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 Monday March 9, 2025
(Reported on Tuesday March 10, 2025)

Government

Arab, Ala., Hit by $430,000 Phishing Fraud
Read more at [Govtech](#)

FBI warns of phishing attacks impersonating US city, county officials
Read more at [Bleeping Computer](#)

Financial Institutions

Bank Phishing Refunds Should Be Easier, Says CJEU Advisor
Read more at [BankInfoSecurity](#)

UNC4899 Breached Crypto Firm After Developer AirDropped Trojanized File to Work Device
Read more at [TheHackerNews](#)

Healthcare

Alabama Hospital Recently Informed About 2024 Data Breach
Read more at [HIPAAJournal](#)

Other

ShinyHunters claims ongoing Salesforce Aura data theft attacks
Read more at [Bleeping Computer](#)

Fake Claude Code install pages highlight rise of "InstallFix" attacks
Read more at [HelpNetSecurity](#)

Ericsson US discloses data breach after service provider hack
Read more at [Bleeping Computer](#)

New "LeakyLooker" Flaws in Google Looker Studio Could Enable Cross-Tenant SQL Queries
Read more at [TheHackerNews](#)

Microsoft Teams phishing targets employees with A0Backdoor malware
Read more at [Bleeping Computer](#)

News from Monday March 9, 2025
(Reported on Tuesday March 10, 2025)

Salt Typhoon is hacking the world's phone and internet giants
Read more at TechCrunch

Dutch govt warns of Signal, WhatsApp account hijacking attacks
Read more at Bleeping Computer

Attackers use AiTM phishing kit, typosquatted domains to hijack AWS accounts
Read more at HelpNetSecurity

How AI Assistants are Moving the Security Goalposts
Read more at KrebsOnSecurity