Chrome extensions that lie about their permissions

blog.malwarebytes.com/puppum/2020/08/chrome-extensions-that-lie-about-their-permissions/

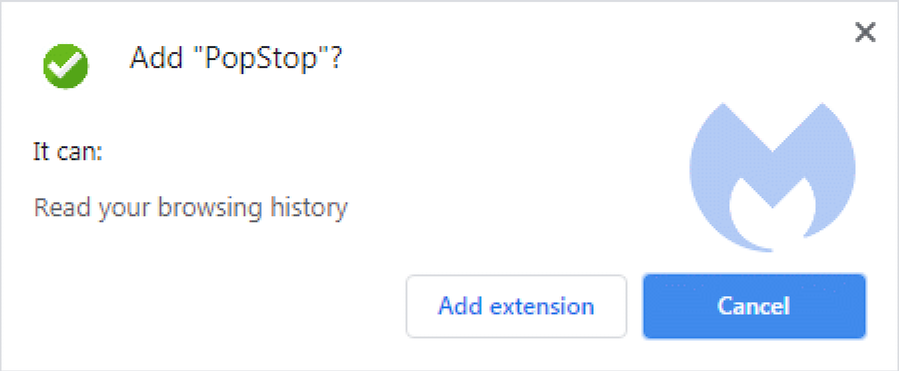
Pieter Arntz

August 13, 2020

"But I *checked* the permissions before I installed this pop-up-blocker—it said nothing about changing my searches," my dad retorts after I scold him for installing yet another search-hijacking Chrome extension. Granted, they are not hard to remove, but having to do it over and over is a nuisance. This is especially true because it can be hard to find out which of the Chrome extensions is the culprit if the browser starts acting up.

What happened?

Recently, we came across a family of search hijackers that are deceptive about the permissions they are going to use in their install prompt. This extension, called PopStop, claims it can only read your browsing history. Seems harmless enough, right?



Add "PopStop"?

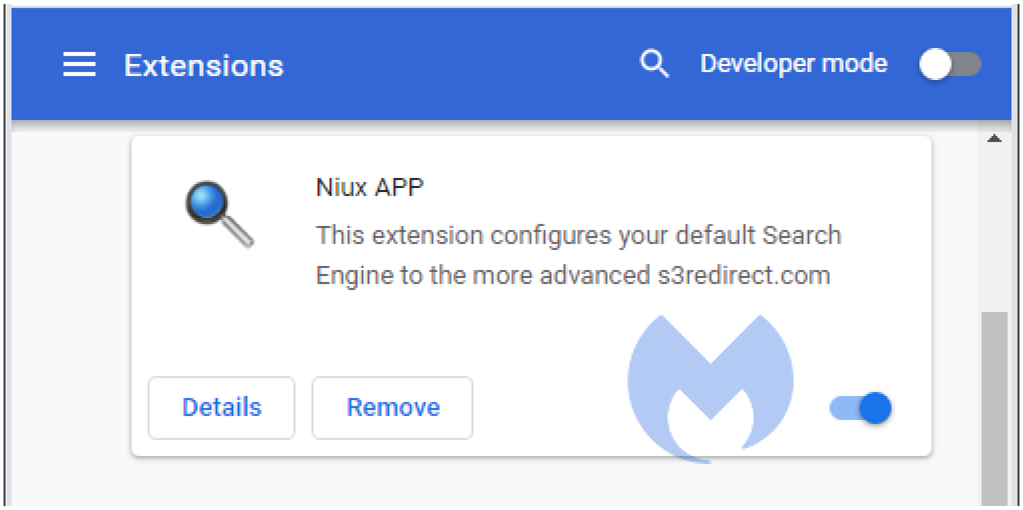
It can:

Read your browsing history

The install prompt in the webstore is supposed to give you accurate information about the permissions the extension you are about to install requires. It already is habit for browser extensions to only ask for permissions needed to function properly up front—then ask for additional permissions later on after installing. Why? Users are more likely to trust an extension with limited warnings or when permissions are explained to them.

But what is the use of these informative prompts if they only give you half the story? In this case, the PopStop extension doesn't just read your browsing history, as the pop-up explains, but it also hijacks your search results.

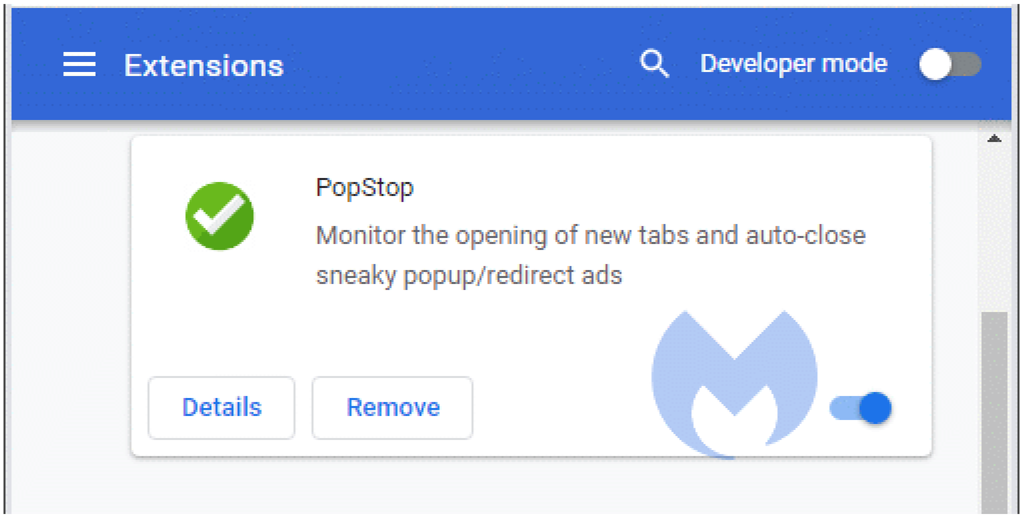
Some of these extensions are more straightforward once the user installs them and they are listed under the installed extensions.



Niux APP

This extension configures your default Search Engine to the more advanced s3redirect.com

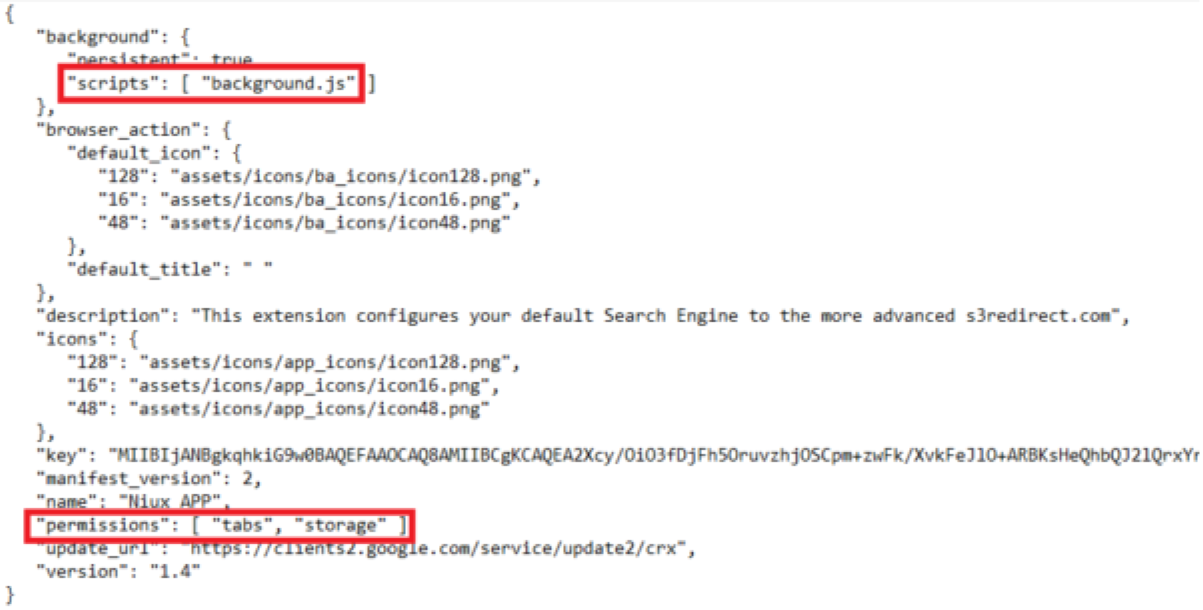
But others are consistent in their lies even after they have been installed, which makes it even harder to find out which one is responsible for the search hijack.


Extensions
Developer mode
PopStop
Monitor the opening of new tabs and auto-close sneaky popup/redirect ads
Details
Remove

How is this possible?

Google had at some point decided to bar extensions that obfuscate their code. By doing so, it's easier for them to read the plug-in's programming and conduct appropriate analysis.

The first step in determining what an extension is up to is in looking at the manifest.json file.



```
{
   "background": {
      "persistent": true,
      "scripts": [ "background.js" ]
   },
   "browser_action": {
      "default_icon": {
         "128": "assets/icons/ba_icons/icon128.png",
         "16": "assets/icons/ba_icons/icon16.png",
         "48": "assets/icons/ba_icons/icon48.png"
      },
      "default_title": " "
   },
   "description": "This extension configures your default Search Engine to the more advanced s3redirect.com",
   "icons": {
      "128": "assets/icons/app_icons/icon128.png",
      "16": "assets/icons/app_icons/icon16.png",
      "48": "assets/icons/app_icons/icon48.png"
   },
   "key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2Xcy/Oi03fDjFh5OruvzhjOSCpm+zwFk/XvkFeJ1O+ARBKsHeQhbQJ21QrxYr
   "manifest_version": 2,
   "name": "Niux APP",
   "permissions": [ "tabs", "storage" ],
   "update_url": "https://clients2.google.com/service/update2/crx",
   "version": "1.4"
}
```

Registering a script in the manifest tells the extension which file to reference, and, optionally, how that file should behave.

What this manifest tells us is that the only active script is "background.js" and the declared permissions are "tabs" and "storage". More about those permissions later on.

The relevant parts in background.js are these pieces, because they show us where our searches are going:

```
const BASE_DOMAIN = 's3redirect.com', pid = 9126, ver = 401;
chrome.tabs.create({url: `https://${BASE_DOMAIN}/chrome3.php?q=${searchQuery}`});
        setTimeout(() => {
          chrome.tabs.remove(currentTabId);
        }, 10);
```

This script uses two chrome.tabs methods: One to create a new tab based on your search query, and the other to close the current tab. The closed tab would have displayed the search results from your default search provider.

Looking at the chrome.tabs API, we read:

> “You can use most chrome.tabs methods and events without declaring any permissions in the extension’s manifest file. However, if you require access to the url, pendingUrl, title, or favIconUrl properties of tabs.Tab, you must declare the “tabs” permission in the manifest.”

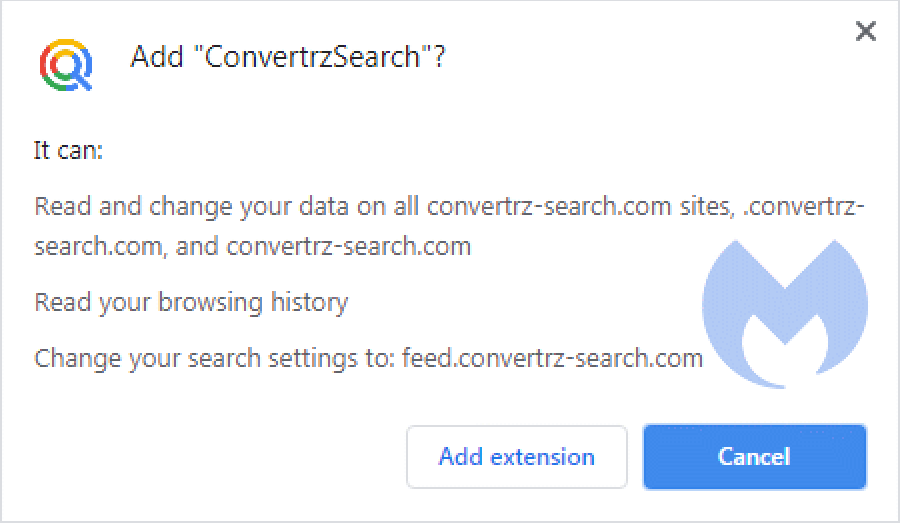
And indeed, in the manifest of this extension we found:

```
"permissions": [ "tabs", "storage" ],
```

The “storage” permission does not invoke a message in the warning screen users see when they install an extension. The “tabs” permission is the reason for the “Read your browsing history” message. Although the chrome.tabs API might be used for different reasons, it can also be used to see the URL that is associated with every newly-opened tab.

The extensions we found managed to avoid having to display the message, “Read and change all your data on the websites you visit” that would be associated with the “tabCapture” method. They did this by closing the current tab after capturing your search term and opening a new tab to perform the search for that term on their own site.

The “normal” permission warnings for a search hijacker would look more similar to this:



Add "ConvertrzSearch"?

It can:

Read and change your data on all convertrz-search.com sites, .convertrz-search.com, and convertrz-search.com

Read your browsing history

Change your search settings to: feed.convertrz-search.com

The end effect is the same, but an experienced user would be less likely to install this last extension, as they would either balk at the permission request or recognize the plug-in as a search hijacker by looking at these messages.

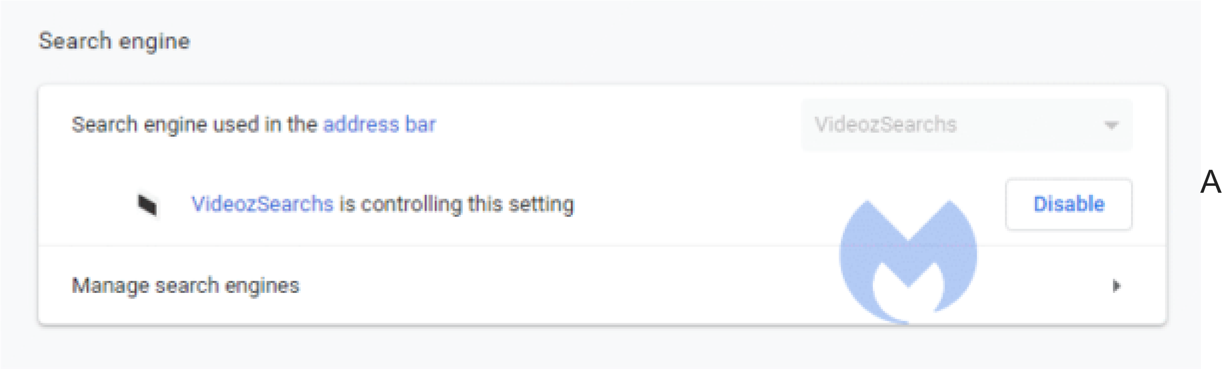
Are these extensions really lying?

Some might call it a lie. Some may say no, they simply didn't offer the whole truth. However, the point of those permissions pop-ups is to give users the choice on whether to download a program by being upfront about what that program asks of its users.

In the case of these Chrome extensions, then, let's just say that they're not disclosing the full extent of the consequences of installing their extensions.

It might be desirable if Google were to add a possible message for extensions that use the chrome.tabs.create method. This would inform the user that his extension will be able to open new tabs, which is one way of showing advertisements so users would be made aware of this possibility. And chrome.tabs.create also happens to be the method that this extension uses to replace the search results we were after with their own.

An additional advantage for these extensions is the fact that they don't get mentioned in the settings menu as a "regular" search hijacker would.



Search engine

Search engine used in the address bar: VideozSearchs

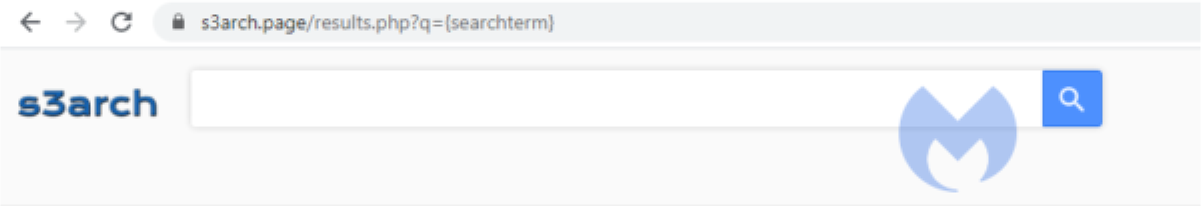
VideozSearchs is controlling this setting

Manage search engines

A search hijacker that replaces your default search engine would be listed under Settings > Search engine

Not being listed as the search engine replacement, again, makes it harder for a user to figure out which extension might be responsible for the unexpected search results.

For the moment, these hijackers can be recognized by the new header they add to their search results, which looks like this:



s3arch.page/results.php?q={searchterm}

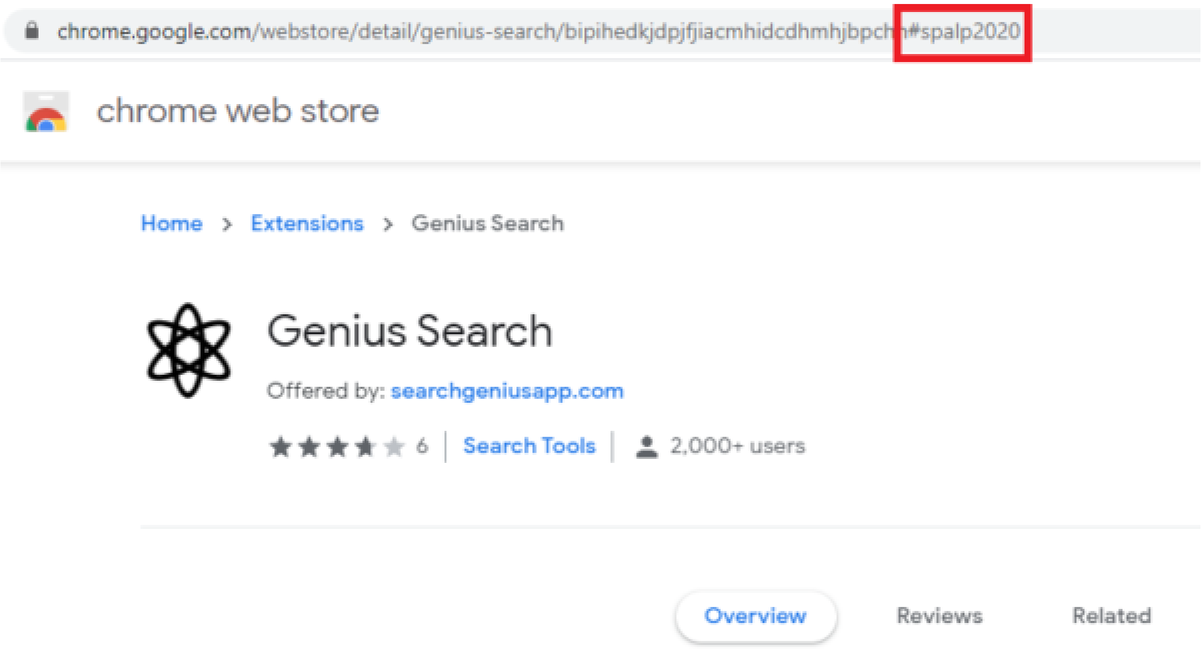
This will probably change once their current domains are flagged as landing pages for hijackers, and new extensions will be created using other landing pages.

Further details

These extensions intercept search results from these domains:

- aliexpress.com
- booking.com
- all google domains
- ask.com
- ecosia.org
- bing.com
- yahoo.com
- mysearch.com
- duckduckgo.com

It also intercepts all queries that contain the string “spalp2020”. This is probably because that string is a common factor in the installer url’s that belong to the powerapp.download family of hijackers.



chrome.google.com/webstore/detail/genius-search/bipihedkjdpjfjiacmhidcdhmhjbpchn#spalp2020

Search hijackers

We have written before about the interests of shady developers in the billion-dollar search industry and reported on the different tactics these developers resort to in order to get users to install their extensions or use their search sites[1],[2],[3].

While this family doesn't use the most deceptive marketing practices out there, it still hides its bad behavior in plain sight. Many users have learned to read the install prompt messages carefully to determine whether an extension is safe. It's disappointing that developers can evade giving honest information and that these extensions make their way into the webstore over and again.

IOC's

extension identifiers:

pcocncapgaibfcjmkkalopefmmceflnh

dpnebmclcgcbggnhicpocghdhjmdgklf

search domains:

s3redirect.com

s3arch.page

gooogle.page <= note the extra "o"

Malwarebytes detects these extension under the detection name PUP.Optional.SearchEngineHijack.Generic.

Stay safe, everyone!