

# MARC BLANCHARD VIRUS DOCTEUR

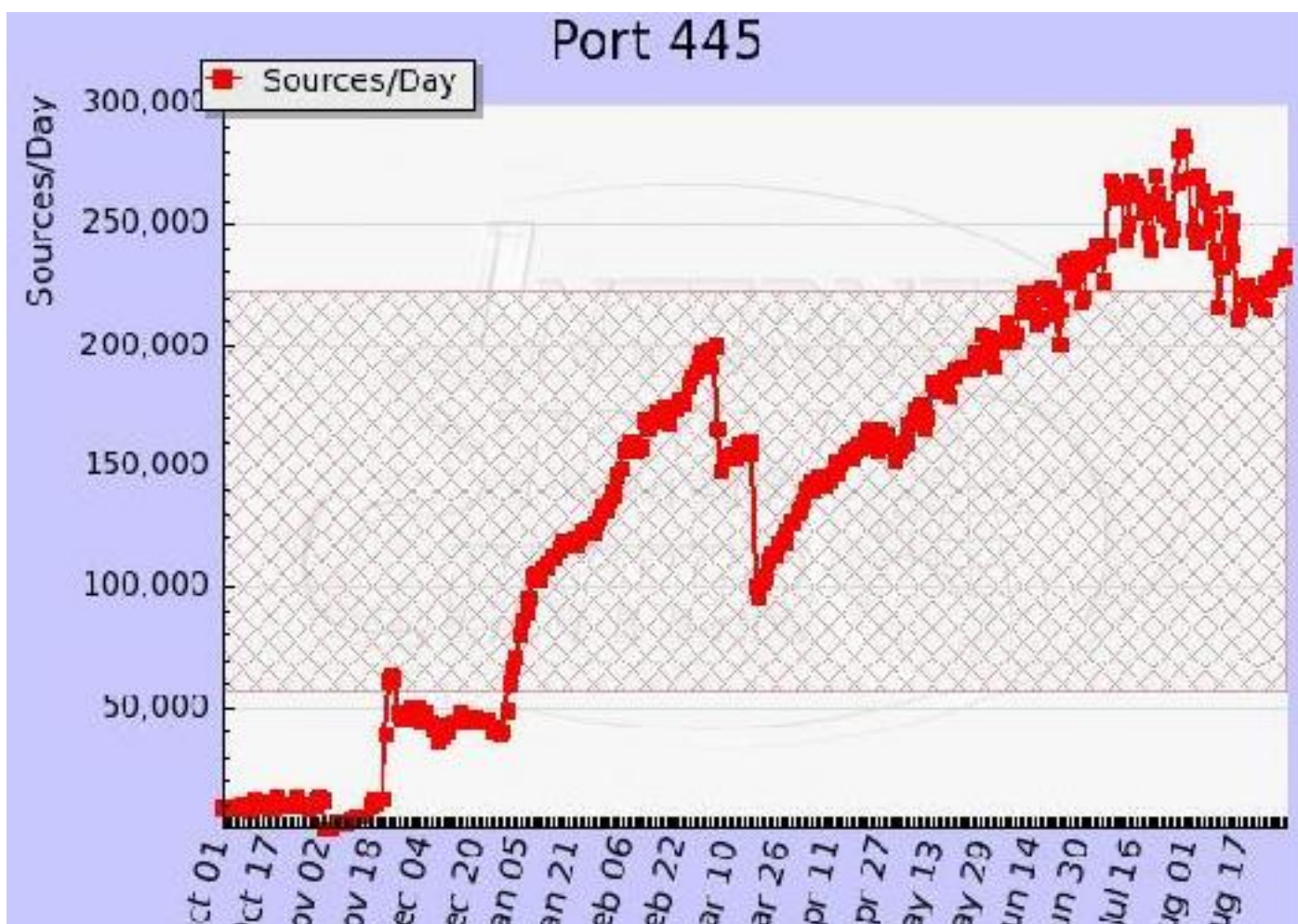
## CONFIKER - Project description

### *What is the current situation with Confiker?*

More than 54.8% of european companies has the confiker pandemy. Their networks participate to the evolution of this parallel network and computers are soldiers to participate to some important attacks like DDOS, spam, terrorism, etc...

This is a real pandemy because MS did lot of efforts to patch for its OS's, also AV Vendors do their maximum to try to clean and detect this stormworm.

But the pandemy continues :



Every concerned security companies do their best to block it as soon that they have new informations on this stormworm, but this stormworm changes its behaviors, codes, infections algorithms, each time these security companies find solutions to clean or stop or block this stormworm.

Each time Confiker continue to spread and to infect, as the graph shows.

So it is really a plague to reach the zero day to protect computers.

### ***What is the goal of this project?***

To trace and log the confiker activities, changes and study the behaviors.

### ***With what?***

Personal development tool : Malicious Applications Probes version 3.0.0.0

Network Sniffer tool : Packet Analyzer 1.0.1

Taxinomy Phenotype Collector : version 2.0.0.1

### ***For what?***

To start to have isomorphic analysis and result

To run in specific time, these results to predict homomorphic results with equal or more variations.

To add on these results, i will take the uncertain informations, like :

-The network stability

-The behavior depending of the hybrid networks where Confiker will work

-The communication between some confiker soldiers

-And in case of attacks in real time, some publishing of homomorphism behaviors concerning this T-Time attack.

The result should born diagrams on methods and geocalisations of the confiker activities.

### ***Project agenda :***

I will firstable report only what it is happen on the behavior in order to collect maximum of isomorphic informations on one LAN with 1 Win2003 server infected and 3 XPs. They are not virtualized, they are true computers. The firewall that lets this lan to go to the net and accepts inbound - outbound connexions on 445 & 80 ports.

The second step will be to continue to have the first infected LAN, but another LAN will be infected with 1 Win2008 and 2 XP and 1 Vista. This LAN has access on the first infected lan. FW

rules between these 2 lans don't let the 445 port, but accept 80 port to go outside.

When i will be sure to have enough isomorphic informations, i will start to cross these informations to start a reseach on homomorphic results with a taxinomic methods.

These datas and personnal comments will be published on this section of my blog. You will not find on these posts my researches methods, because it is a Taxinomy Methods software that i use. But when i will estimate to get enough infomations, i'll publish on this blog the complete conclusion.

***I remind some re-publishers that these researches are under copyright and you must contact me for more informations. My phone number is : + 33 (0)6 63 58 10 97 Please let message on voice mail***

***NOTA : I dont answer to remove any infection or provide any help on antivirus products !!! Please contact your AV Vendor for support & assistance.***

### ***Contributors :***

I wish particulary thanks contributors to this project :

- Elsa Pigeat from ELP-Informatique.
- Welcr for his reports when attacks occured.
- Laurent for his help for the installation and recabling ethernet and electricity of the VirusLab computers bay.
- My wife that analyzes some isomorphic results & her patience for time I research and publish ;-)
- All of you, readers, with your personal posts, that you send me to encourage this big project

## Commentaires

2009-09-28 15:17:05 - Computer Support - anil@support1000.com -  
<http://www.support1000.com>

Thanks for sharing this info post.

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-19 11:24:20  
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/>