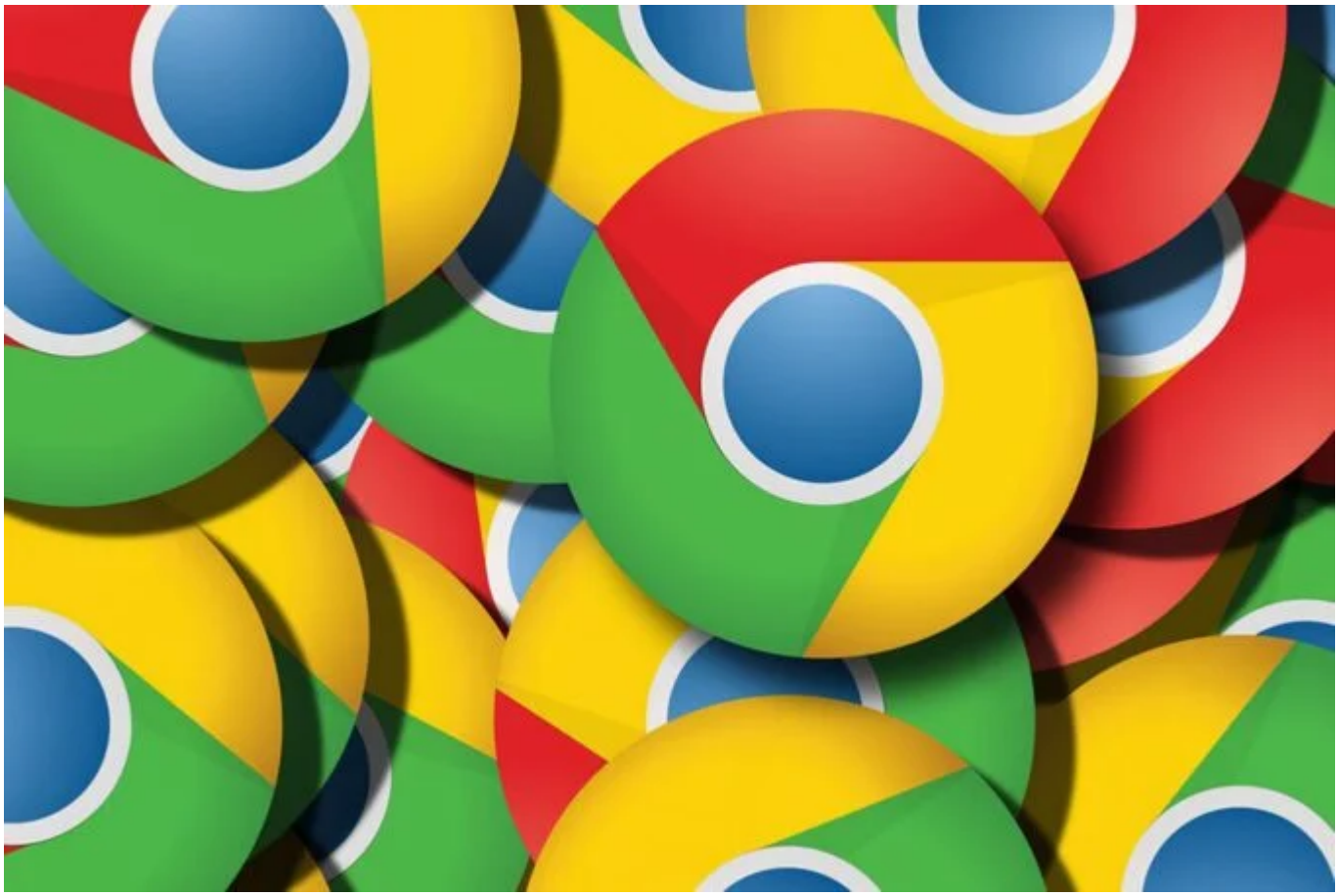
Désinstallez ces 34 extensions Chrome, elles sont dangereuses

Gabriel Manceau :



Des dizaines d'extensions malveillantes, téléchargées plus de 87 millions de fois, ont été découvertes sur le Chrome Web Store de Google.
On vous conseille de regarder si certaines d'entre elles ne sont pas déjà installées sur votre navigateur web.

Une nouvelle vague d'**extensions malveillantes** a été repérée sur le magasin d'application de **Google Chrome**.
Si la plupart d'entre elles ont été retirées du Store, vous devez absolument les désinstaller de votre ordinateur.

34 extensions malveillantes sur le Chrome Web Store

Le Chrome Web Store a toujours été un endroit privilégié pour les pirates qui souhaitent diffuser des logiciels malveillants.
La faute a une modération pas toujours optimale, y compris lorsque les utilisateurs sonnent l'alerte.
L'histoire a commencé avec Vladimir Palant, un chercheur en cybersécurité qui a découvert qu'une extension appelée « PDF Toolbox » contenait du code suspect. Pourtant, l'application avait d'excellentes notes (4,2 en moyenne) et deux millions de téléchargements.

Mais, des « fonctionnalités supplémentaires » ont été découvertes, dont une qui permettait au plugin de charger du code arbitraire sur les pages consultées par l'utilisateur.
Le chercheur est donc parti à la recherche d'extensions permettant le même type de fonctionnalités.
Il a découvert 34 extensions malveillantes qui, combinées, ont été téléchargées 87 millions de fois entre 2021 et 2022.
Voici la liste complète des extensions malveillantes à désinstaller maintenant :

- Autoskip for Youtube
- Soundboost
- Crystal Adblock
- Brisk VPN
- Clipboard Helper
- Maxi Refresher
- Quick Translation
- Easyview Reader view
- PDF Toolbox
- Epsilon Ad blocker
- Craft Cursors
- Alfablocker ad blocker
- Zoom Plus
- Base Image Downloader
- Clickish fun cursors
- Cursor-A custom cursor
- Amazing Dark Mode
- Maximum Color Changer for Youtube
- Awesome Auto Refresh
- Venus Adblock
- Adblock Dragon
- Readl Reader mode
- Volume Frenzy
- Image download center
- Font Customizer
- Easy Undo Closed Tabs
- Screence screen recorder
- OneCleaner
- Repeat button
- Leap Video Downloader
- Tap Image Downloader
- Qspeed Video Speed Controller
- HyperVolume
- Light picture-in-picture

La plupart de ces extensions ont depuis été supprimées par Google, mais la liste n'est pas exhaustive.
En effet, de nouvelles applications malveillantes ont été découvertes depuis la précédente liste de 32

extensions repérées par Avast.

Les dangers de ce type d’extensions et comment s’en protéger

Le principal problème des extensions pour navigateur web réside dans l’accès aux données des utilisateurs dont ils disposent.
Pour qu’une extension fonctionne, elle a généralement besoin de pouvoir lire et modifier les données des sites web que vous visitez.
Si ces permissions ne sont pas accordées, vous ne pouvez tout simplement pas les utiliser.

Avec de tels accès, les développeurs d’extensions malveillantes peuvent suivre toutes vos activités en ligne, les collecter et les vendre, mais aussi voler vos identifiants, mots de passe et moyens de paiement.
L’intégration de publicité dans les pages web et le remplacement dans les résultats de recherche sont également des grands classiques.

Piratage massif de ChatGPT : comment vérifier si votre compte est compromis

Pour vous protéger au mieux des extensions malveillantes, Kaspersky conseille de ne pas trop en installer et de lire les avis des utilisateurs avant de les installer (même si cela a ses limites).
Désinstaller régulièrement les extensions que vous n’utilisez pas est aussi un bon moyen d’éviter les mauvaises surprises.
Enfin, l’installation d’une solution antivirus est par ailleurs un moyen simple et efficace pour vous protéger face à ce type de menaces.

Source : Kaspersky

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230709
"C'est ensemble qu'on avance"