C’est quoi le „hijacking“ ?

On parle de plus en plus de „**browser hijacking**“, mais c’est quoi au fait ? Bien entendu les deux mots viennent de l’anglais et signifient :

- **browser** = navigateur, fureteur (Internet Explorer, Firefox, Netscape, Opera, etc.)
- **hijacking** = détournement.

„**Browser hijacking**“ par conséquence veut dire, ***détournement du navigateur***. Lorsque vous ouvrez votre navigateur pour aller surfer sur Internet, votre navigateur s’ouvre avec une page de démarrage spécifique. Cette page de démarrage reste en principe toujours la même. Si vous utilisez **Internet Explorer** c’est par conséquent le site Internet de **MSN®** qui s’ouvre pour **Firefox®** c’est la page de **Mozilla®**. Mais cette page de démarrage peut être aussi échangée par une autre adresse URL, soit que c’est vous qui la prédéfinissez ou bien elle sera changée par un script malicieux qui s’est installé sur votre ordinateur. Si soudainement votre page de démarrage a changé et que vous êtes dirigé envers un site Internet douteux, c’est que vous êtes victime d’un „**browser hijacking**“, d’un détournement de votre navigateur.

Comment devenir victime ?

Quand vous utilisez l’échange de fichiers, dit le **P2P** (**peer to peer**), ou disons plutôt „**de pire en pire**“, vous vous exposez à des risques de contamination informatique assez sévères. Télécharger des logiciels et/ou des fichiers de musique et de vidéo gratuits sur ces plateformes d’échange de fichiers (P2P) n’est pas toujours légal (dépendant du pays), mais cache aussi des risques informatiques pour votre ordinateur. La plupart des serveurs **P2P** sont contaminés avec des ***spyware, adware et autres malware qui ne veulent rien d’autre que d’infecter votre machine et en prendre le contrôle.*** Vous pouvez aussi attraper cette malware en vous baladant sur des sites Internet douteux et à caractère pornographique (xxx), etc.

Évitez de visiter des sites Internet se terminant avec un „**z**“; par exemple :

Newz, warez, gamez, serialz, goodz, etc.

Lire aussi les articles suivants :

- Spyware c’est quoi ?
  http://www.internetmonitor.lu/Spyware-FR-_a406.html

- Installation d’antispywares
  http://www.internetmonitor.lu/Spyware-FR-_a415.html

- PC-zombie
  http://www.internetmonitor.lu/Demantelement-d-un-reseau-de-10-000-PC-zombies_a354.html

- KaZaa
  http://www.internetmonitor.lu/Kazaa-classe-comme-le-logiciel-espion-le-plus-menacant_a467.html

- http://www.internetmonitor.lu/Kazaa-45-des-fichiers-executables-seraient-infectes_a155.html

- Vade-mecum de la sécurité
  http://www.internetmonitor.lu/Le-vade-mecum-de-la-Securite-PC-Internet_a616.html

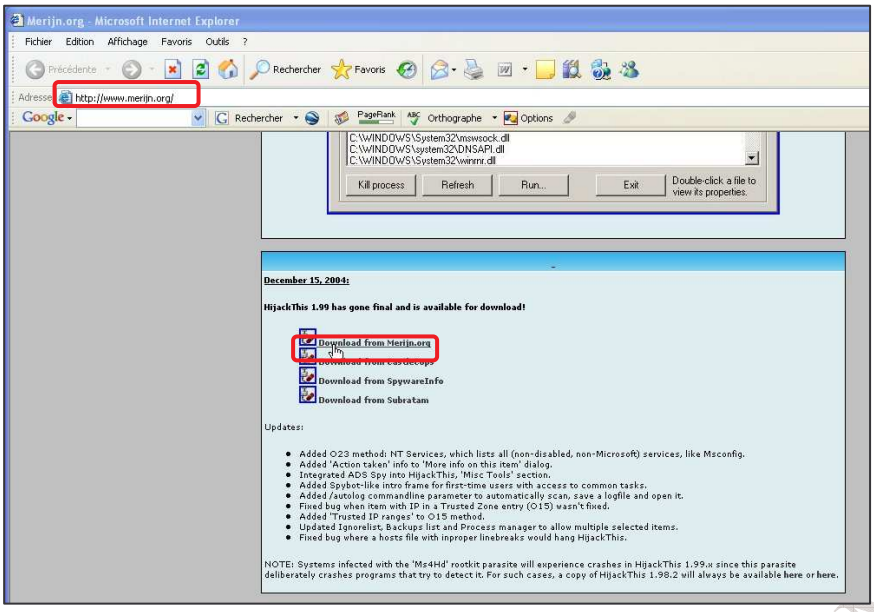
- Pratique de la sécurité
  http://www.internetmonitor.lu/Pratique-Securite-PC-Internet_a659.html

Quand votre navigateur a été détourné, il vous emmène en principe sur un site Internet qui vous propose de télécharger un logiciel antiespion payant en vous disant que votre ordinateur est contaminé et/ou vous êtes dirigés envers des sites douteux…

Surtout ne téléchargez pas ces logiciels, soyez méfiants. Ces logiciels contiennent eux-mêmes des malware. Avant de télécharger un logiciel antispyware vérifiez à l’adresse suivante s’il n’est pas douteux, par hasard :

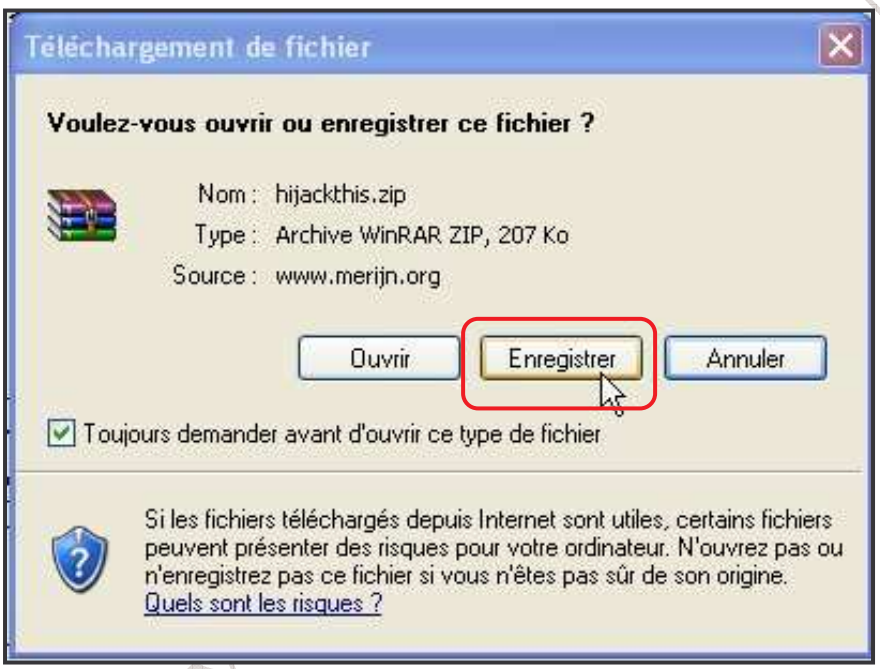
SPYWARE WARRIOR : http://www.spywarewarrior.com/rogue_anti-spyware.htm.

Comment se débarrasser des „hijacker“ ?



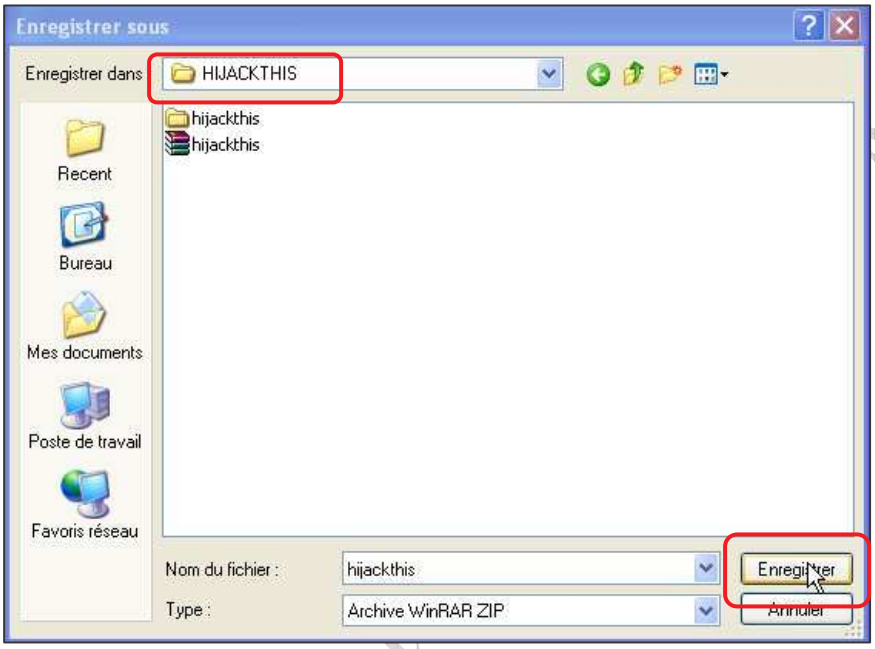
Connectez-vous à Internet et choisissez l’adresse URL suivante : www.merijn.org.

La fenêtre ci-contre s’ouvrira. Recherchez l’utilitaire „**HijackThis“**. Cliquer sur le lien „**Download from Merijn.org“**.

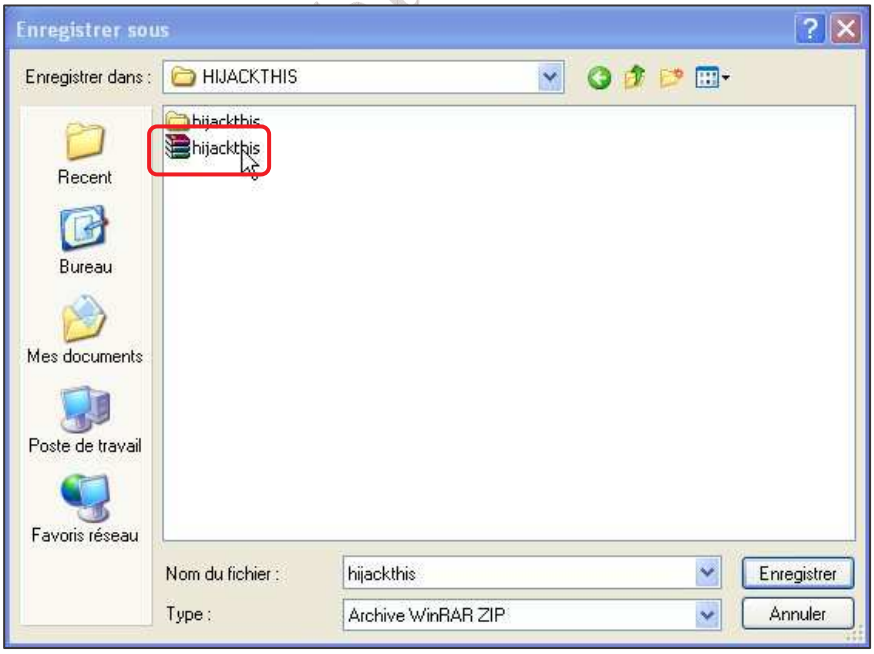


La fenêtre ci-contre s’affiche. Cliquer sur le bouton „**Enregistrer**“.

La boîte de dialogue ci-contre s’affiche montrant le progrès du téléchargement avec une barre graphique. Le téléchargement terminé, cliquez sur le bouton „**Ouvrir**“.

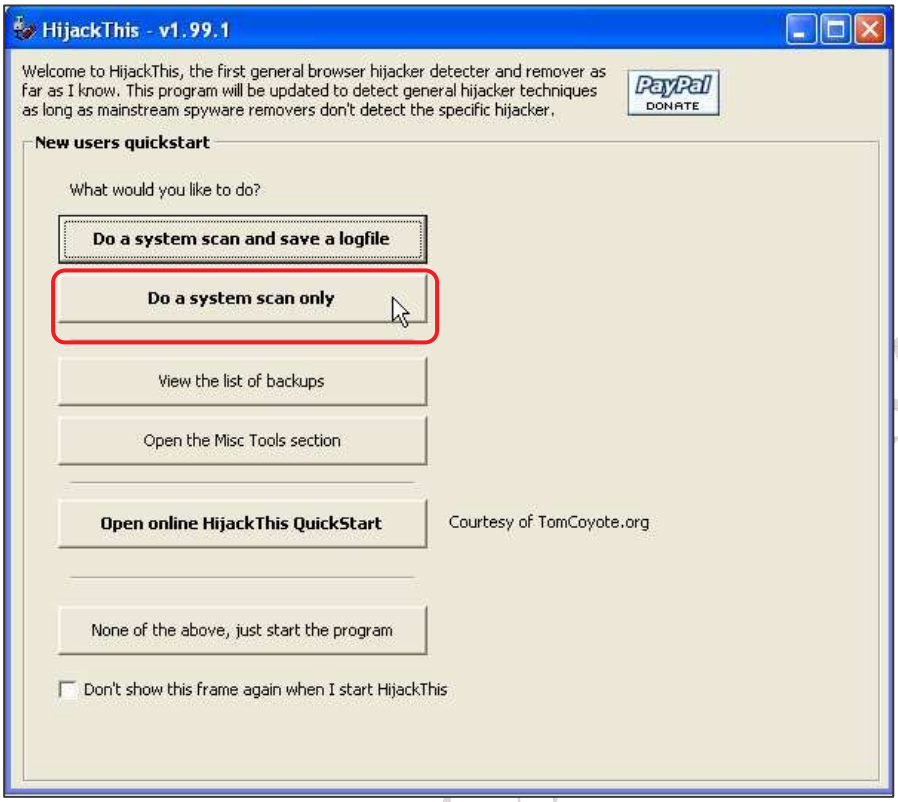


Créez un dossier, libellé avec „**HIJACKTHIS**“ et enregistrez le téléchargement. Cliquer sur le bouton „**Enregistrer**“.

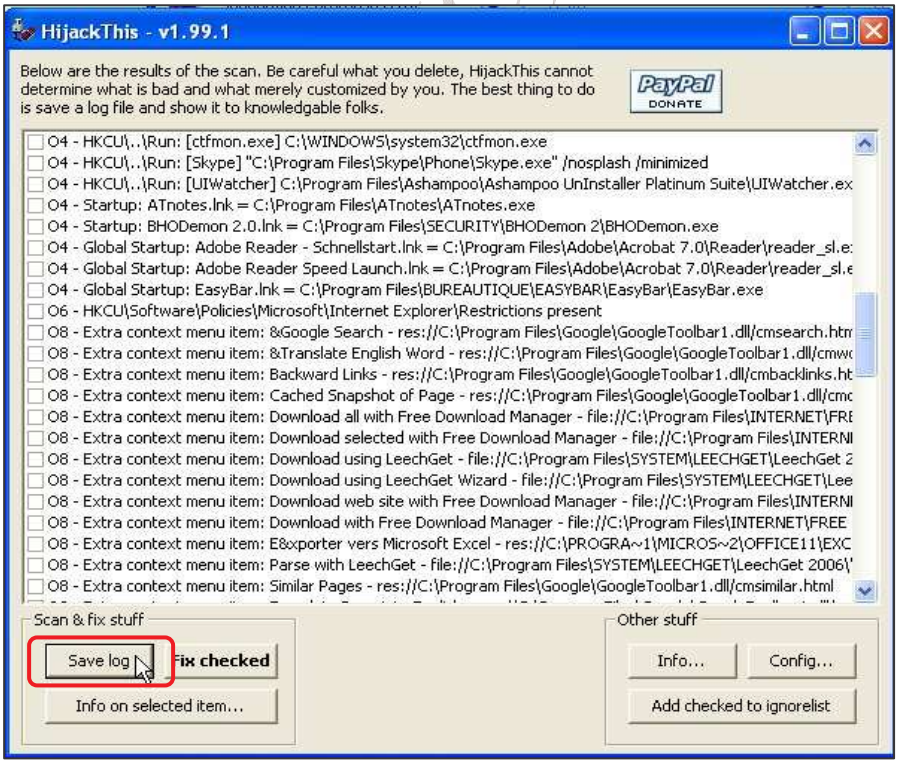


La fenêtre ci-contre s’affiche. Double-cliquer le fichier zippé (compressé).

Après avoir décompressé le fichier dans le dossier prévu, ouvrez le dossier. Double-cliquer sur l’icône montrée ci-contre.

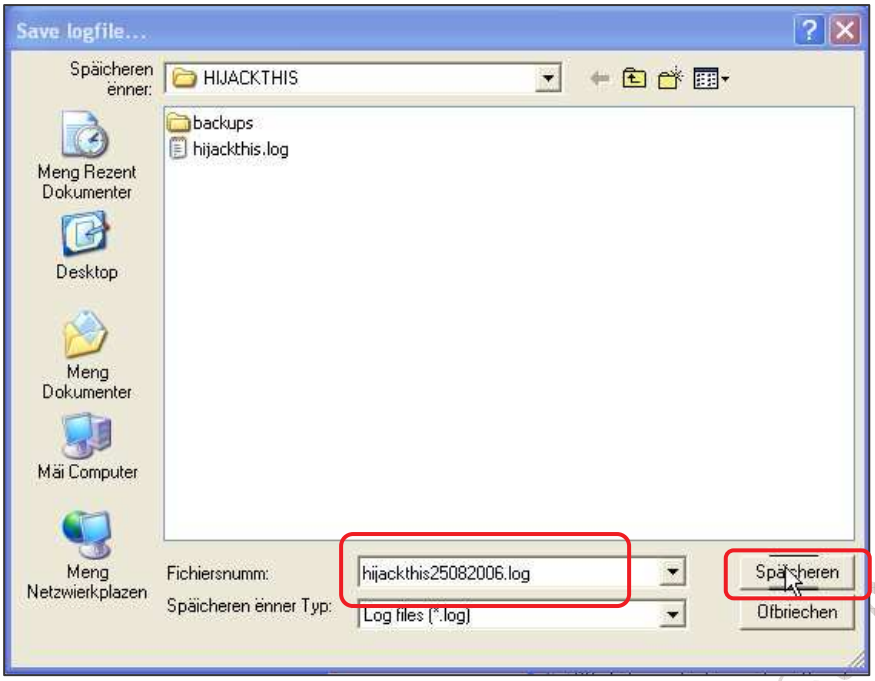


La boîte de dialogue ci-contre s’affiche. Cliquer sur le bouton „**Do a system scan only“**.



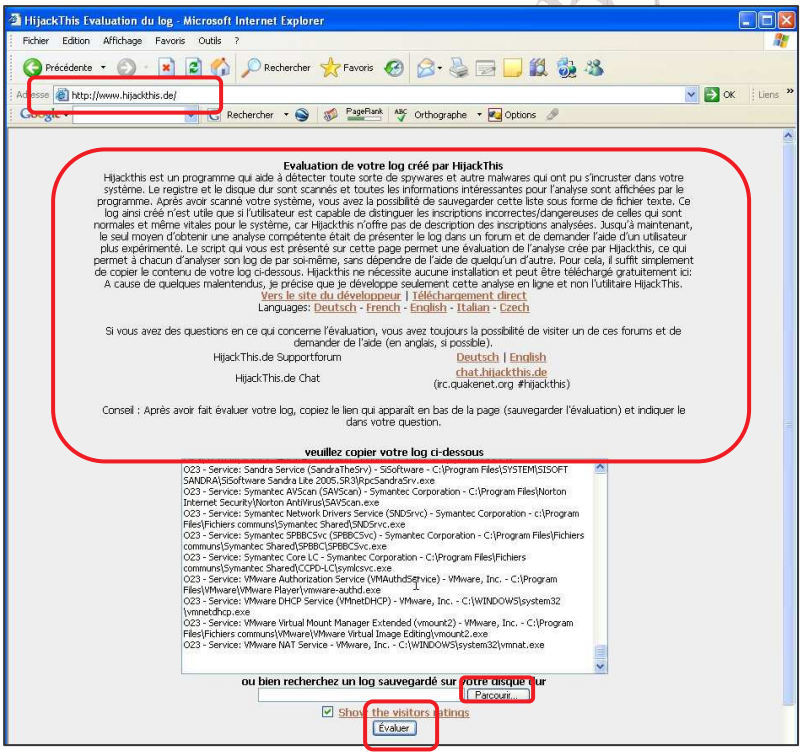
La fenêtre ci-contre s’affiche vous montrant les détails du scan. Cliquer sur le bouton „**Save log“**.

Surtout ne faites aucune autre manipulation, sauf si vous êtes expert et que vous reconnaissez vous-même quels sont les éléments nuisibles à éradiquer !



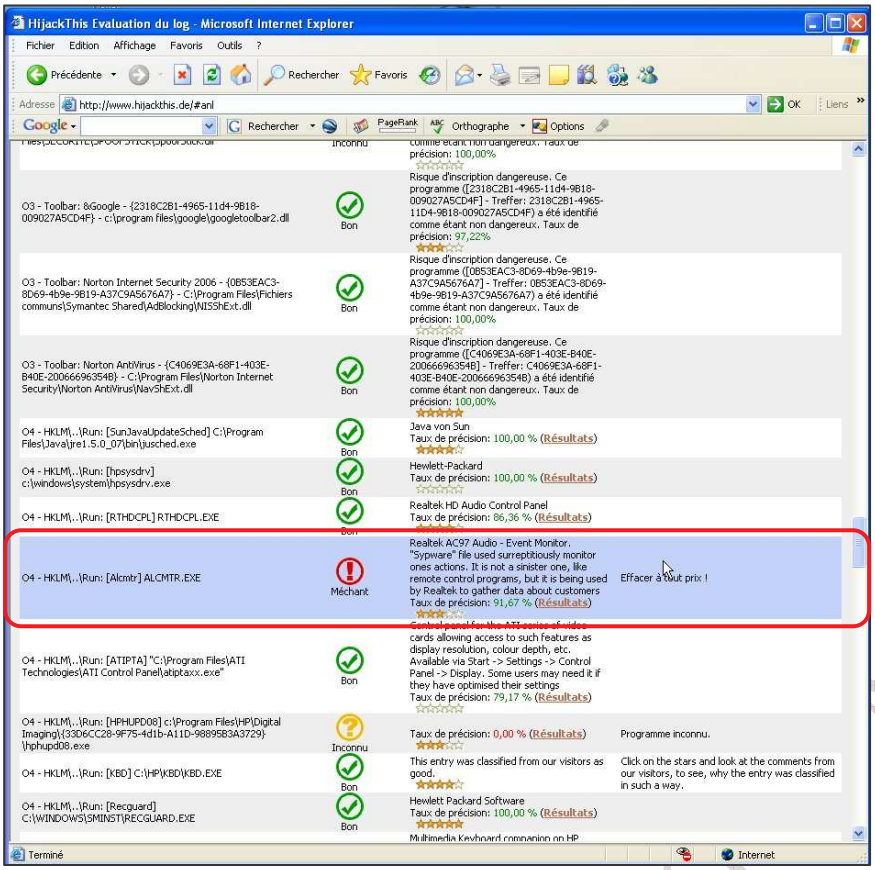
La fenêtre ci-contre s’affiche. Libeller l’enregistrement avec la date comme montré ci-contre. Cliquer sur le bouton „**Enregistrer**“.

La première phase de détection d’un „**browser hijacking**“ est terminée. Vous avez fait un scan complet de votre ordinateur et vous avez enregistré son contenu. Maintenant il faut encore déchiffrer le contenu du scan. Pour ce faire, connectez-vous par connexion Internet à l’adresse URL suivante : http://www.hijackthis.de.



La fenêtre ci-contre s’ouvre avec un explicatif en détail comment procéder.

Cliquer sur le bouton „**Parcourir**“ et choisissez le lieu d’emplacement de votre log. Dans notre exemple ci-dessus, **„Mes documents/HIJACKTHIS/hikackthis25082006.log**“. Cliquer ensuite sur le bouton „**Évaluer**“.



La fenêtre ci-contre s’affiche, vous expliquant les résultats obtenus et comment procéder.

Voilà, vous êtes maintenant assuré et/ou bien rassuré d’avoir attrapé une de ces bestioles informatiques les plus coriaces à enlever. Avec ce petit utilitaire gratuit vous saurez maintenant comment y procéder.