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 July 02, 2025
(Reported on Thursday July 03, 2025)

Government

DOJ investigates ex-ransomware negotiator over extortion kickbacks
Read more at Bleeping Computer

Sovereign by Design: Data Control in a Borderless World
Read more at GovInfoSecurity

CISA Adds One Known Exploited Vulnerability to Catalog
Read more at Cisa.gov

Financial Institutions

'Skynet' Tries to Outwit AI Malware Analysis
Read more at BankInfoSecurity

Healthcare

Texas Centers for Infectious Disease Associates Announces 19K-Record Data Breach
Read more at TheHIPAAJournal

Feds Notify 103,000 Medicare Beneficiaries of Scam, Breach
Read more at HealthcareInfoSecurity

Other

NimDoor crypto-theft macOS malware revives itself when killed
Read more at Bleeping Computer

AT&T rolls out Wireless Account Lock protection to curb the SIM-swap scourge
Read more at Arstechnica

North Korean Hackers Target Web3 with Nim Malware and Use ClickFix in BabyShark Campaign
Read more at TheHackerNews

That Network Traffic Looks Legit, But it Could be Hiding a Serious Threat
Read more at TheHackerNews

News from Wednesday July 02, 2025
(Reported on Thursday July 03, 2025)

Qantas Airlines Breached, Impacting 6M Customers
Read more at [DarkReading](#)

Spain arrests hackers who targeted politicians and journalists
Read more at [Bleeping Computer](#)