

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 01, 2026
(Reported on Friday October 02, 2026)**

Local Government

Preparing governments for an era of interconnected cyber risk | Threat Report/Analysis | [Microsoft Security Blog](#)

Microsoft's annual threat report finds government agencies worldwide faced sharply rising cyberattacks, now 27% of observed malicious activity, up from 17% a year earlier.

China-Linked Hackers Impersonate AI Experts to Target US Policy Insiders | Phishing/Social Engineering | [Infosecurity Magazine](#)

China-linked threat group TA419 impersonated AI policy experts to phish Microsoft 365 credentials from US AI policy specialists.

Financial Institutions

Metamask discloses security incident affecting its infrastructure | Security Incident | [Bleeping Computer](#)

Crypto wallet provider MetaMask reported an active security incident impacting part of its infrastructure, with investigation still ongoing.

Healthcare

Data Breaches Announced by Saber Healthcare & Buchalter | Data Breach | [HIPAA Journal](#)

Ohio-based Saber Healthcare and California law firm Buchalter each disclosed separate data breaches affecting sensitive personal information.



CPAP Medical Supplies and Services Agrees to Pay Up to \$500K to Resolve Data Breach Lawsuit | Data Breach | [HIPAA Journal](#)

Florida sleep apnea equipment provider settles data breach lawsuit for up to \$500,000 following patient data exposure.

Other

Fortinet warns of critical FortiMail flaw exploited in zero-day attacks | Zero-Day/Vulnerability | [Bleeping Computer](#)

Fortinet disclosed a critical FortiMail vulnerability under active zero-day exploitation that allows attackers to execute unauthorized commands on affected devices.

Operation KillSwitch: Police Dismantle KillSec Ransomware Group | Ransomware | [Security Affairs](#)

International law enforcement seized the dark web leak site of KillSec ransomware group, dismantling an operation tied to roughly 1,000 victims.

WordPress Backdoor Rebuilds Itself After Cleanup Using Files, Database, and Shared Memory | Malware | [The Hacker News](#)

Researchers detail a WordPress backdoor dubbed SC that uses files, database entries, and shared memory to automatically reinstall itself after removal.

CloudSyncD MacOS Backdoor Hides Behind Fake Zoom Installer | Malware | [Infosecurity Magazine](#)

New macOS malware called CloudSyncD poses as a Zoom installer to steal credentials and deploy a two-stage backdoor on infected machines.

