

MARC BLANCHARD VIRUS DOCTEUR

[ALERTE] Un vers se propage sur le réseau Skype et sa VoIP

ALERTE Un vers se propage sur le réseau Skype et sa VoIP

Les noms de ce vers varient selon les éditeurs AV, Skipi chez Kaspersky, se propage sous forme de messages provenant du carnet d'adresse des utilisateurs skype infectés.

Arrivée du malware

Le worm arrive si les utilisateurs de Skype recevant ces messages ayant des liens sur lesquels une image érotique peut être téléchargée.

Activation du malware :

L'activation se fait des téléchargements d'une de ces images, qui en fait est un fichier JPG.SCR. L'extension SCR, selon les operating systems est cachée.

Si l'utilisateur clique sur le bouton "OUVRIR", l'infection de la machine commence, car le vers utilise l'API de skype.

Si l'utilisateur a son Skype de lancé, le vers enverra ses liens sous forme de messages (au nom de la personne infectée) à tout le carnet d'adresse Skype du poste.

Méthode d'infection :

Des que le code est exécuté, il copie ces fichiers dans le répertoire \Windows\System32 :

```
winlgcvers.exe mshtmlat32.exe wndrivr32.exe sdrivew32.exe
```

Il patche les clefs de registres :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
```

Deux clefs sont créées :

HKEY_CURRENT_USER\Software\RMX

HKEY_LOCAL_MACHINE\SOFTWARE\RMX

Le vers télécharge son code sur les sites suivants :

cpa-site.com lookingat.us www.freewebs.com www.gamesforum.com www.kale45.php0h.com
4444mb.com zopa.110mb.com mylawsite.net attorney-site.com ragezone.com blog.co.uk
kupralana77.110mb.com members.lycos.co.uk ragai.myartsonline.com bedclip.com
alladultmale.com

Technologie de retrovirus :

Afin de ne pas être détecté, et lui permettant de changer son propre code malicieux à volonté, le vers patche le fichier HOSTS tous les sites des serveurs de mises à jour des antivirus les plus connus.

Nota : Ce fichier doit être, en théorie, vide de nom de domaines.

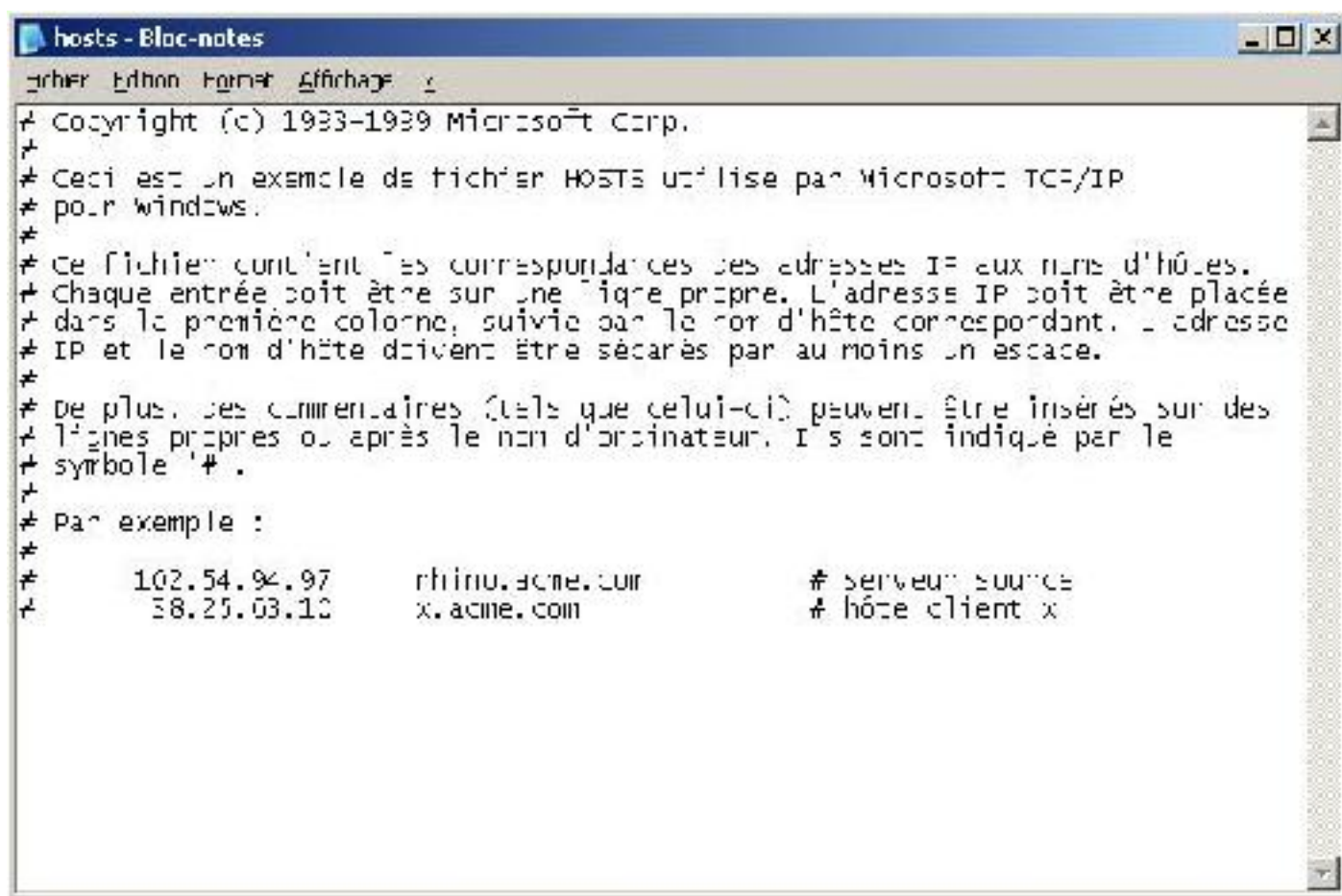
Recommandation :

Forcez les mises à jour des bases antivirales.

Si l'antivirus refuse de se mettre à jour :

- Ouvrez notepad puis accédez au fichier HOSTS situé dans c:\windows\system32\drivers\etc
- effacez les noms de domaines inscrits dans ce fichier

Voici pour exemple un fichier hosts sain :



```
hosts - Bloc-notes
-----
* Copyright (c) 1993-1999 Microsoft Corp.
*
* Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP
* pour Windows.
*
* Ce fichier contient les correspondances des adresses IP aux noms d'hôtes.
* Chaque entrée doit être sur une ligne propre. L'adresse IP doit être placée
* dans la première colonne, suivie par le nom d'hôte correspondant. L'adresse
* IP et le nom d'hôte doivent être séparés par au moins un espace.
*
* De plus, des commentaires (tels que celui-ci) peuvent être insérés sur des
* lignes propres ou après le nom d'ordinateur. Ils sont indiqués par le
* symbole '#'.
*
* Par exemple :
*
*      102.54.94.97      rhino.acme.com      # serveur source
*      38.25.63.12      x.acme.com        # hôte client x
```

- Relancez la mise à jour de votre antivirus

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-11 19:27:04
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>