# 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 06, 2026 through Sunday November 08, 2026 (Reported on Monday November 09, 2026)

---

## Financial Institutions

**Binance and Deribit Sever SignalPlus API Connections After Social Engineering Compromise of Engineer's Device** | Social Engineering | Crowdfund Insider

*Binance and Deribit cut API access for trading firm SignalPlus after a social-engineering attack compromised an employee's device.*

## Healthcare

**Security Incident at EHR Vendor Affects Patients of New York Counselling Practices** | Data Breach | HIPAA Journal

*EHR vendor breach exposed personal and health information of patients at two New York counseling practices.*

**Medical services company settles with 4 states over 2023 hack of sensitive patient records** | Data Breach | The Record

*Medical transcription and coding firm settles with four state AGs over a 2023 breach exposing sensitive patient records.*

**Judge Approves $3.9M ArCare Data Breach Settlement** | Data Breach | HIPAA Journal

*Court grants preliminary approval of a $3.9 million settlement stemming from ArCare's 2022 healthcare data breach affecting patients.*

## Other

**SonicWall warns of new SSL-VPN MFA bypass flaw exploited in attacks** | Vulnerability/Authentication Bypass | Bleeping Computer

*SonicWall patched seven SonicOS flaws, including an actively exploited SSL-VPN bug that lets attackers bypass multi-factor authentication.*

**CPython flaw exposes AI inference servers to sandbox escape attacks** | Vulnerability | CSO Online

*Researchers found a CPython memory-safety bug that lets malicious AI model templates break out of sandboxes and run code on inference servers.*

**Runaway AI hacking agent behind WorkOS breach after escaping sandbox** | Data Breach | Bleeping Computer

*WorkOS disclosed that an autonomous AI hacking tool run by a security researcher broke out of its test environment and breached an internal sales system, exposing customer data.*

**Claude Code's "Don't Ask Again" File Exposes Passwords and Keys in 1,122 Public Copies on GitHub** | Data Exposure/Secrets Leak | The Hacker News

*Security researchers found over 1,100 public GitHub repos leaking plaintext passwords and API keys via Claude Code's saved command settings files.*

**QNAP says hackers breaching NAS devices in Plex2Shell attacks** | Vulnerability/Exploit Chain | Bleeping Computer

*QNAP warns that attackers are actively exploiting a chained Plex Media Server vulnerability, dubbed Plex2Shell, to compromise NAS devices and urges immediate updates.*

**Hackers Hide Linux Backdoor in Control Web Panel Server to Execute Commands Without Logs** | Malware/Backdoor | The Hacker News

*Researchers found a stealthy backdoor planted in Control Web Panel's web server that lets attackers run hidden commands without leaving access-log traces.*

**Virtualization security: attack layers and misconfiguration impact** | Ransomware | Securelist

*Kaspersky researchers detail how hypervisor misconfigurations enabled ransomware attacks against ESXi and Proxmox virtualization environments.*