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 February 14, 2025, through Sunday February 16, 2025 (Reported on Monday February 17, 2025)

Government

Salt Typhoon Exploits Cisco Devices in Telco Infrastructure
Read more at Darkreading

How District Leaders Use AI to Save Time, Help Teachers, and More
Read more at Edweek.org

Navy FCU's Online Outage Sparks Frustration—And Talk of Jumping Ship
Read more at CUtoday.info

Financial Institutions

The Benefits of the M&A Frenzy in Fraud Solutions
Read more at BankInfoSecurity

Healthcare

Court: UnitedHealth Must Answer for AI-Based Claim Denials
Read more at HealthcareInfoSecurity

Berry, Dunn, McNeil & Parker Agree to $7.25 Million Data Breach Settlement
Read more at TheHIPAAJournal

Other

Analyst Burnout Is an Advanced Persistent Threat
Read more at Darkreading

Nearly a Year Later, Mozilla is Still Promoting OneRep
Read more at KrebsonSecurity

Microsoft: Hackers steal emails in device code phishing attacks
Read more at Bleeping Computer

The Danger of IP Volatility, (Sat, Feb 15th)
Read more at SANS

New FinalDraft malware abuses Outlook mail service for stealthy comms
Read more at Bleeping Computer

News from Friday February 14, 2025, through Sunday February 16, 2025 (Reported on Monday February 17, 2025)

How Diablo hackers uncovered a speedrun scandal
Read more at Arstechnica

Android's New Feature Blocks Fraudsters from Sideloading Apps During Calls
Read more at TheHackerNews