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 January 30, 2026, to Sunday February 01, 2026
(Reported on Monday February 02, 2026)

Government

State CIO Group Seeks Federal Support for AI, Cybersecurity
Read more at GovInfoSecurity

The Risks and Rewards of AI in School: What to Know
Read more at Edweek.org

U.S. convicts ex-Google engineer for sending AI tech data to China
Read more at Bleeping Computer

Financial Institutions

Groups Warn $32B Google-Wiz Deal Threatens Cloud Competition
Read more at BankInfoSecurity

Healthcare

Why AI Use in Healthcare Requires Continuous Oversight
Read more at HealthcareInfoSecurity

Healthcare Interactive: More Than 3 Million Individuals Affected by July 2025 Security Incident
Read more at The HIPAA Journal

Other

Exposed MongoDB instances still targeted in data extortion attacks
Read more at Bleeping Computer

New Apple privacy feature limits location tracking on iPhones, iPads
Read more at Bleeping Computer

Cloud storage payment scam floods inboxes with fake renewals
Read more at Bleeping Computer

Mandiant details how ShinyHunters abuse SSO to steal cloud data
Read more at Bleeping Computer

**News from Friday January 30, 2026, to Sunday February 01, 2026
(Reported on Monday February 02, 2026)**

Iran-Linked RedKitten Cyber Campaign Targets Human Rights NGOs and Activists
Read more at TheHackerNews

Mandiant Finds ShinyHunters-Style Vishing Attacks Stealing MFA to Breach SaaS Platforms
Read more at TheHackerNews

CERT Polska Details Coordinated Cyber Attacks on 30+ Wind and Solar Farms
Read more at TheHackerNews