

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 Thursday October 15, 2026
(Reported on Friday October 16, 2026)**

Local Government

Federal bankruptcy courts dealing with outages after contractor cyberattack | Supply Chain | [The Record](#)

A cyberattack on a government contractor disrupted federal bankruptcy court systems, halting production of bankruptcy notices nationwide.

AI-Powered Espionage Campaign Targets Government Linux Infrastructure | Malware/Espionage | [Palo Alto Networks Unit 42](#)

Researchers detail a nation-state-style espionage campaign using AI-assisted tooling, custom malware, and web shells to steal credentials from government Linux systems.

The next election influence campaign will target your AI chatbot | Influence Operation / Disinformation | [CyberScoop](#)

Researchers find coordinated hyperlocal content designed to manipulate AI chatbots' responses about political candidates and election races.

Healthcare

July 2026 Healthcare Data Breach Report | Data Breach | [HIPAA Journal](#)

Monthly HIPAA Journal report tallies 77 US healthcare data breaches impacting 500+ individuals reported to HHS in July 2026.



Other

Critical PwnEscape Linux Kernel Vulnerability Lets Guest VMs Read Host Memory | Vulnerability | [The Hacker News](#)

Critical Linux kernel networking flaw lets guest VM code read host memory, confirmed exploitable against Vercel's cloud sandboxes.

Hackers exploit Collabora RCE flaw to backdoor Nextcloud servers | Vulnerability/Remote Code Execution | [Bleeping Computer](#)

Attackers are actively exploiting a critical RCE flaw in Collabora Online's Nextcloud app to install backdoors on compromised servers.

NGINX Fixes 5 Flaws, Including Possible RCE and a TLS Bug That May Skip Client-Cert Checks | Vulnerability | [The Hacker News](#)

NGINX patched five vulnerabilities, including memory bugs enabling possible remote code execution and a two-decade-old TLS flaw that could bypass client certificate checks.

Hackers hijack D-Link, Ubiquiti devices to resell your stolen bandwidth | Botnet/Proxyjacking | [Bleeping Computer](#)

Attackers are compromising D-Link and Ubiquiti network devices worldwide to covertly sell victims' bandwidth through a residential proxy service.

Next.js Ships Out-of-Band Patch for Two Critical RCE Flaws in Caching and SVG Processing | Vulnerability | [The Hacker News](#)

Next.js issued an emergency patch fixing two critical unauthenticated RCE bugs in React Server Components and SVG image handling, plus a high-severity DoS flaw.

Fake Arch Linux packages push malware with root privileges | Supply Chain | [Bleeping Computer](#)

Attacker uploaded malicious AUR packages mimicking popular Arch Linux tools yay and paru to install malware with root access.

