

MARC BLANCHARD VIRUS DOCTEUR

25th September 2009 - Isomorphic external behavior

The 25th morning, one of my diagnosticians called me to inform me a strange behavior on several networks.

The behavior is on each network computer:

- Local DNS down : mean that computers cannot go anymore to the internet because their DNS is 127.0.0.1
- IPCONFIG : shows errors and doesn't accept any arguments
- NSLOOKUP : also fails.
- No scheduled tasks created usually by the worm
- No rootkit
- Some plug&play drivers are loaded with NT_AUTHORITY and processes dependencies are showed.
- The network computers could goes to the net with dns name of sites, but could go with true IP Addresses.

If we try to stop or delete or just copy, the worm reacts by a blue screen or reboot

So, we decided to make some audits of these computers to check their behaviors. To be more sure concerning the results that we will get, we ask to 3 differents companies do let us to make researches and behavior analysis.

We decided to take a family as following:

- 1 WIN2008
- 1 XPSP3
- 1 XPSP2
- 1 WIN2003

All of these computers OS's are with latest MS patches including the MS09-01

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-28 20:00:05
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/>