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 August 14, 2026, through Sunday August 16, 2026 (Reported on Monday August 17, 2026)

Local Government

ERP Security Struggles to Keep Pace With AI Agents| AI/ERP Security| GovInfoSecurity

As organizations connect more artificial intelligence agents to ERP systems, new security risks are emerging around identity, authorization, and access to sensitive enterprise data.

Financial Institutions

SAP Commerce Cloud CVE-2026-58231 Targeted in Exploitation Attempts Days After Patch | Vulnerability | The Hacker News

Attackers are targeting a maximum-severity SAP Commerce Cloud flaw that can allow unauthenticated arbitrary code execution, with exploitation attempts observed days after a patch was released.

Healthcare

How AI Could Reshape Biological, Biosecurity Threats | AI-Enabled Biosecurity Threat| GovInfoSecurity

Rapid adoption of AI in biotechnology and pharmaceutical research could also lower barriers for malicious actors seeking to develop or enhance biological threats.

Vishing Attack Provides Threat Act with Access to Quantum Health Network | Data Breach/Vishing | HIPAA Journal

Quantum Health disclosed that a vishing call tricked a user into providing network access, allowing an attacker to steal files containing personal and protected health information.

Data Theft/Extortion Incident Confirmed by Beverly Hills Plastic Surgeon | Data Theft/Extortion | HIPAA Journal

A Beverly Hills plastic surgery practice confirmed unauthorized network access and file theft involving sensitive patient information after being contacted by an individual claiming to have breached its systems.

Other

Microsoft confirms GitHub is down worldwide| Service Outage | Bleeping Computer

GitHub experienced a widespread service disruption affecting developers and organizations that depend on the platform for source-code hosting and software-development workflows.

Philips and GE investigating Clop ransomware data theft claims| Ransomware/Data Theft | Bleeping Computer

Philips and GE are investigating claims by the Clop ransomware group that it stole company data, raising potential exposure concerns at two major technology and healthcare-related manufacturers.

Anthropic confirms Claude is down in major outage affecting multiple services| Service Outage | Bleeping Computer

Anthropic experienced a major Claude service disruption that affected access to multiple AI models and services relying on its platform.

Unisoc VoLTE Video Call Exploit Chain Can Give Attackers Full Android Kernel Access | Remote Code Execution | The Hacker News

Researchers disclosed a two-stage exploit chain in Unisoc-powered Android devices that can begin with a malicious VoLTE video call and escalate from modem compromise to full Android kernel access.

Apple macOS Screen Sharing Flaw Exploited on Internet-Exposed Macs to Install Monero Miner | Vulnerability/Cryptojacking | The Hacker News

Attackers are exploiting a critical macOS Screen Sharing authentication flaw on internet-exposed systems to gain root access and install Monero cryptocurrency miners.

Who's Tracking You? Use This New Service to Find Out | Privacy/Adtech Security | Krebs on Security

New service DecryptAds correlates public adtech records to reveal data brokers and advertising partners, helping identify privacy, malicious-advertising, and supply-chain risks across websites and apps.
