

AI Sidebar Extension Monetizes Its Own Updates

 netskope.com/blog/ai-sidebar-extension-monetizes-its-own-updates

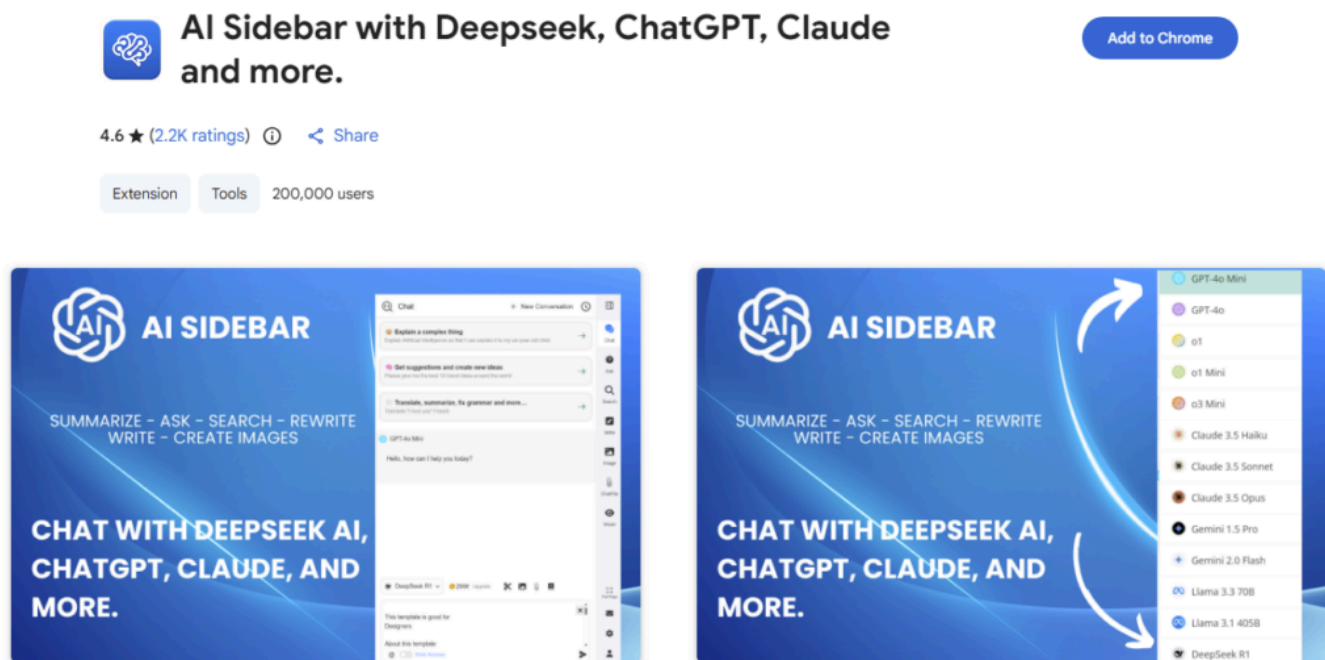
Vini Egerland

August 11, 2026

The Chrome extension “[AI Sidebar with DeepSeek AI](#)” that Google removed from the Chrome Web Store in January 2026 for stealing AI conversation content resumed shipping code to enterprise endpoints in July 2026.

The extension released a benign update removing the data theft code and acknowledged its wrongdoing. After 2 weeks it pulled the rug again with a new update.

Netskope Threat Labs analyzed the new build. While it no longer contains the conversation-exfiltration code, it now contains a monetization payload that opens an affiliate link in a foreground browser tab every single time the extension updates and uninstalls. Additionally, it suppresses the redirection of DeepSeek users to ChatGPT.



Extension's Chrome Web Store page

Key findings

- A Chrome extension had been delisted for AI conversation theft. Recently, it was relisted and continued to deliver updates to the surviving install base through Google's CRX content delivery network.
- The operator used a clean-then-poison update sequence. Version 1.7.2.0 distributed no malicious payload. Version 1.7.3.0 introduced it as a surgical 21-line malicious insertion of a monetization payload.

- The monetization payload opens an affiliate link, while abusing a race condition to own the uninstall destination.

Phase one: an AI sidebar that read the conversation

The extension entered the Chrome Web Store as an AI assistant sidebar, and by the time it was removed, it had reported more than 300,000 installs and a 4.6-star rating. Its functionality was real.

In December 2025, OX Security [published research](#) showing that pre-1.7.x versions of this extension scraped ChatGPT and DeepSeek conversation content from the page and posted it, base64-encoded, to `deepaichats[.]com` and `chatsaigpt[.]com` on a recurring interval. Since then, the code was removed before v1.7.x, and the extension's own privacy policy now acknowledges it.

5. What We Do NOT Do

- We do **not** track your browsing history or the list of sites you visit.
- We do **not** continuously read, monitor, or record the pages you browse in the background. Website content (such as a screenshot or selected text) is accessed only when you actively use a feature that requires it.
- We do **not** collect or send usage analytics or telemetry. (A previous version of the extension contained URL-tracking code; it has been fully removed.)
- We do **not** sell your personal data, and we do **not** use it for advertising.

Extension's policy page

Phase two: the same extension ID, a new build

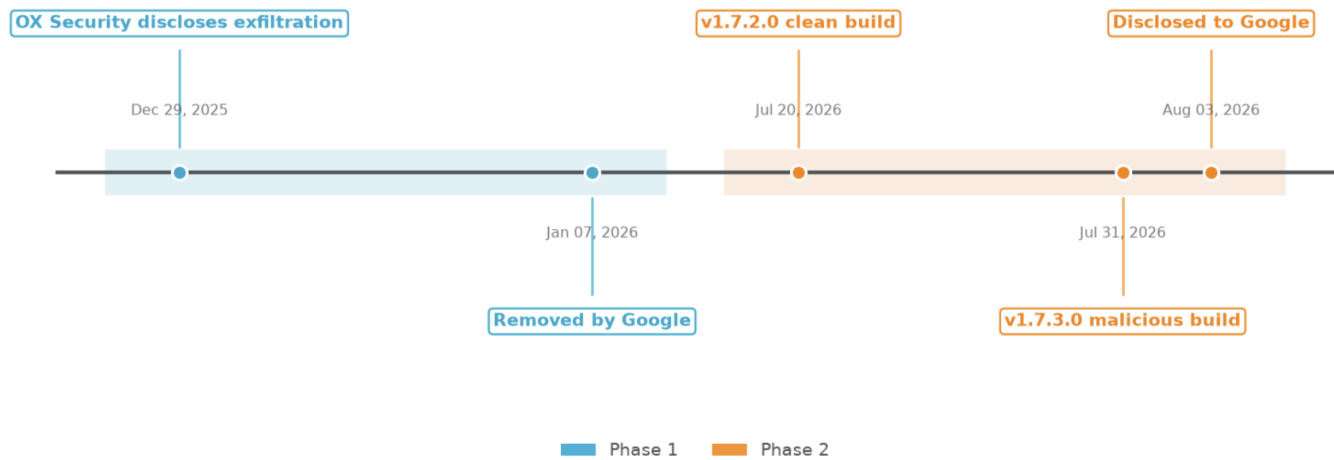
In July 2026, Netskope Threat Protection detected and blocked the latest version 1.7.3.0 of the `.crx` object arriving on enterprise endpoints from Google CDN.

The extension is actively listed on the Chrome Web Store as of August 2026, seemingly re-approved for distribution, and it distributes the malicious build: a user installing the extension today receives the affiliate-fraud payload.

We have observed hundreds of users acquiring the malicious version daily; it is ongoing and growing at twice the rate of the previous version. The extension being relisted is the primary driver, auto-update secondary.

Campaign Timeline: Delisted AI Sidebar Extension

Phase 1: conversation exfiltration and removal. Phase 2: clean build, then poisoned update via Google CRX CDN.



Extension version release timeline

Before the operator inserted the monetization code, it shipped Version 1.7.2.0, a functional, benign extension to establish a clean update history.

It was distributed from July 20 to 31, 2026, nearly 2 weeks before version 1.7.3.0 replaced it with the additional functions: The diff between the two versions of `blueBackground.js` is a surgical 21-line insertion.

What version 1.7.3.0 actually does

What replaced the exfiltration code is a monetization chain built on the extension update and uninstall events. The service worker declares a partner URL and opens it in a foreground tab whenever Chrome reports an update:

“Partner URL”: the redirect URL

```

177 // Show consent gate on first install (instead of aitopia setup)
178 chrome.runtime.onInstalled.addListener(async (details) => {
179     if (details.reason === "install") {
180         // On first install, open consent gate in a new tab
181         chrome.tabs.create({
182             url: chrome.runtime.getURL("consent-gate.html"),
183             active: true,
184         });
185     }
186
187     if (details.reason === "update") {
188         chrome.tabs.create({
189             url: PARTNER_URL,
190             active: true,
191         });
192     }

```

Update listener opening “Partner URL”

The `active: true` argument means that no user interaction is required. The link resolves through Bitly to Buzzy, an AI video generation service that runs a public affiliate program [paying 30% commission on referred subscriptions](#). We have no indication the service is aware its referral program is being driven this way.

Comments were left, not only indicating AI-developed code, but also explicitly indicating “deliberately not on install”, which tells you the design intent. Firing on install would produce one referral per user. Firing on update produces one per user per release, and the operator controls the release cadence.

The uninstall path is claimed the same way, and here the code documents its own tradecraft:

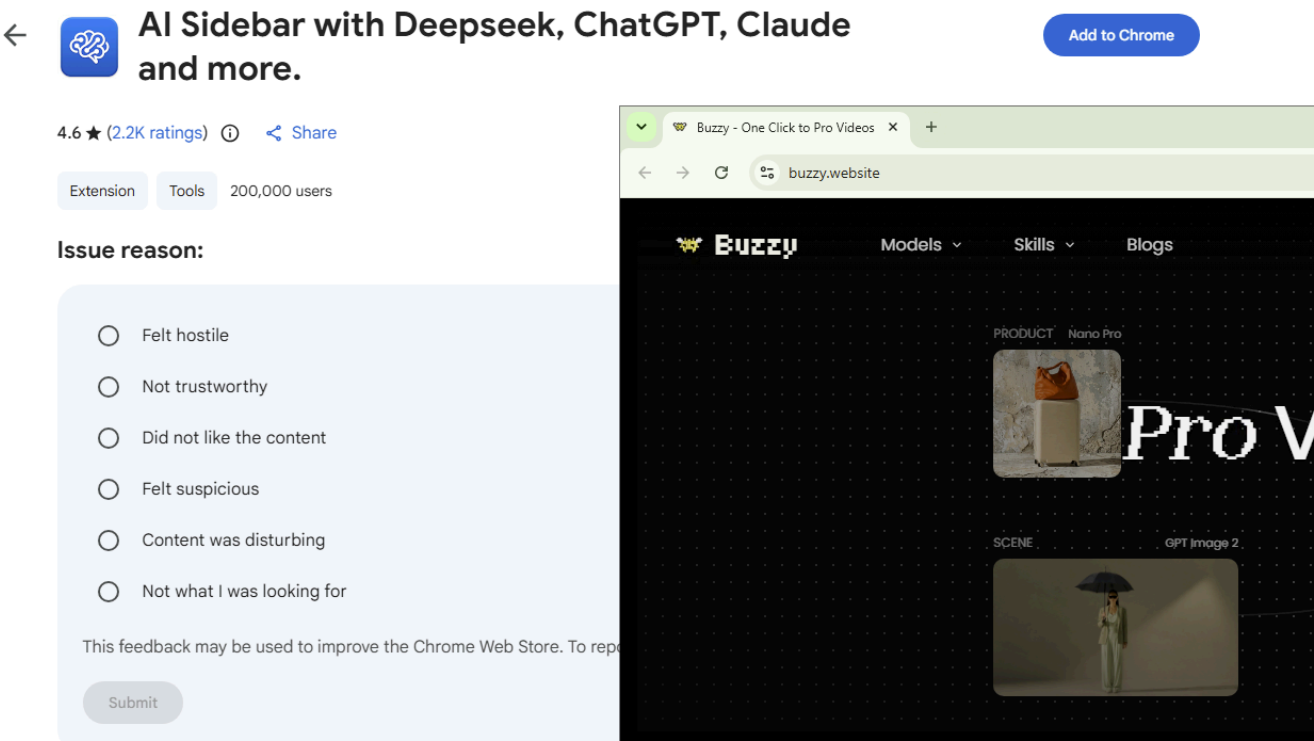
```

18 // The aitopia service-worker also calls setUninstallURL (gated on its remote
19 // app_details.app_uninstall flag) from inside an async chain, so it can land
20 // after ours and win. Set it on every service-worker start and re-assert once
21 // aitopia's config fetch has had time to settle.
22 function setUninstallUrl() {
23     chrome.runtime.setUninstallURL(PARTNER_URL, () => {
24         if (chrome.runtime.lastError) {
25             console.warn(
26                 "[DeepSeek Background] setUninstallURL failed:",
27                 chrome.runtime.lastError.message,
28             );
29         }
30     });
31 }

```

Uninstall listener opening “Partner URL”

Chrome allows exactly one uninstall URL per extension, and the last writer wins. The bundled legitimate code registers its own after an asynchronous configuration fetch, so the operator writes the value twice, five seconds apart, to land after it, which means that a user who removes the extension still generates a referral on the way out.



The operator

“Extchange.com” is named twice in the package, as developer and as data controller, with `info@extchange[.]com` as the privacy contact. The domain was registered in February 2024. Registrant details are not publicly disclosed. It is consistent with an operator whose cover is legitimacy rather than anonymity, using the Aitopia white-label SDK, shipping a genuinely functional product with revenue hooks bolted on.

Welcome to AI Sidebar with Deepseek, ChatGPT, Claude and more.

This extension lets you chat with AI from a sidebar on any website. Using it involves some processing of your data that is necessary to make the AI work — here is exactly what happens, so you know before you start.

Necessary to provide the service:

- **AI chat** — the messages you type are sent to the AI provider to generate a reply. Without this the sidebar cannot function.
- **aitopia.ai** — the technology provider that powers the sidebar (acting as our processor).
- **Your preferences** — stored locally in your browser only.

 **Privacy Notice:** The messages you send are processed by the AI provider to generate responses. We do not sell your data and the extension does not collect analytics or track the pages you visit.

Continue

Prefer not to use it? Just close this tab — the extension stays inactive until you continue — or remove it from your browser at any time.

 [Read Full Privacy Policy](#)

Developed by Extchange.com | Technology partner: aitopia.ai

Note the footer: “Developed by Extchange.com | Technology partner: aitopia.ai” , while Chrome Web Store listing publishes the extension under the developer display name “DeepSeek AI” with contact `info@deepseek[.]ai`.

Details

Version

1.7.3

Offered by

DeepSeek AI

Developer

✉ Email ^

info@deepseek.ai

Updated

July 31, 2026

Size

6.45MiB

Conclusion

The interesting part is not the payload (Affiliate referral fraud is a low-severity outcome), but it is the delivery: a publisher that Google removed for data theft in January was relisted on the Chrome Web Store and still shipping code to enterprise browsers through Google's own CRX distribution infrastructure in July. All it took was a clean release to build a trustworthy release history for only two weeks, to then surgically insert a 21-line payload into an otherwise identical build.

The same mechanism that delivered an affiliate link would deliver anything else the operator chooses to compile next – while monetizing such updates.

Relying solely on marketplace curation is no longer enough to protect enterprise environments from malicious browser extensions. To effectively reduce your attack surface, adopt a proactive control framework:

Maintain fleet visibility: Keep a complete inventory of all installed extensions across your organization.

- Enforce default-deny: Block extension installs by default, allowing them only through explicit policy exceptions.
- Inspect inline content: Perform inline inspections on extension packages, even when delivered via vendor-owned content delivery networks (CDNs).
- Extend remediation: Treat an extension's removal from an official web store as the prompt to begin internal remediation, not as proof that the threat is resolved.
- Treat extensions as a software supply chain, as a publisher controls what ships to existing installs through the vendor's own CDN.

For this extension specifically, remove ID `inhcgfbbfdjbjogdfjbcloglkmhnooop` from managed browsers and confirm it is not present in any force-install or allowlist policy.

Netskope One

Netskope Threat Protection inspects .crx downloads inline as part of Next Generation Secure Web Gateway (NG SWG) traffic and detects version 1.7.3.0 of this extension as

Trojan.GenericFCA.Script.37952 with Netskope AV and through Netskope Advanced Heuristic Analysis.

Netskope Advanced Threat Protection identifies the covert behavior: silent tab injection and uninstall-URL hijacking.

Netskope NG SWG URL Filtering categorizes the Phase 1 exfiltration domains chatsaigpt[.]com and deepaichats[.]com as C&C Server and Malicious Site.

Customers running Netskope Enterprise Browser (EB) can enforce extension policy at the browser layer: allowlist (only approved IDs load), blocklist (named IDs are blocked), or force-install (approved extensions are pushed automatically). Either the allowlist or a targeted blocklist entry for inhcgfpbfdbjogdfjbclgolkmhnooop would prevent this extension from running, independent of whether the CRX download was caught at the network layer.

Disclosure

We reported the extension to Google's Chrome Web Store before publishing this post.

Indicators of compromise

Type	Indicator	Notes
Chrome Extension ID	inhcgfpbfdbjogdfjbclgolkmhnooop	Trojanized extension ("AI Sidebar with DeepSeek AI")
SHA256	2a57de8abd0d15e92784280e5d39906d69a2ae7bb9b2875c77c626e9f0794e05	v1.7.3.0 CRX, malicious
SHA256	d3e0045b4151b360fdc054c5a7a0364afb3d8aea12dfef38f3374bb977a8c579	v1.7.2.0 CRX, clean predecessor
URL	https://bit[.]ly/3RPe03x	Affiliate redirect; opened silently on every update and on uninstall (affiliate redirect, not C2; retargetable, destination can change)
Domain	deepaichats[.]com	Prior C2 for conversation exfiltration (pre-1.7.x; now offline)
Domain	chatsaigpt[.]com	Prior C2 for conversation exfiltration (pre-1.7.x; now offline)

Information presented in this post is based on aggregate usage data collected by the Netskope Security Cloud platform relating to a subset of Netskope customers.



Vini is a CISSP-certified threat researcher at Netskope Threat Labs, where he focuses on the security implications of emerging technologies, supply chain compromise, and post-compromise tactics.