

MARC BLANCHARD VIRUS DOCTEUR

17th september 2009 : Isomorphic behaviors

Isomorphic behaviors :

On XP:

Time : 00:05

No activity confirmed

Reboot

Relaod MAP

Reload Network Analyzer

No Scheduled taks were created or modified.

No activities on mutex processes or registries or files creation / modification

Reinjection of sample.

"NOTA : It seems that for few second, the sample stays on /WINDOWS/SYSTEM32 and is deleted after its injection on the system to be on active activities (only in RAM)."

On WIN2003:

The activity seems stabilized and proceed to infection and get external sites / Internal network each 2 hours.

No file were modified or created on the system, the infection is active in RAM

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-19 13:10:50
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/>