Weknow.ca virus, Browser hijacker

Jorge Davila - 2018-10-15 - Comments (0) - Antivirus and Malware

This article is specifically for the Browser Hijacker "Weknow.ca"

It changes your browser default search engine to the image below and it does not let you change it back.

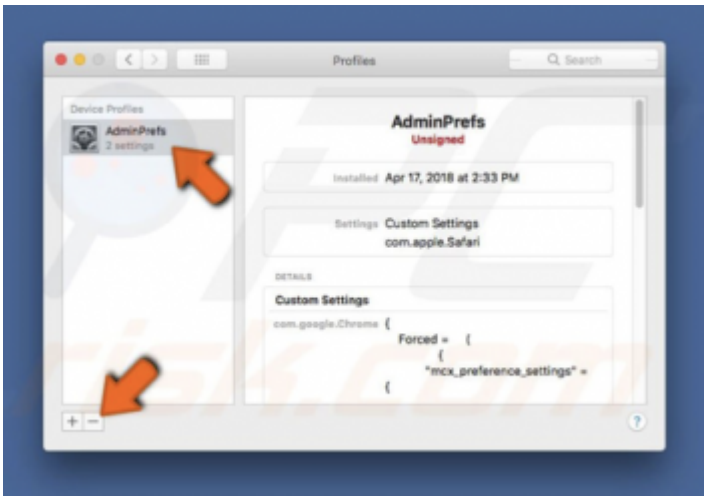
It takes over your browser (primarily google chrome) and it does not let you change the default search engine.

Similar to chumsearch.com, weknow.ac is a fake web search engine that supposedly enhances the browsing experience by generating improved results. Judging on appearance alone, weknow.ac may seem legitimate and useful, however, this site is promoted using rogue download/installation set-ups that modify browser options without permission. Furthermore, weknow.ac continually records information relating to users' Internet browsing activity.

The best approach I have tried that has the best results to fully remove it, is this.

I first go to System preference and click on profile.

At most times, you will find the AdminPrefs Profile on the list with 2 Certificates.



Then, I removed all this files, and all core google / safari folders.

Close/Quit your Chrome browser, then double check w/ Activity Monitor (in Utilities) - ensure that non Google or Chrome related processes are still running in background.

Remove your Chrome for Mac fully, via Terminal (in Utilities). To do so, run the following commands as admin (copy then paste - keep in mind that you may need to run the following commands several times):

(I went directly to the folders and got rid of everything to make sure)

cd Library/

cd Application\ Support/

cd Google

(Then...)

rm -r /Applications/Google\ Chrome.app/

rm -r ~/Library/Application\ Support/Google/Chrome/

rm ~/Library/Application\ Support/CrashReporter/Google\ Chrome*

rm ~/Library/Preferences/com.google.Chrome*

rm ~/Library/Preferences/Google\ Chrome*

rm -r ~/Library/Caches/com.google.Chrome*

rm -r ~/Library/Saved\ Application\ State/com.google.Chrome.savedState/

rm ~/Library/Google/GoogleSoftwareUpdate/Actives/com.google.Chrome

rm ~/Library/Google/Google\ Chrome*

rm -r ~/Library/Speech/Speakable\ Items/Application\ Speakable\ Items/Google\ Chrome/

I found all this information in the web, but the best option I found here.

https://productforums.google.com/forum/#!topic/chrome/Vr0sf_NYNuE

I did not do step 8, since after removing all those files and rebooting the computer, I reinstalled Chrome and the problem was solved.

For information on how to remove it on a Windows base system, follow the link below.

https://malwaretips.com/blogs/remove-weknow-ac