

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 Wednesday October 14, 2026
(Reported on Thursday October 15, 2026)**

Local Government

Palo Alto Networks warns of PAN-OS RCE flaw exploited in attacks | Zero-Day | [Bleeping Computer](#)

Palo Alto Networks patched an actively exploited zero-day remote code execution flaw in PAN-OS firewalls after attackers used it in real-world attacks.

DHS Inspector General Finds That TSA is Not Properly Safeguarding Passenger Facial Recognition Data | Vulnerability | [EFF Deeplinks](#)

DHS watchdog audit found TSA's facial recognition system has a significant security weakness that could expose travelers' biometric data.

Officials see gaps in election communications as AI makes foreign influence easier | Disinformation/Influence Operations | [NextGov](#)

Officials warn that weakening coordination between federal, state, and industry partners leaves US election systems more exposed to AI-enabled foreign disinformation ahead of midterms.

Financial Institutions

Hirudo Android malware replaces banking apps to evade security checks | Malware | [Bleeping Computer](#)

New Hirudo Android malware swaps legitimate banking apps for malicious clones to bypass security checks and steal credentials.



Healthcare

Twin Cities Pain Clinic Settles Data Breach Litigation | Data Breach | [HIPAA Journal](#)

Minnesota pain management clinic reaches class action settlement over a 2025 data breach exposing patient information.

Other

Microsoft and partners disrupt vast Chinese-language phishing kit ecosystem | Phishing | [CyberScoop](#)

Microsoft and partners dismantled a large Chinese-language phishing-as-a-service operation that sent over a billion fraudulent messages to 75,000+ organizations worldwide.

Unit 42 Uncovers PEERSTITCH, a Stealthy FortiGate Implant | Vulnerability/Malware Implant | [Palo Alto Networks Unit 42](#)

Unit 42 details PEERSTITCH, a stealthy ARM64 implant deployed on 500+ FortiGate firewalls via exploitation of FortiManager flaw CVE-2024-47575.

ROMULUS Malware Server Leverages ClickFix to Deliver Multiple Payloads | Malware | [Infosecurity Magazine](#)

Researchers found a ClickFix-based malware delivery server called Romulus distributing multiple malware payloads, signaling the technique's shift into reusable attacker infrastructure.

How Claude Code's 256KB blind spot put developers' secrets in the preview pane | Vulnerability | [CSO Online](#)

Researchers found a Claude Code Desktop flaw letting malicious JavaScript in HTML files run automatically, risking developer credentials and systems.

Anthropic 'SneakPeek' Flaw Is a Silent Zero-Click Threat | Vulnerability | [Dark Reading](#)

Security flaw in Claude Code Desktop's preview pane could let attackers silently exfiltrate developer credentials like SSH keys and AWS tokens.

