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 Tuesday November 10, 2026
(Reported on Wednesday November 11, 2026)

Healthcare

Sutherland Healthcare Solutions; Hoag Memorial Hospital Presbyterian Announce Cyber Incidents | Data Breach | HIPAA Journal

A healthcare business associate and a California hospital system each disclosed separate cyber incidents resulting in exposure of patient data.

Ridgecrest Regional Hospital in California takes systems offline after cyber incident | Unknown/Under Investigation | DysruptionHub

A California hospital took IT systems offline after a cyber incident, causing lingering prescription delays despite restored phone and payment systems.

Other

Binance warns of iOS flaw that could leak crypto wallet secrets | Vulnerability | Bleeping Computer

Binance disclosed an iOS vulnerability letting malicious apps access other apps' private files, potentially exposing crypto wallet seed phrases and credentials.

Hackers Exploit Critical Xen Orchestra Auth Bypass Flaw to Gain Admin Access | Vulnerability (Authentication Bypass) | The Hacker News

Attackers are actively exploiting a critical cookie-parsing flaw in Xen Orchestra to bypass authentication and gain admin access.

Railway breach leads to $740,000 in fraudulent AI charges | Data Breach | Bleeping Computer

Cloud hosting provider Railway suffered an infrastructure breach exposing customer auth secrets for up to 100,000 workspaces, enabling $740,000 in fraudulent AI usage charges.

SGLang RCE Exploit Breaches NEAR AI, Steals Data From 18 Agents and About 100 Users | Vulnerability/RCE Exploit | The Hacker News

Attacker exploited a remote code execution bug in the SGLang inference engine to breach NEAR AI servers, exposing data from 18 agents and about 100 users.

Hackers exploit trusted AWS access to breach multiple cloud environments | Supply Chain | Bleeping Computer

Attackers used stolen AWS credentials from Qubole's big data platform to infiltrate and steal data from multiple customer cloud environments.

Fireworks AI Confirms Wider Breach Affecting Customer Datasets, Model Weights and Notion AI Chats | Data Breach | The Hacker News

Fireworks AI revealed its earlier breach expanded to expose customer datasets, model weights, billing data, and internal Notion chat logs.

New malware doesn't call home, it turns your Exchange server into its home | Malware | CSO Online

ESET identified a new modular malware toolset dubbed 'Cereal' that embeds persistently on Exchange servers for long-term espionage.

AI Coding Agents Leak Thousands of Secrets to GitHub | Data Exposure/Credential Leak | Dark Reading

A flawed default command in Anthropic's Claude Code AI coding tool caused thousands of API keys and credentials to be pushed into public GitHub repositories.

Qubole supply chain attack exposed AWS, Entra ID, and Okta credentials | Supply Chain | CSO Online

Attackers exploited Qubole's AWS cross-account IAM roles to infiltrate customer environments and harvest AWS, Entra ID, and Okta credentials.
