

MARC BLANCHARD VIRUS DOCTEUR

[Scientifique] Les Egenes et nous !!! Partie 1

Un egène est un code malicieux mobile, mais mobile sous plusieurs formes aussi bien au niveau de leurs mobilités dans un réseau qu'au niveau de son propre code.

Nous parlons des réseaux Zombies.

Mais que savons nous de leurs:

- Activités ou de leurs objectifs
- Méthodes de fonctionnement
- Géolocalisations
- Durées de vie
- Modélisations
- Interactions sur internet
- Stabilités

En 2002, sur les undergrounds, une idée avait pris forme quant aux nouvelles dispositions sur les propagations de façons la plus transparente possible des egènes malicieux.

Rappel sur la VCI : Virus Communication Interface

Les Infections InterProcess :

Les egènes sont chargés en RAM et peuvent communiquer avec la VCI elle-même logée dans sa propre adresse virtuelle.

Les egènes envoient les informations du type comportement, ce qui a été contaminé, comment, pourquoi l'infection ne s'est-elle pas effectuée, etc? à la VCI en utilisant des protocoles basés TCPIP.

La Stratégie de la VCI :

La « Virus Communication Interface » est capable :

- d'envoyer et de recevoir les informations à une catégorie de egènes appelés Codes Modulaires

- La VCI est capable de se connecter au net pour télécharger des nouveaux exploits et de nouvelles formes de métamorphismes et les envoyer nominativement aux virus modulaires afin que leurs actions soient modifiées

Les 7 étapes que les codes malicieux doivent suivre :

- Portable : Le egène doit être développé pour être indépendant de la plateforme ? pas seulement sous Windows

- Invisible : Le egène doit être implémenté pour utiliser des technologies métamorphiques utilisant les APIs systèmes pour rester indétectable le plus longtemps possible

- Indépendant : Auto-réplication Auto-execution sans interaction utilisateur, Embarquement de bases d'exploits

- Intelligent (auto-apprentissage): Le Worm doit être capable d'appliquer lui-même un nouvel exploit « en ligne » avec l'utilisation du protocole WormNet

- Intégrité : Egene Modulaire (utilisant la V.C.I.) sont capables d'appliquer des changements substantiels de façon autonome afin d'être le plus caché possible

- Transparence : Pas de code constant (le code est toujours différent) et crypté Les cryptages pourront être différents à chaque contamination de fichiers ou d'ordinateurs cibles en utilisant ou pas la VCI ou via les Inter-Process Communication

- Courte durée de vie : Le egène est de travailler seul, de downloader / Uploader des nouvelles sources d'attaques ou d'exploit

Une fois la mission effectuée, il sera prévu une autodestruction après s'être installé sur une autre machine du subnet via un scanner réseau, un botnet et un rootkit

Durée moyenne d'installation sur la machine victime est estimée entre 2heures et 4 jours

.... A suivre ... Que s'est-il passé depuis ?

Commentaires

2007-09-07 12:43:05 - HoMmE DeS bOiS

super enfin des infos techniques nouvelles que l'on a pas l'habitude de lire ailleurs :-)

bon travail, davai davai

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-06 17:33:57
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/>