

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 11, 2025 (Reported Wednesday November 12, 2025)

Government

US Congress Moves to Revive CISA 2015 After Shutdown

Read more at [GovInfoSecurity](#)

Financial Institutions

How Prompt Injection Is Breaking Digital Forensics Norms

Read more at [BankInfoSecurity](#)

Walmart Deploys New AI Tools To Simplify Holiday Shopping Experience

Read more at [CUpday.info](#)

Healthcare

Healthcare Sees 224% Annual Increase in Attacks Targeting Mobile Devices

Read more at [TheHIPAAJournal](#)

First Choice Dental Agrees to Pay up to \$1,225,000 to Settle Data Breach Lawsuit

Read more at [TheHIPAAJournal](#)

Other

Synology fixes BeeStation zero-days demoed at Pwn2Own Ireland

Read more at [Bleeping Computer](#)

Microsoft Patch Tuesday for November 2025, (Tue, Nov 11th)

Read more at [SANS](#)

Google says new cloud-based "Private AI Compute" is just as secure as local processing

Read more at [Arstechnica](#)

WhatsApp Malware 'Maverick' Hijacks Browser Sessions to Target Brazil's Biggest Banks

Read more at [TheHackerNews](#)

Patch Now: Microsoft Flags Zero-Day & Critical Zero-Click Bugs

Read more at [DarkReading](#)



**News from Tuesday November 11, 2025
(Reported Wednesday November 12, 2025)**

Microsoft: Windows 11 23H2 Home and Pro reach end of support

Read more at [Bleeping Computer](#)

GootLoader Is Back, Using a New Font Trick to Hide Malware on WordPress Sites

Read more at [TheHackerNews](#)

Grandparents to C-Suite: Elder Fraud Reveals Gaps in Human-Centered Cybersecurity

Read more at [DarkReading](#)

SAP fixes hardcoded credentials flaw in SQL Anywhere Monitor

Read more at [Bleeping Computer](#)

