Quand votre navigateur siphonne en secret vos échanges avec des IA

WEB Une société de cybersécurité a découvert que des extensions très populaires pour Chrome et Edge espionnaient les utilisateurs

ANOUCH SEYDTAGHIA

Visite d'un data center de Google le 14 novembre 2025. *(MIDLOTHIAN, TEXAS/BLOOMBERG FINANCE LP)*

Ce sont des programmes en apparence totalement innocents: les extensions pour navigateur web. Que vous employiez Chrome, Firefox, Safari ou Edge, vous avez peut-être installé ces services supplémentaires. Ces extensions servent à personnaliser le navigateur pour ajouter des outils et des fonctions, automatiser des tâches ou changer la manière dont les pages web s'affichent ou se comportent (par exemple en supprimant les publicités). Ces extensions se téléchargent généralement via des magasins en ligne (un peu comme des applications), parfois contrôlés par les sociétés qui proposent ces navigateurs, comme Google.

Les extensions peuvent être très pratiques et faciliter la vie des internautes. Mais parfois, elles peuvent se retourner contre eux. Mi-décembre, la société Koi Security a publié une étude édifiante sur certains de ces programmes. Cette firme a découvert que des extensions siphonnent l'entier des conversations avec des chatbots, conversations qui peuvent contenir des éléments très sensibles, que ce soit au niveau privé ou professionnel.

Une bonne note, mais...

Et pourtant, ce sont des extensions en apparence sûres. Il y a notamment le programme Urban VPN Proxy, conçu (et c'est terriblement paradoxal) pour protéger la vie privée de l'utilisateur. Cette extension semble irréprochable, étant utilisée par plus de 6 millions d'internautes, affichant une note de 4,7 étoiles (sur 5 maximum) dans le magasin de Google, après avoir reçue pas moins de 58 000 avis d'utilisateurs. De plus, le programme affiche le badge «à la une» signifiant qu'un employé de Google l'a analysé.

Mais Urban VPN Proxy est extraordinairement curieux, notamment depuis une mise à jour datant de juillet dernier. L'extension aspire toutes les conversations effectuées avec dix chatbots, dont ChatGPT, Claude, Gemini, Perplexity, Grok ou encore Meta AI. «Pour chaque plateforme, l'extension inclut un script «exécuteur» dédié, conçu pour intercepter et capturer les conversations. La collecte est activée par défaut grâce à des options intégrées dans la configuration de l'extension. Il n'existe aucune option permettant à l'utilisateur de désactiver cette fonctionnalité. La seule façon d'arrêter la collecte de données est de désinstaller complètement l'extension», estime la société de cybersécurité.

Abus de confiance

L'extension aspire tout: chaque requête envoyée à l'IA, chaque réponse reçue, ou encore les horodatages des conversations. Toutes ces données sont ensuite revendues à des annonceurs. Koi Security note que les développeurs de l'extension avertissent l'utilisateur d'une analyse de ces conversations avec des chatbots, mais dans un langage si alambiqué qu'il est incompréhensible pour l'internaute.

> Il n'existe aucune option permettant à l'utilisateur de désactiver la fonctionnalité

D'autres extensions similaires posent les mêmes problèmes, telles 1ClickVPN Proxy, Urban Browser Guard, Urban Ad Blocker ou 1ClickVPN Proxy. Au total, ces programmes comptent plus de 8 millions d'utilisateurs. Comme le souligne Koi Security, les extensions pour navigateurs bénéficient d'une confiance particulière. «Elles fonctionnent en arrière-plan, ont un accès étendu à votre activité de navigation et se mettent à jour automatiquement sans autorisation. Lorsqu'une extension promet confidentialité et sécurité, les utilisateurs ont peu de raisons de soupçonner qu'elle fait le contraire.» Si vous avez installé l'une de ces extensions, désinstallez-la immédiatement. Sachez que toutes vos conversations avec l'IA depuis juillet 2025 ont été enregistrées et partagées avec des tiers, conclut la société de cybersécurité.

A noter qu'en juillet dernier, Koi Security avait constaté qu'une autre extension pour le navigateur Chrome, FreeVPN. One, comptant plus de 100 000 installations et un badge vérifié, prenait des captures des écrans des utilisateurs.

Alternatives suisses

Qu'en conclure? D'abord, qu'il est difficile de faire confiance à qui que ce soit en ligne. Ni aux développeurs peu scrupuleux de ces extensions ni à Google, qui ne fait manifestement pas assez le ménage dans son magasin. Il est ainsi recommandé de ne charger que des extensions créées par des développeurs connus. Et de n'installer que celles qui sont vraiment utiles, et de supprimer toutes les autres.

Enfin, si vous cherchez à protéger au mieux vos conversations avec des chatbots, il est conseillé de n'utiliser que des chatbots offrant un maximum de confidentialité. A ce titre, Lumo, développé par la société genevoise Proton, et Euria, proposé par Infomaniak, offrent un très haut niveau de protection. ■