

MARC BLANCHARD VIRUS DOCTEUR

24th September 2009 - Isomorphic behaviors

On XP and 2003 all is stabilized.

BUT : a new information is coming today.

I received on comments some complains that the DNS was changed on several networks on the uses computers.

So after analysis, it seems that a new bahavior is coming today :

- No scheduled task was created

- nobody can access to the internet, the DHCP doesn't answer, the workstation DHCP is disabled and it is impossible to fix IP addr or to run ipconfig

- All DNS are located on 127.0.0.1

- All entries on TCP/IP parameters are blocked by the malware, so impossible to modify some values.

But if users try to access to the internet, he can if and only if numeric IP addresses are written.

So this new behavior is needed to be studied.

That's why i decide to install a new computer infected by this new generation and try to analyze what's happen and how.

So, when this new plateforme will be online, i will report this one also on this section.

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-24 21:27:20
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/>