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 Thursday July 23, 2026
(Reported on Friday July 24, 2026)

Local Government

Iranian Hackers Target Siemens and Schneider Industrial Systems, CISA Warns | Targeted Campaign | Infosecurity Magazine

CISA warns Iranian threat actors are actively targeting US-based Siemens and Schneider industrial control systems.

Financial Institutions

How Synthetic Identity Fraud is Coming for Machine Identities | Synthetic Identity Fraud | The Hacker News

Attackers are adapting synthetic identity fraud techniques to create fake machine identities for cybersecurity exploitation.

Healthcare

Report Shows Surge in Malicious Insider Incidents; Mega Data Breaches | Data Breach | HIPAA Journal

New report documents significant increase in malicious insider threats and large-scale data breaches during first half of 2026.

Heart Care Centers of Illinois Discovers Historic Phishing Attack Exposed Patient Data | Phishing | HIPAA Journal

Illinois cardiovascular practice disclosed a phishing attack that compromised patient health information in a historic breach.

Other

Check Point hole grants unauthenticated attackers full SmartConsole admin privileges | Vulnerability | CSO Online

Check Point confirms active exploitation of critical flaw allowing unauthenticated admin access to SmartConsole management platform.

Microsoft 365 outage affects Teams, SharePoint and other services | Service Outage | Bleeping Computer

Major Microsoft 365 service disruption impacted Teams, SharePoint and related services for North American users.

China-Nexus JadeProx Uses New TriBack Loader in Government and Healthcare Attacks | Malware | The Hacker News

China-linked threat actor deploys new TriBack Loader malware targeting government and healthcare entities across Asia and Latin America.

Microsoft's 3-day patching directive comes with added operational risk | Vulnerability Management | CSO Online

Microsoft mandates Windows administrators apply security patches within three days, citing AI-accelerated exploit development risks.