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 August 13, 2026
(Reported on Friday August 14, 2026)

Local Government

Attackers target zero-day vulnerability in geospatial data platform GeoServer | Zero-Day Vulnerability (SQL Injection) | CSO Online

Hackers actively exploit an unpatched SQL injection zero-day in GeoServer, an open-source platform used by government, defense, and science sectors.

White House taps security firms for offensive hack-back operations | Offensive Cyber Operations/Policy | Bleeping Computer

White House memo directs a federal coordination center to let vetted private security firms seek approval for offensive hack-back operations against foreign cybercrime groups.

Healthcare

AnMed Investigating Ransomware Group's Data Theft Claims | Ransomware/Data Breach | HIPAA Journal

US health system AnMed investigates data theft claims after ransomware group The Gentlemen alleges it breached the network.

OnePoint Patient Care and Clay-Platte Family Medicine Settle Data Breach Lawsuits | Data Breach | HIPAA Journal

Two US healthcare organizations reached class-action settlements over prior patient data breaches, offering claims to affected individuals.

Other

Apple sends new 'Threat Notification' alerts over mercenary spyware attacks | Spyware | Bleeping Computer

Apple issued new threat notifications warning select iPhone users they were individually targeted by state-sponsored mercenary spyware attacks.

AI agents wage near-autonomous cyberattack on Asian government networks | AI-Orchestrated Intrusion | CSO Online

Researchers detail a multi-day campaign in which autonomous AI agents largely self-directed network mapping and intrusion against Taiwanese government and nuclear-safety systems.

Akira hackers disable EDR with Safe Mode, steal data but fail to encrypt | Ransomware | Bleeping Computer

Akira ransomware affiliate booted a victim's system into Safe Mode with Networking to bypass EDR protections, exfiltrating data though encryption ultimately failed.

It took $58 to break Microsoft's SCCM, but a patch made it harder | Vulnerability | CSO Online

Security researchers demonstrated a low-cost attack chain letting a basic domain user escalate to full system control in Microsoft SCCM before a patch mitigated it.