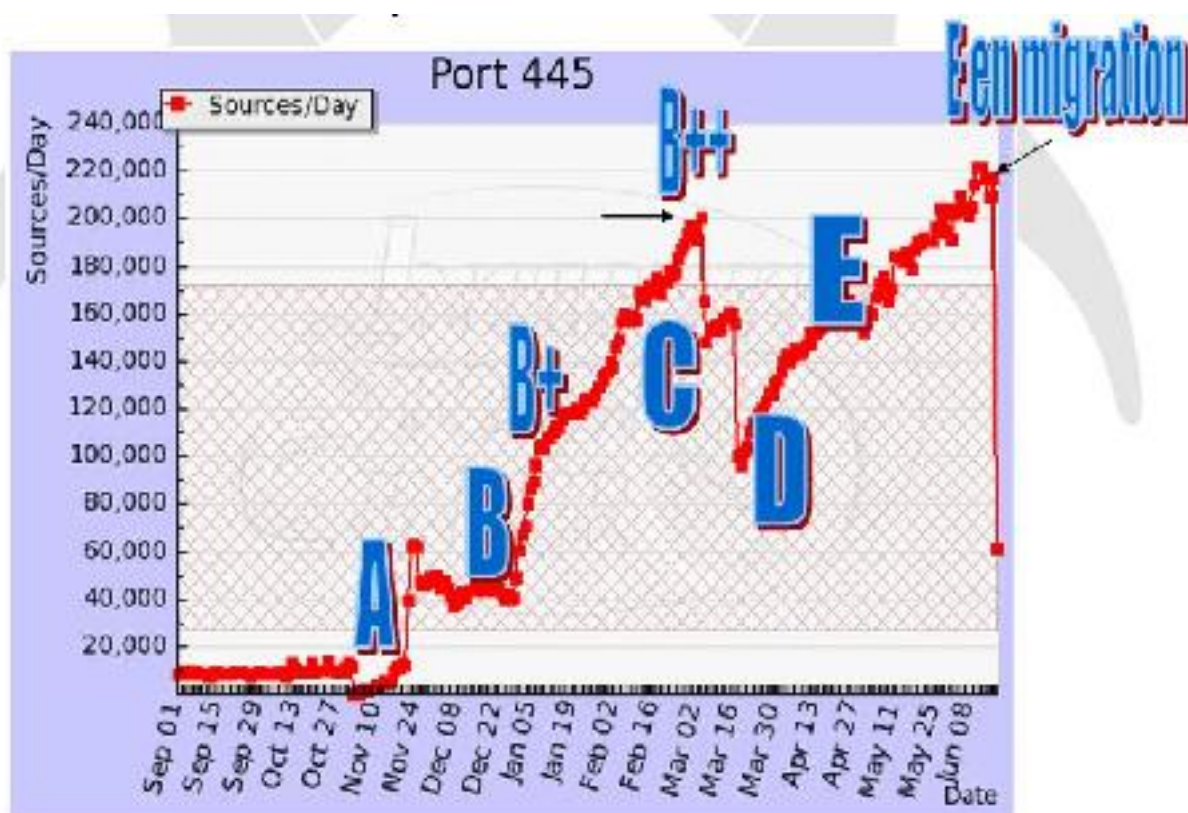


MARC BLANCHARD VIRUS DOCTEUR

Suivi de l'activité de Confiker

Confiker est toujours là !

Il évolue de jour en jour, et est redéveloppé au quotidien.



Recherche optimisée par www.blanchard.com

Pourquoi évolue-t-il de cette façon ?

Comme nous pouvons le constater avec l'image ci-dessous, une enveloppe vide est chargée en mémoire sans aucun code.

```

Entry point in file offset: 0x0055
File format: PE executable (Win32)

74 00 e9 a4 13 01 00 00 00 00 00 00 00 00 00 00 : 00000 t ün!!3
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00010
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00020
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00030
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00040
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00050
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00060
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00070
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00080
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 00090
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000a0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000b0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000c0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000d0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000e0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 000f0

The program terminates successfully.

```

Cela implique que l'enveloppe attend un code dynamiquement et en temps réel venant via une technologie botnet pour agir.

Dans ce cas d'enveloppe vide, un antivirus traditionnel ne peut dans ce cas détecter ce type de code. Seules des solutions de détections actives peuvent répondre à ce type d'egene.

C'est typiquement le fonctionnement de Confiker, qui, de par ses changements subtentiels, évolue à un vitesse fulgurante.

C'est pourquoi de nombreuses variantes maintiennent le réseau Confiker, un peu comme en dents de scie, au fur et à mesure que les détections génériques ou heuristiques puissent être mises à jour, pour détecter de nouvelles variantes...on entre ainsi dans une course contre la montre

...à suivre....

Copyright : Blanchard [Virus Docteur] Marc - 2009-07-02 16:59:00
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/>