
## C’est quoi le „hostfile hijacking“ ?

Si votre antivirus et/ou autre logiciels de sécurité ne fonctionnent plus, les chances que vous êtes devenus victime d’un „**Hostfile Hijacking“** sont grandes.

Le fichier „**hosts“** a été manipulé, ce qui permet à l’attaquant de bloquer les mises à jour des logiciels de sécurité !

Sous **Windows® XP** vous pouvez vérifier à l’emplacement „**C:\Windows\System32\Drivers\etc“** s’il y a eu manipulation de ce fichier.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

Vous pouvez ouvrir ce fichier avec **l’éditeur de texte** (**Notepad**). En principe il ne doit figurer qu’une seule entrée, le „**localhost“** qui a **l’adresse IP „127.0.0.1“**.

Au cas où vous trouveriez d’autres entrées dans ce fichier, vous avez tout intérêt de faire une copie de ce fichier, d’enlever les entrées superflues et de remplacer le fichier par celui que vous venez d’éditer et qui ne contient que l’entrée du « localhost » et puis de redémarrer votre ordinateur ! Puis réessayez si les mises à jour fonctionnent à nouveau. Bonne chance !

Afin de vous munir contre une telle attaque, il existe aussi un logiciel gratuit „**Browser Hijack Retaliator“**.

**„Browser Hijack Retaliator“** peut être téléchargé à l’adresse URL
http://www.zamaansoft.com/products/bhr/index.php.

Copyright © by Gust MEES (LU)


**Browser Hijack Retaliator :**

Cet utilitaire est très simple à manier. Une fois téléchargé il travaille en arrière plan et il devient actif dès que vous lancez Internet Explorer.
Il présente aussi d’autres fonctionnalités telles que :

- Programmes ouverts au démarrage.
- Indication des „**BHO“** (**Browser Helper Objects** ». Les “**BHO**” sont des utilitaires d’aide pour le navigateur, comme par exemple la „**Google tool bar**“.

Après le téléchargement du logiciel lancez-le et cliquez sur le bouton „**HOSTS File“**. L’écran ci-dessus s’affiche, montrant les fichiers hosts dans la fenêtre blanche. Fermez-le logiciel au cas où il n’y aurait que „**127.0.0.1“** d’affiché, comme montré dans a figure ci-dessus, tout est correct. Au cas où vous trouveriez plus d’un fichier, il faudra restaurer ce fichier. Pour ce faire, cliquez sur le bouton „**Restore“**. L’utilitaire restaurera le fichier et le remet dans son état d’origine. Fermez le logiciel maintenant.

Il contrôlera en arrière plan les actions sur Internet et vous êtes protégés contre les **détournements de votre navigateur** (**browser hijacking**).

Copyright (C) by Gust MEES (LU)