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 Wednesday February 04, 2026 (Reported on Thursday February 05, 2026)

Government

Cybersecurity's New Business Case: Fraud
Read more at GovTech

Victims Are Rebuffing Ransomware Mass Data Theft Campaigns
Read more at BankInfoSecurity

Tulsa, Okla., Airport Tech Teams Contain Ransomware Attack
Read more at GovTech

Financial Institutions

Suspect Nabbed After Bold Daytime Robbery Of Austin Telco FCU
Read more at CUtoday.info

Healthcare

Questions Loom Ahead of Substance Abuse Privacy Rules Shift
Read more at HealthcareInfoSecurity

FBI Urges Organziations to Take 10 Actions to Improve Cyber Resilience
Read more at TheHIPAAJournal

Other

Hackers compromise NGINX servers to redirect user traffic
Read more at Bleeping Computer

CISA: VMware ESXi flaw now exploited in ransomware attacks
Read more at Bleeping Computer

CISA warns of five-year-old GitLab flaw exploited in attacks
Read more at Bleeping Computer

EDR killer tool uses signed kernel driver from forensic software
Read more at Bleeping Computer

Critical n8n flaws disclosed along with public exploits

News from Wednesday February 04, 2026
(Reported on Thursday February 05, 2026)

Read more at Bleeping Computer

The Double-Edged Sword of Non-Human Identities
Read more at Bleeping Computer

New Amaranth Dragon cyberespionage group exploits WinRAR flaw
Read more at Bleeping Computer