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 17, 2026
(Reported on Wednesday November 18, 2026)

Healthcare

Healthcare firms fail to monitor AI tools as shadow AI leads to breaches | Data Breach | Cybersecurity Dive

Report finds healthcare organizations' unmonitored use of AI tools, or 'shadow AI,' is contributing to data breaches amid overstretched security teams.

Alleged ransomware group member extradited from Italy to face US charges in hospital, school extortion case | Ransomware/Extortion | CyberScoop

A Kazakh national was extradited to the US to face charges for a ransomware extortion conspiracy that targeted hospitals and schools.

Other

Oracle reveals fix-this-ASAP-grade Java4Shell bug that allows attacks on many third-party apps | Vulnerability | The Register

Oracle discloses a critical Java vulnerability enabling unauthenticated remote code execution or JVM crashes across many third-party applications.

Google spots the first hacker AI system that finds and exploits flaws autonomously | AI-Enabled Autonomous Exploitation | CSO Online

Google's threat intelligence team identified the first known AI-driven hacking tool capable of independently discovering and exploiting software vulnerabilities without human guidance.

Tor releases emergency update amid ongoing DDoS attack | DDoS | Bleeping Computer

Tor Project rushed out a relay software patch after a sustained DDoS campaign overwhelmed network relays and disrupted service for most operators.

Researchers Claim Two RCE Exploits That Bypass Telegram's New Android Defenses | Vulnerability/Exploit Bypass | The Hacker News

Security researchers found that malicious bot widgets can evade Telegram Android's new sandbox filter to achieve remote code execution.

Cloud keys leaked in Docker Hub images are stolen within seconds | Credential Exposure / Supply Chain | Bleeping Computer

Researchers found automated bots scanning and exploiting cloud credentials exposed in public Docker Hub images within seconds of upload.

Trigram Campaign Impersonates About 50 AI and Blockchain Brands to Target Devs with Infostealers | Social Engineering / Infostealer Malware | The Hacker News

Large-scale campaign dubbed Trigram spoofs roughly 50 AI and blockchain company brands to trick developers in Europe and the US into running infostealer malware.

Researchers hijack Hugging Face account for popular Kokoro AI model | Supply Chain | Bleeping Computer

Security researchers exploited weak ownership checks on Hugging Face to seize control of the widely-used Kokoro text-to-speech AI model's account.

Researchers Detail iPhone Flaw That Let Apps Record Audio Despite Denied Microphone Permission | Vulnerability | The Hacker News

Researchers disclosed a now-patched Apple audio service flaw that allowed iOS apps to record audio despite users denying microphone permission.

Google and Anthropic push for faster patches as AI collapses bug discovery timelines | Vulnerability Disclosure Policy | CSO Online

Google Project Zero and Anthropic shorten vulnerability disclosure windows, citing AI tools accelerating bug discovery and exploit development.