

# MARC BLANCHARD VIRUS DOCTEUR

## Les éditeurs Antivirus ciblés par les attaquants..mauvais signe!

Le 7 février 2009 : Kaspersky subit une attaque sur son site USA, et les bases antivirales innaccessibles pendant plus de 1h30

Le 9 février 2009 : BitDefender subit également une attaque.

Le 11 février 2009, c'est le tour de F-Secure.

Tout cela me laisse penser qu'il s'agit d'une guerre que commencent les cyber delinquants contre les seuls freins : les éditeurs d'antivirus.

Il faut dire que ces derniers temps, les cyber-délinquants n'y vont pas de main morte. Si on prend quelques exemples dont on ne parle pas en presse, car les alertes virus semblent ne plus intéresser personne, ceci dit, elles continuent de plus en plus.

Nous subissons la guerre du numérique, et personne ne semble réagir, ormis notre gouvernement qui a quand même mis la main à la poche pour lutter contre ce cyber-terrorisme.

En exemple, on nommera le Confiker (Autorunner.5555), les DNS changers (vous croyez être sur un site, vous êtes sur un autre, et un pirate vous espionne), Poison.51 qui met en marche la webcam et le microphone de ses victimes en y ajoutant un key logger sophistiqué qui prend les abscisses et les ordonnées des clics de souris que l'internaute effectue et audite tout ce que la victime tape au clavier (et si un clavier virtuel est lancé, la code malicieux prend une image), Virut qui lui fait son petit chemin de propagation pour affecter ses victimes dans un réseau zombie de grande ampleur, etc, bref de petites vermines qui font bien des déboires, pour au final, un seul résultat : l'appât du gain ! C'est bien connu, celui qui a le gain et la maîtrise peut provoquer ce qu'il souhaite....

Il est clair que la réactivité des antivirus sur les mises à disposition des antidotes inquiètent les cyber-delinquants. Il leur faut développer des freins.

Alors que certains éditeurs d'antivirus optent leurs technologies et leurs publicités sur le 'CLOUDING' (envoi des fichiers des utilisateurs sur des serveurs antivirus sur internet pour les analyser en temps réel), les dernières attaques des éditeurs antivirus démontrent bel et bien que le clouding ou le management des flux internet déportés chez un tiers, qui n'est que ni plus ni moins l'éditeur antivirus, est très dangereux.

C'est ce que j'expliquais dans un de mes posts sur le bon choix d'un antivirus ;-) )

Bref, les freins dont je parle, sont relativement simples :

a. Les codes malicieux qui déroutent les DNS soit sur le 127.0.0.1 soit sur un serveur internet qui ne contient que des données notamment des fichiers très anciens des antidotes des éditeurs antivirus

**Résultat** : pas de mise à jour

**Conséquence** : liberté pour le cyber-délinquant de publier ses malwares qui ne seront détectés que bien plus tard.

b. Utilisant la même technique, éviter que les systèmes Windows, linux ou autre ne se mettent à jour pour palier aux failles de sécurités de l'OS.

c. S'attaquer à la source : c'est à dire mettre un cyber-désordre chez les éditeurs antivirus, firewall, antispam, etc, afin de rendre inaccessible les sites de mises à jour.

A ce niveau, il faut s'inquiéter.

C'est pourquoi, certains éditeurs, qui utilisent des techniques de mises à jours moins sophistiquées que par exemple le clouding ou les services managés, se retrouvent beaucoup moins vulnérables, car il démultiplient leurs serveurs de mises à jour, changent les adresses IPs plus que régulièrement, ainsi que les noms DNS, permettant ainsi un risque bien moins grand.

Copyright : Blanchard [Virus Docteur] Marc - 2009-02-14 00:04:52  
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/>