

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 March 6, 2026 through March 8, 2026 (Reported on Monday March 9, 2026)

Government

FBI investigates breach of surveillance and wiretap systems

Read more at [Bleeping Computer](#)

CISA Warns of macOS and iOS Vulnerabilities Exploited in Attacks

Read more at [CyberSecurityNews](#)

Financial Institutions

TransUnion Launches AI Analytics Orchestrator Agent To Speed Credit Insights

Read more at [CUtoday.info](#)

Healthcare

HHS OCR Fines Firm \$10K in Breach Affecting 15M

Read more at [BankInfoSecurity](#)

Other

Microsoft: Hackers abusing AI at every stage of cyberattacks

Read more at [Bleeping Computer](#)

Chrome Extension Turns Malicious After Ownership Transfer, Enabling Code Injection and Data Theft

Read more at [TheHackerNews](#)

Termite ransomware breaches linked to ClickFix CastleRAT attacks

Read more at [Bleeping Computer](#)

OpenAI Codex Security Scanned 1.2 Million Commits and Found 10,561 High-Severity Issues

Read more at [TheHackerNews](#)

How AI Assistants are Moving the Security Goalposts

Read more at [Krebs on Security](#)

Hackers abuse .arpa DNS and ipv6 to evade phishing defenses

Read more at [Bleeping Computer](#)



**News from Friday March 6, 2026 through March 8, 2026
(Reported on Monday March 9, 2026)**

Anthropic Finds 22 Firefox Vulnerabilities Using Claude Opus 4.6 AI Model

Read more at [TheHackerNews](#)

Microsoft Azure CTO set Claude on his 1986 Apple II code, says it found vulns

Read more at [TheRegister](#)

