

MARC BLANCHARD VIRUS DOCTEUR

15th sept 2009 : Isomorphic behaviors

On XP:

Isomorphic behaviors :

At 04:15, a new DLL was pushed without any approval of me or OS notification on the /windows/system32 to the system detected as C or D variant

No trace on registries. Seem to be used by the active infection in memory.

Always same sites connexions for the moment but four google search appeared after this DLL

On WIN2003:

1. Infection Time: 23h55 with copy of sample on WIN2003 system

2. Injection on the system the sample named : gvlwnwlj.yb

3. Infection started

4. Isomorphic behaviors :

- Go to google in 80 port

- Network scanning on 445 port 192.168.1.0/24

After 15 minutes :

Communications with sites .cn, .info, etc. and apply a search with following order: /search?q=0 but i can note that these sites are completely different than the XP computer.

An answer on http under 445 port get a radmin connexion

Another site send an flr_agent and a magiccontrol

Communications seems to be always with local port 4903 to the 80 of these sites

No OS scheduled tasks were modified or created

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-19 11:43:32
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/>