Date: Lundi 04 octobre 2004 à 22:15:37
Sujet: 3 Sécurité et Hacking

Trojan Bootconf , Trojan.Qhosts.A, Search the Web ou Globefinder

Comment se débarasser de ces trojans.

Je vais vous expliquez comment vous débarasser du Trojan.Bootconf, Qhosts.A, Qhosts.B, TrojanClicker.Win32 qui connu sous de nombreux nom différents.

Vous pouvez facilement savoir si vous êtes infecté par ce trojan car il remplace votre page d'accueil par une autre, souvent "Search the Web" ou "Globefinder".

Vous aurez beau rétablir votre anicenne page d'accueil , au lancement suivant elle aurat de nouveau été remplacée.

Certaines personnes auront aussi une barre de recherche assez gênante.

Beaucoup de personne on étaient contaminées en installant MSN Plus, pendant l'instalation, il vous est demandé si vous voulez installé le programme publicitaire de MSN Plus, la plupart des personnes qui ont acceptées n'ont pas fait attention ce qui a entrainé l'insatllation de nombreux spywards sur leur PC.

Pour éradiquer ce troyen il y a plusieurs solutions, vous pouvez insatller un bon anti-virus qui se chargera de l'effacer, mais cela ne marchera pas forcément.

C'est pourquoi je vous conseille de suivre ces instructions pour l'effacer de votre disque dur définitivement.

1. Allez dans "Démarrage", puis sur "Exécuter", taper "Regedit" et accepter.

Ouvrir la route suivante En HKEY_CURRENT_USERSoftwareMicrosoftInternet Explorer et supprimer les registres suivants:

Search = http://%6f%75%74%2e%74%72%75%65%2d% [etc.]

SearchURL = http://%6f%75%74%2e%74%72%75%65%2d%63 [etc.]

Faire de même avec dans HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerSearch :

SearchAssistant = http://%6f%75%74%2e%74%72%75 [etc.]

CustomizeSearch = http://%6f%75%74%2e%74%72%75 [etc.]

Dans HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerMain

Search Page = http://%6f%75%74%2e%74%72%75%65 [etc.]

Default_Search_URL = http://%6f%75%74%2e%74%72 [etc.]

Search Bar = http://%6f%75%74%2e%74%72%75%65%2d [etc.]

Default_Page_URL = http://%6f%75%74%2e%74%72%75 [etc.]

Start Page = http://%6f%75%74%2e%74%72[etc.] about:blank

Dans HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerStyles
User Stylesheet = c:windowsWeboslogo.bmp
Use My Stylesheet = "1"

Faire la même chose dans HKEY_LOCAL_MACHINE.

2. Allez dans "Démarrage", puis "Exécuter", tapez "msconfig".
Dans la listede l'onglet "Démarrage" désactiver (décochez) "Internat.Conf" : C/Windows/System/bootconf.exe" (Si l'antivirus ne l'a déjà fait).

3. Supprimer ce fichier dans sa localisation C:/Windows/System (Si l'antivirus ne l'a déjà fait)

4. Supprimer C:/Windows/web/oslogo (Si l'antivirus ne l'a déjà fait)

5 . Supprimer C:/Windows/hosts.. Fichier (Attention Ne pas supprimer son homonyme hosts..Fichier Sam)

6 . Rétablir vos paramètres Internet et supprimer une fois pour toute la feuille de Style Windows/web/oslogo"

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=13