberattack recovery plans under the CI-Fortify initiative.

Digital forensics firm with US federal contracts covered up ties to Russia, DOJ alleges | Supply Chain | [The Record](#)

DOJ charges two executives for concealing that forensic data-extraction software sold to US federal agencies was developed in Russia.

Financial Institutions

Brooklyn Court Sentences Crypto Impersonator Who Drained Nearly 100 Coinbase Accounts | Social Engineering | [Crowdfund Insider](#)

Man sentenced to 4-12 years for a social engineering scheme that impersonated Coinbase support to steal \$16 million from nearly 100 customer accounts.



Healthcare

Oculus Pathology Notifies 20,000 Patients About April 2026 Security Incident | Data Breach | [HIPAA Journal](#)

Texas-based Oculus Pathology reported a security incident exposing personal and health data of over 20,000 patients.

AI scanning tools found security gaps at rail operator and hospitals, Wiz says | Vulnerability/Exposed Systems | [NextGov](#)

Security researchers using AI-driven scanning uncovered exposed access to a rail administration system and a hospital alert channel with sensitive data.

Other

Attackers Exploit WordPress CVE-2026-87902 Within Hours of Disclosure | Vulnerability/Zero-Day Exploitation | [The Hacker News](#)

Attackers began exploiting a critical WordPress local file inclusion flaw enabling unauthenticated remote code execution within hours of its public disclosure.

Crook used three open source agents to break into a Fortune 500 hospitality company, a major US airline and 25+ other orgs | Unauthorized Access/Intrusion via Open Source Agentic Tools | [The Register](#)

A lone attacker leveraged cheap open-source AI agents to breach a Fortune 500 hotel chain, a major US airline, and 25+ other organizations.

Hackers now exploit critical Roundcube flaw in code injection attacks | Vulnerability | [Bleeping Computer](#)

A previously patched high-severity Roundcube Webmail vulnerability is now being actively exploited in code injection attacks, per Canadian cyber authorities.

There's a new way to break RSA that's faster than anything we've seen before | Cryptographic Vulnerability | [Ars Technica](#)

Researchers developed a faster method for forging RSA signatures without factoring the private key, significantly reducing the estimated security of certain blind-signature implementations while posing limited risk to widely used RSA configurations.

