malwarebytes.com

Millions of people spied on by malicious browser extensions in Chrome and Edge

Pieter Arntz

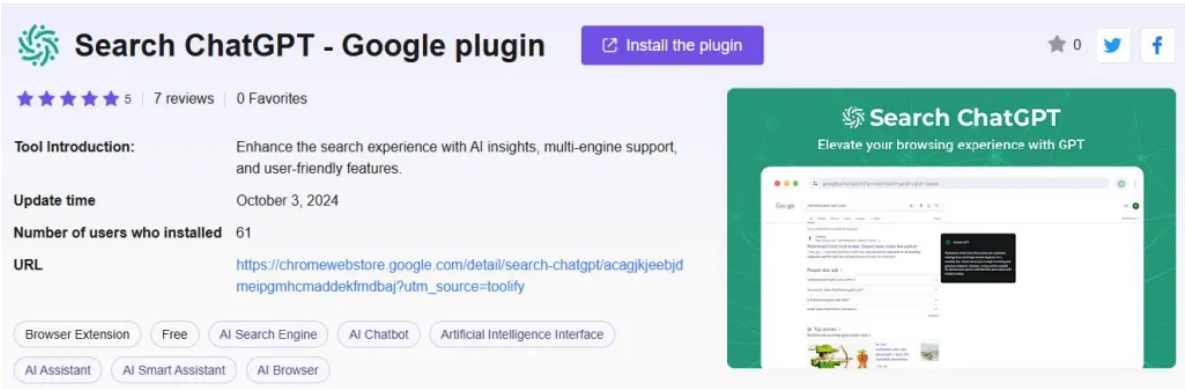
6–8 minutes

Researchers have discovered a campaign that tracked users' online behavior using 18 browser extensions available in the official Chrome and Edge webstores. The total number of installs is estimated to be over two million.

These extensions offered functionality, received good reviews, touted verification badges, and some even enjoyed featured placement.

But when an extension has been available in the web store for a while, cybercriminals can insert malicious code through updates to the extension. Some researchers refer to the clean extensions as "sleeper agents." These sleeper agents are the bases for future malicious activity.

Here's one example of a malicious extension which poses as a search for Chat GPT, and was available for months.



Some of these extensions behaved nicely for years, which made the researchers think they might have been compromised. What these extensions did after they got "woken up" was they deployed a browser hijacking mechanism that activates every time someone navigates to a new page.

Every time the person visits a website, the extension would:

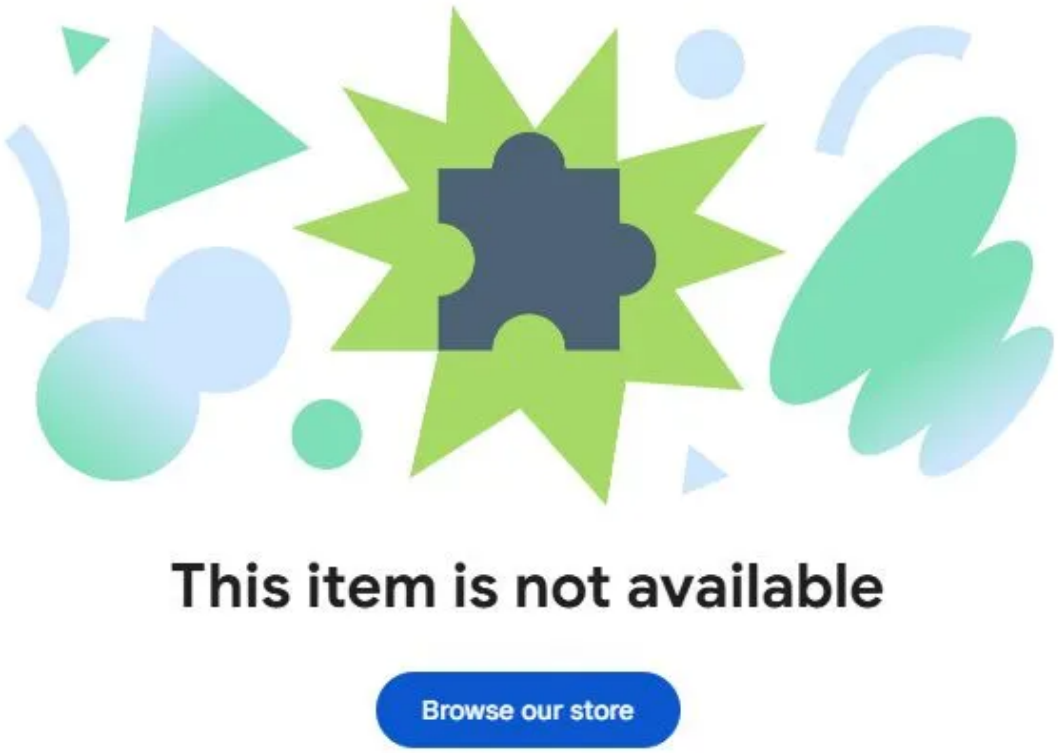
1. Capture the URL of the page they're visiting.
2. Send it to a remote server along with a unique ID issued to track the user.
3. Receive potential redirect URLs from the command and control (C&C) server.

4. Automatically redirect your browser if instructed by the C&C server to do so.

The researchers used the following example of how this might work:

> "You receive a Zoom meeting invitation and click the link. Instead of joining your meeting, one of the malicious extensions intercepts your request and redirects you to a convincing fake page claiming you need to download a "critical Zoom update" to join. You download what appears to be legitimate software, but you've just installed additional malware onto your system, potentially leading to full machine takeover and complete compromise of your device."

Most of the malicious extensions have been removed from the web stores.



Reportedly, 1.7 million people installed these malicious extensions from the Chrome web store and a total of 2.3 million users were affected.

Although we always advise people to only install extensions from official web stores, this proves that not all extensions you download from there are safe. However, the risk involved in getting an extension from outside the web store is even bigger.

Extensions listed in the web store undergo a review process before being admitted. This review, a mix of automated and manual checks, assesses the extension's safety, compliance with policies, and overall user experience. The goal is to protect users from scams, malware, and other malicious activities.

What to do

Check your computer to see if you have any of these extensions:

- Emoji keyboard online (Chrome)
- Free Weather Forecast (Chrome)
- Unlock Discord (Chrome)
- Dark Theme (Chrome)
- Volume Max (Chrome)
- Unblock TikTok (Chrome)
- Unlock YouTube VPN (Chrome)
- Geco colorpick (Chrome)
- Weather (Chrome)
- Unlock TikTok (Edge)
- Volume Booster (Edge)
- Web Sound Equalizer (Edge)
- Header Value (Edge)
- Flash Player (Edge)
- Youtube Unblocked (Edge)
- SearchGPT (Edge)
- Unlock Discord (Edge)

If you find any of the above extensions, try doing the following:

- Clear all browsing data (history, cookies, cached files, site data) to remove any tracking identifiers or session tokens that may have been stolen or set by the malicious extension. Note: you will then have to log in on a lot of sites since they will not remember you.
- Monitor your accounts for any suspicious activity if you visited any sensitive sites (such as online banking) while one of these extensions was installed. Make sure to change your passwords for those accounts.
- Enable two-factor authentication (2FA) where possible for added protection.
- Reset your browser settings to default. This can help undo any changes the extension may have made to your search engine, homepage, or other settings. Note: this will also undo any changes you have made manually. Alternatively, look for signs like unexpected redirects, changed search engines, or new toolbars.
- Keep an eye on your email and text messages for security alerts or notifications about unfamiliar access.
- Make sure your browser and all remaining extensions are up to date.
- Run a full system Malwarebytes scan to check for additional infections. This will also allow you to remove all affected extensions from Chrome and Edge.

Malwarebytes blocks these domains so our users are safe.

To close off, one last word of general advice. If an extension asks for additional permissions after an update, that's a good reason to look closely at what it requires and if that makes sense for the reason you're using the extension.

List of malicious extensions and their domain names

Chrome extensions:

kgmeffmlnkfnjpgmdndccklfigfhajen Emoji keyboard online

dpdibkjjgbaadnnjhkmmnenkmbnhpobj Free Weather Forecast

gaiceihehajjahakcglkhmdbbdclbnlf Free Weather Forecast

mlgbkfnjdmaoldgagamcnommbbnhfnhf Unlock Discord

eckokfcjbjbgjifpcbdmengnabecdakp Dark Theme

mgbhdehiapbjamfgekfpebmhmnmcmemg Volume Max

cbajickflblmpjodnjoldpiicfmecmif Unblock TikTok

pdbfcnhlobhoahcamoefbfodpmklgmjm Unlock YouTube VPN

eokjikchkppnkdipbiggnmlkahcdkikp Geco colorpick

ihbiedpeaicgipncdnnkikeehnjiddck Weather

Edge extensions:

jjdajogomggcjifnjgkpghcijgkbcjdi Unlock TikTok

mmcnmppeeghenglmidpmjkaiamcacmgm Volume Booster

ojdkklpgpacpicaobnhankbalkkgaafp Web Sound Equalizer

lodeighbngipjjedfelnboplhgediclp Header Value

hkjagicdaogfgdifaklcgajmgefjllmd Flash Player

gflkbgebojohihfnnplhbdakoipdbpdm Youtube Unblocked

kpilmncnoafddjpnbhepaiilgkdcieaf SearchGPT

caibdnkmpnjhjdfnomfhijhmebigcelo Unlock Discord

Domains:

admitab[.]com

edmitab[.]com

click.videocontrolls[.]com

c.undiscord[.]com

click.darktheme[.]net

c.jermikro[.]com

c.untwitter[.]com

c.unyoutube[.]net

admitclick[.]net

addmitad[.]com

admiitad[.]com

abmitab[.]com

admitlink[.]net

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.