

MARC BLANCHARD VIRUS DOCTEUR

3rd october 2009 - Isomorphic Behavior

On one of the conficker networks that i pratice the research sent alarm :

- The alarm is :

Robotization MAP on hybrid network has detected a suspicious activity :

Date : Sat-03-Oct-2009_12_08_50

Suspicious file : c:\windows\system32\twndbpam.dll

It is detected as a generic confiker by AVs.

This file was pushed automatically by the worm.

Here is its entry point:

Entry point in file offset: 0x153f0 File format: PE executable (Win32)

80 7c 24 08 01 0f 85 c2 01 00 00 60 be 00 60 00 ; 00000

10 8d be 00 b0 ff ff 57 eb 10 90 90 90 90 90 90 ; 00010

8a 06 46 88 07 47 01 db 75 07 8b 1e 83 ee fc 11 ; 00020

db 72 ed b8 01 00 00 00 01 db 75 07 8b 1e 83 ee ; 00030

fc 11 db 11 c0 01 db 73 ef 75 09 8b 1e 83 ee fc ; 00040

11 db 73 e4 31 c9 83 e8 03 72 0d c1 e0 08 8a 06 ; 00050

46 83 f0 ff 74 74 89 c5 01 db 75 07 8b 1e 83 ee ; 00060

fc 11 db 11 c9 01 db 75 07 8b 1e 83 ee fc 11 db ; 00070

11 c9 75 20 41 01 db 75 07 8b 1e 83 ee fc 11 db ; 00080

11 c9 01 db 73 ef 75 09 8b 1e 83 ee fc 11 db 73 ; 00090

e4 83 c1 02 81 fd 00 f3 ff ff 83 d1 01 8d 14 2f ; 000a0

83 fd fc 76 0f 8a 02 42 88 07 47 49 75 f7 e9 63 ; 000b0

ff ff ff 90 8b 02 83 c2 04 89 07 83 c7 04 83 e9 ; 000c0

04 77 f1 01 cf e9 4c ff ff ff 5e 89 f7 b9 f6 00 ; 000d0

00 00 8a 07 47 2c e8 3c 01 77 f7 80 3f 00 75 f2 ; 000e0

8b 07 8a 5f 04 66 c1 e8 08 c1 c0 10 86 c4 29 f8 ; 000f0

Copyright : Blanchard [Virus Docteur] Marc - 2009-10-06 00:47:41
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/>