

MARC BLANCHARD VIRUS DOCTEUR

16th september 2009 : Isomorphic behaviors

On XP:

Time: 23:49

There is not any more communications with sites.

There is not any more some internal network browsing.

At 23h29 : all activities were active.

The sample disappeared of the system.

I can conclude 2 things:

1. Or the sample has a bug
2. Or the sample disappeared by itself after some time, to try to be reloaded to access to another external sites

I decided to wait 24h to see if the sample try to be reactivated by itself.

No Schedule Tasks were created, but maybe some trace in memory could stay on hidden mutex processes.

On WIN2003:

At 23h24 : The malware stays active, but i can see that the accesses to external sites, the google parsing and internal networks scanning decreased comparing at 24 hours before and seems to be stabilized each 2 hours.

The sample disappeared of the /WINDOWS/SYSTEM32

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-19 12:16:46
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/>