

MARC BLANCHARD VIRUS DOCTEUR

28th Spetember 2009 - Confiker launch attack confirmed - 1st homomorphic report

After the isomorphic external report and the viruslab behaviors, i confirm that an attack happened around the confiker network.

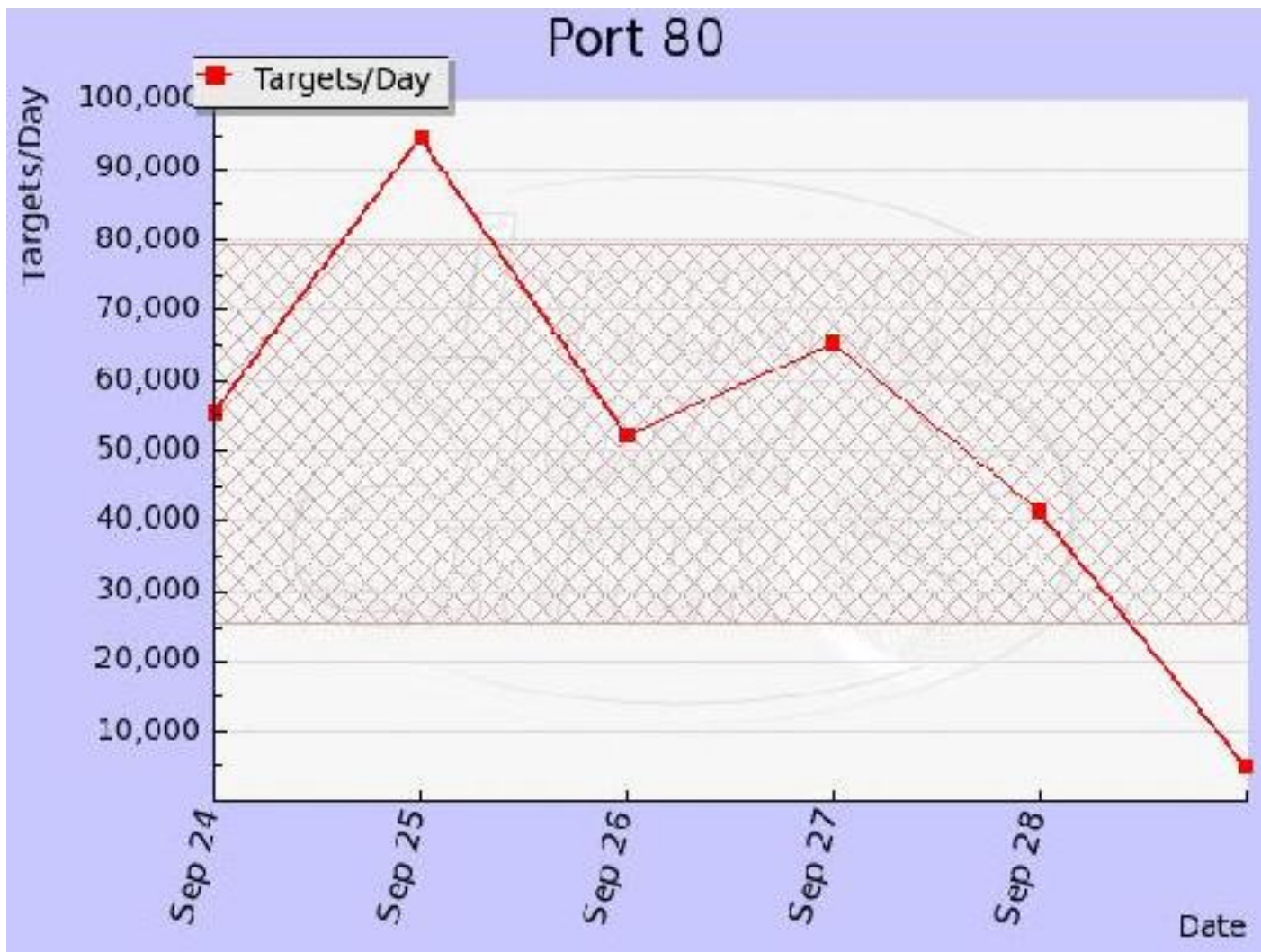
Here is the homomorphic report of this attack:

Last week, some files were created temporaly by confiker that listed the hard disks structures.

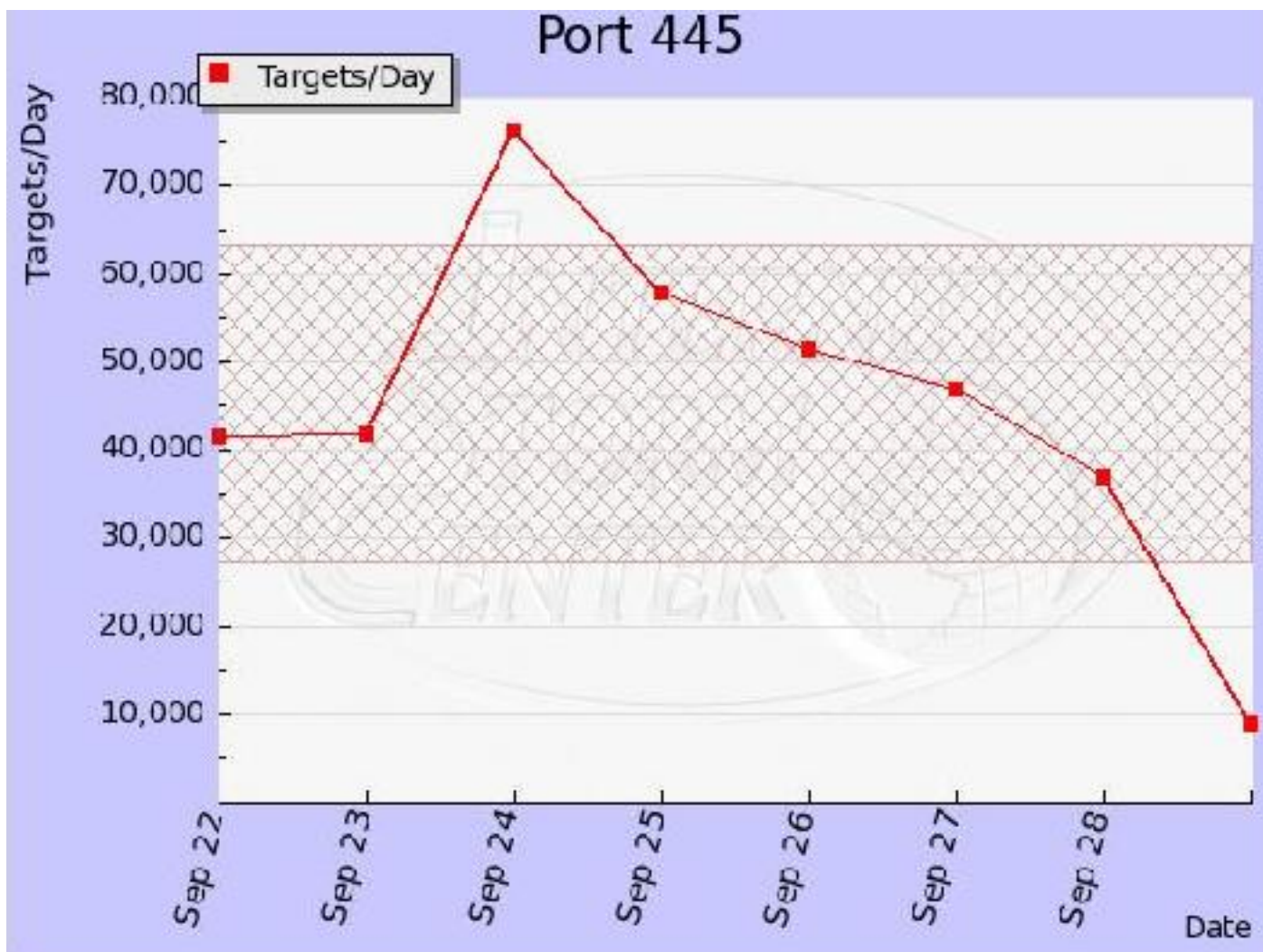
Some requests were shown that tested the bandwith of confiker' soldiers.

The attack was executed friday 25th against some IP's that are for the moment confidential (76000 requests during 19 minutes per attacked IPs).

Here is the graph on traffic on 80 port:



[Here is the graph on 445 traffic:](#)



What results mean:

The 445 port travels the behavior of attack to soldiers the 24th September 2009.

The behavior is following:

- 1- Bandwith analysis of soldiers
- 2- Push to soldiers the informations concerning the future attack
- 3- Files analysis to check if the orders are available on soldiers
- 4- block the internet traffic in order to use the complete bandwith of soldiers. In this case, the fact to route to soldiers the DNS to localhost, will block users to go to the internet. The soldiers computers can go to the internet with hard coded sites, i mean with IPs instead of human domain names.

The 80 port behavior : the attack is launched the day after, the 25th september 2009

- 1- Run the complete attack on 80 port as the picture shows the 25th september 2009 on some

IPs. The soldiers sent 76000 requests during 19 minutes per attacked IPs.

2- We can see that this attack decreased significantly on saturday, but stay active, because some logs report that during attacks some communications were done, maybe to attacks other IPs. That's why, the graph shows you a little decreasing.

Copyright : Blanchard [Virus Docteur] Marc - 2009-09-29 14:35:43
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/>