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 April 2, 2026
(Reported on Friday April 3, 2026)

Government

Breach Roundup: Feds Confirm 'Major' Hack of FBI System
Read more at BankInfoSecurity

Financial Institutions

Cryptohack Roundup: Charges in Uranium Finance Case
Read more at BankInfoSecurity

Healthcare

Stryker Fully Operational After March Cyberattack
Read more at HIPAAJournal

Other

Cisco Patches 9.8 CVSS IMC and SSM Flaws Allowing Remote System Compromise
Read more at TheHackerNews

Artificial Intelligence Critical Vulnerability in Claude Code Emerges Days After Source Leak
Read more at SecurityWeek

Money transfer app Duc exposed thousands of driver's licenses and passports to the open web
Read more at TechCrunch

Attempts to Exploit Exposed "Vite" Installs (CVE-2025-30208), (Thu, Apr 2nd)
Read more at SANS

Residential proxies evaded IP reputation checks in 78% of 4B sessions
Read more at Bleeping Computer

Hackers Exploit CVE-2025-55182 to Breach 766 Next.js Hosts, Steal Credentials
Read more at TheHackerNews

Not Toying Around: Hasbro Attack May Take 'Weeks' to Remediate
Read more at DarkReading

News from Thursday April 2, 2026
(Reported on Friday April 3, 2026)

Hackers Abuse DOCX, RTF, JS, and Python in Stealthy Boeing RFQ Malware Campaign
Read more at CyberSecurityNews

New 'Storm' Infostealer Remotely Decrypts Stolen Credentials
Read more at InfoSecurityMagazine

Perplexity's "Incognito Mode" is a "sham," lawsuit says
Read more at Arstechnica