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 November 05, 2026
(Reported on Friday November 06, 2026)

Local Government

US Government Email Systems Open to Abuse Thanks to Typos | Vulnerability/DNS Misconfiguration | Dark Reading

Security researchers found that outdated or mistyped DNS records in US federal agency domains can let attackers hijack email communications.

Financial Institutions

Bank Phishing Sites Show Fake 'Suspended' Pages to Evade Takedowns | Phishing | Security Week

Researchers found over 200 bank phishing sites that cloak content, showing fake 'suspended' pages to repeat visitors to dodge takedown efforts.

Healthcare

Vida Y Salud-Health Systems & Hampton Regional Medical Center Settle Data Breach Lawsuits | Data Breach | HIPAA Journal

Two US healthcare providers reach class-action settlements over lawsuits stemming from prior patient data breach incidents.

Other

DigiCert data breach exposes customer information, identity documents | Data Breach | Bleeping Computer

DigiCert disclosed that a server migration error exposed an internal system online, letting unauthorized parties access customer data and identity documents.

OpenSSH Issues Emergency Fix for Flaw Letting Long Passwords Bypass SSH Auth on Alpine Linux | Vulnerability | The Hacker News

Critical OpenSSH flaw allowed attackers with network access to bypass authentication on password-less Alpine Linux accounts using long passwords, prompting emergency patches.

3 Charged in Scheme to Use AI to Impersonate CEOs and Attorneys to Steal $129 Million | Social Engineering | Security Week

Prosecutors charged three men with using AI-generated voice and video to impersonate executives and lawyers, defrauding companies of $129 million.

OpenAI built an AI pipeline to find, exploit and patch Linux flaws | Vulnerability/Exploit Development | CSO Online

OpenAI's autonomous AI system discovered and built working exploits for 948 Linux privilege-escalation flaws, then generated patches for review.

Threat actors use agentic AI tooling to find and abuse exposed secrets | Secrets Exposure / OAuth Application Compromise | Microsoft Security Blog

Microsoft reports attackers using an AI-driven offensive security tool to scan GitHub for leaked OAuth secrets and hijack cloud applications.

The SOC Files 5: Ghost in the pipeline, or a fileless SharePoint breach by Storm-2603 | Vulnerability Exploitation / Fileless Malware | Securelist

Kaspersky details Storm-2603's ToolShell SharePoint exploit chain and fileless post-exploitation tactics used to evade endpoint detection.

Researchers Bypass ChatGPT Lockdown Mode to Exfiltrate Chats Without User Interaction | Vulnerability/Prompt Injection | The Hacker News

Security researchers found a patched flaw letting attackers bypass ChatGPT's Lockdown Mode to silently exfiltrate user chat data via prompt injection.

Anthropic won't fix a Claude Dispatch flaw that could let attackers execute remote commands across corporate boundaries | Vulnerability | The Register

Researchers detail an unpatched Claude Dispatch flaw that chains privilege escalation into remote code execution across organizational boundaries, which Anthropic has declined to fix.
