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 November 13, 2026 through Sunday November 15, 2026 (Reported on Monday November 16, 2026)

Local Government

FAA Rules Out AI, Hackers Behind US Ground Stop | Network/System Anomaly (Non-Malicious) | BankInfoSecurity

FAA investigators traced a nationwide flight ground stop to a data overload from two contractor routers, ruling out hacking or AI system failure.

Healthcare

Metabase Zero-Day Exploited in Dorsata Data Breach Affecting 58,000 Patients | Zero-Day | HIPAA Journal

Healthcare tech firm Dorsata suffered a breach exposing 58,000 patients' data after attackers exploited a Metabase zero-day vulnerability.

Oregon Dental Practice Reports Two Data Breaches Affecting More Than 31,000 Patients | Data Breach | HIPAA Journal

Two Oregon-area dental practices disclosed separate data breaches exposing personal and health information of over 31,000 patients combined.

Other

The firewall becomes the foothold: Attackers turn Check Point gateways against customers | Vulnerability/Privilege Escalation (actively exploited) | CSO Online

Attackers actively exploit a root-privilege flaw in Check Point Gaia OS firewalls, prompting emergency hotfixes from the vendor.

TSMC employee data breach linked to cloud provider | Data Breach | Bleeping Computer

TSMC confirmed employee personal data was exposed after a third-party cloud provider breach led to data being auctioned online.

PostgreSQL Patches 52 Flaws, Including 22-Year-Old Bug Enabling Authenticated RCE | Vulnerability | The Hacker News

PostgreSQL releases patches for 52 flaws, including a 22-year-old type confusion bug enabling authenticated remote code execution.

ArcticRAT Cybercrime Gang Profiles Victim Finances With AI | Malware | Dark Reading

ArcticRAT Android malware evolves into full-device-control tool, using AI to analyze stolen data and profile victims' finances.

New Mior and Skyfall Attacks Let Rogue Cloud Hosts Steal Secrets From AMD SEV-SNP VMs | Vulnerability | The Hacker News

Researchers reveal Mior and Skyfall attacks letting malicious cloud hosts read, alter, or forge attestation of data inside AMD SEV-SNP encrypted virtual machines.

Researchers continue to find serious vulnerabilities in internet connected refrigerators | Vulnerability | CyberScoop

Security researchers disclosed 14 flaws in Dixell refrigeration controllers allowing remote root access, as honeypots record active exploitation attempts.

Policy and Disclosure: 2026 Edition | Vulnerability Disclosure Policy | Google Project Zero

Google Project Zero shortens its vulnerability disclosure timeline, citing AI-assisted bug discovery and exploitation as outpacing current vendor patch windows.
