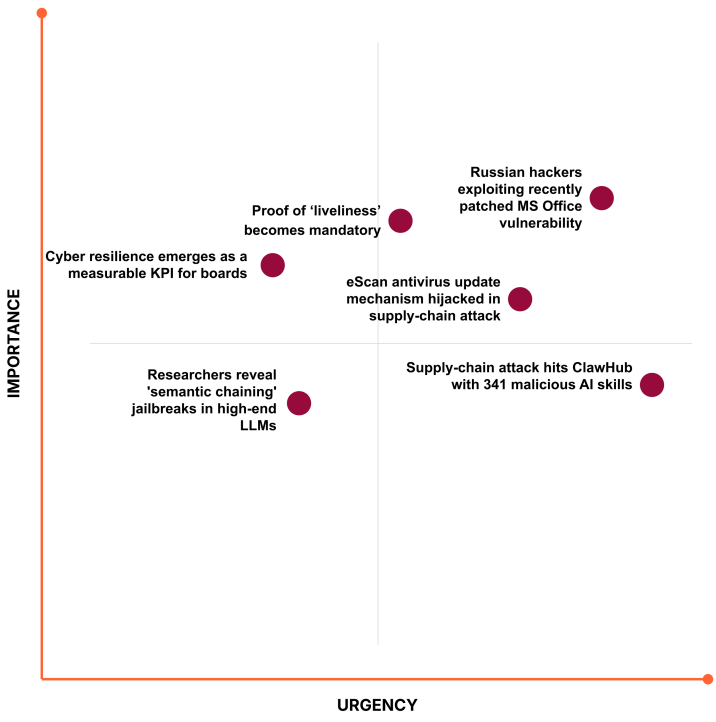
CLOUDFLARE

Cloudflare Cyber Briefing

February 6, 2026

Welcome to the Cloudflare Cyber Briefing from our Field CXO team, helping leaders stay ahead in a fast-moving cyber landscape of threats, technology shifts, and criminal tactics.

What you need to know:



AI cybersecurity

Supply-chain attack hits ClawHub with 341 malicious AI skills

Security researchers have identified a massive campaign, dubbed "ClawHavoc," distributing macOS infostealer malware through the ClawHub skill marketplace. Over 300 trojanized modules for the OpenClaw platform were found masquerading as legitimate crypto and productivity utilities to steal credentials and SSH keys.

CISO's takeaway: The app store model for AI agents creates a massive unvetted supply chain risk within your network. You must treat AI "skills" and plugins as untrusted third-party code. Implement strict access and egress filtering to block silent data exfiltration to attacker-controlled webhooks and use API discovery tools or MCP server portals to monitor for unauthorized outbound calls originating from AI-driven services.

Source: CyberInsider | Read more →

Researchers reveal 'semantic chaining' jailbreaks in high-end LLMs

Security analysts have demonstrated a new semantic chaining technique that successfully bypasses the safety guardrails of advanced models like Gemini Nano Banana and Grok 4. These attacks use layered logical prompts to trick AI into generating malicious payloads or exfiltrating data.

CISO's takeaway: Traditional signature-based security cannot catch logical AI manipulation; you must secure the application layer where these interactions occur. Deploying automated monitoring and guardrails helps detect anomalous request patterns that signify a jailbreak attempt in progress.

Source: Dark Reading | Read more →

Cyber incidents

Russian hackers exploiting recently patched MS Office vulnerability

State-sponsored threat actors are actively exploiting CVE-2026-21509, a high-severity vulnerability in Microsoft Office that allows for unauthorized data access and persistence. Despite a recent patch, many organizations remain vulnerable due to delayed update cycles in complex environments.

CISO's takeaway: Patching lag is a primary vector for nation-state offensive operations. To neutralize this risk without disrupting productivity, ensure endpoint detection and response is on point. Combine this with cloud-native email security to

identify and strip malicious attachments before they ever reach an employee's inbox. Further strengthen your resilience strategy with incident response and business continuity.

Source: Help Net Security | Read more →

---

eScan antivirus update mechanism hijacked in supply-chain attack

Threat actors compromised MicroWorld Technologies' eScan update servers to push multi-stage malware disguised as legitimate software updates. The malware establishes persistence and disables future security patches on infected endpoints.

CISO's takeaway: Supply-chain trust is a primary vulnerability; you must treat all third-party updates as high-risk. Use an appropriate endpoint detection and response solution to monitor endpoints, remote browser isolation for sensitive admin tasks, and enforce strict identity-based controls for server-to-server communications to contain the impact of a compromised trusted vendor.

Source: Check Point | Read more →

Cyber insights

Proof of 'liveliness' becomes mandatory

With deepfakes rendering traditional biometrics and voiceprints obsolete, strategic identity shifts are moving toward proof of liveliness detection and multi-frame analysis. CISOs are being urged to abandon static MFA in favor of continuous, behavioral authentication.

CISO's takeaway: Static credentials are a liability in the age of AI-generated fraud. Move toward a passwordless architecture that leverages hardware keys and client certificate-based authentication to ensure that only verified, live devices and users can access your environment.

Source: The Hacker News | Read more →

Cyber resilience emerges as a measurable KPI for boards

Aon's 2026 outlook indicates that cyber resilience is transitioning from a technical goal to a formal business metric. Organizations are now being measured by their minimum viable company survival time during systemic outages rather than just

breach prevention.

CISO's takeaway: To meet resilience KPIs, build your architecture that delivers them with confidence. Utilizing distributed cloud networking and any-to-any connectivity allows for rapid traffic rerouting and service continuity during a regional or provider-specific outage.

Source: Aon | Read more →

Cloudflare insights

Building vertical microfrontends on Cloudflare's platform

New service binding capabilities allow developers to deploy multiple Workers under a single domain to create seamless, high-performance microfrontends. More can be found here.

Building a serverless, post-quantum Matrix homeserver

A new technical deep-dive explains how to deploy a Matrix homeserver on Workers that uses post-quantum hybrid key agreement to protect all data in transit by default. More can be found here.

Introducing Moltworker: A self-hosted personal AI agent

A new experiment in building private, serverless AI agents that run in secure sandboxes using Workers AI and Containers. More can be found here.

Google's AI advantage: Why crawler separation is the only path to a fair Internet

Cloudflare outlines the competitive risks posed by unified AI crawlers and argues for legally enforceable rules to allow publishers to opt out of AI training without losing search visibility. More can be found here.

CXO events and resources

Join us at our **Trust Forward Summit** on Wednesday, March 25, an exclusive event at RSAC, connecting cybersecurity leaders, AI innovators, and technology executives to tackle the most pressing challenges in digital trust and AI-driven innovation.

Ready to swap conference meetings for a bit of fun? On Night 3 of RSAC, join Cloudflare for an exclusive evening designed for unwinding. At our **CxO Casino Night**, connect with fellow CxOs and visionaries in a relaxed, unscripted lounge atmosphere. Best of all? Every hand dealt supports a charitable cause.

Come chat with Cloudflare's Field CXO team at the following events:

- CS4CA ANZ Summit, February 10–11, Perth, AU
- Peer Point Tokyo, February 11, Tokyo, JP
- 6th CISO 360 Americas, February 11–12, New York, NY, US
- Munich Cyber Security Conference, February 12–13, Munich, DE
- Cloudflare Immerse Dallas, February 12, Dallas, TX, US
- Swiss Cyber Security Days, February 17–18, Bern, CH
- Cloudflare Immerse Madrid, February 19, Madrid, ES
- Government Cybersecurity Showcase Federal, February 25, Ottawa, CA
- Cloudflare AI at Scale: Digital Natives Roundtable, February 26, Sydney, AU