

MARC BLANCHARD VIRUS DOCTEUR

[Scientifique] Les Egenes et nous !!! Partie 2

Que s'est-il passé depuis ?

Sont apparus de façon significative :

- Les backdoors
- Les codes modulaires
- Les botnets
- Les rootkits
- Les exploitations des failles de sécurité OS et Applis
- Les différentes méthodes de chantages
- Spam
- Phishing
- Pharming
- Keyloggers, etc

Les conséquences :

De nouveaux protocoles sont arrivés exploitant :

- Les applications vulnérables
- Les ports IP standardisés,
- De nouvelles utilisations de ports transparentes pour les firewalls
- Du social engineering
- De la fraude bancaire

- De la fraude de DNS et de noms de domaines

Les recherches :

Les recherches épidémiologiques changent car nous sommes confrontés à plusieurs types de techniques comme :

- La publication de egènes malicieux sur une période courte, afin de ne pas être détectés par les antivirus
- Le Pharming et le DNS poisoning deviennent à la mode
- L'exploitation des réseaux Zombies qui sont maintenant très nombreux
- Les 'advanced' worms répliquations très émergente utilisant des techniques de multi-threading

"Explications :

- Les Worms à technologie séquentielle infectent un parc de 180000 machines en moins de 500 minutes
- Les Worms à technologie multi-threading utilisant ainsi le parallélisme infectent 180000 machines en moins de 35 sec"

Etude sur les réseaux de E-genes Zombies :

C'est un environnement flou d'un egène et sa capacité d'interagir à travers divers composants.

C'est pourquoi nous sommes obligés d'appréhender le problème différemment avec les egènes qui utilisent les méthodologies du WormNet.

On établit une Carte d'interaction comprenant :

- La Géolocalisation des egènes dans le monde
- Des prédictions de briques élémentaires pour déterminer la dynamique de cet egene

Nous travaillons également sur la composante Temps

- Satellisation de son action sur un temps court

Nous essayons alors de déterminer son évolution :

- Si elle est cyclique - ou si elle est proportionnelle

En ce qui concerne les briques élémentaires, on essaie d'établir :

- La Définition du réseau zombie
- Si il est Stable ou Instable

- Si sa Qualité est bonne
- Egalement les Process de routage
- Comment les Filtrages peuvent etre effectues par les FW
- Enfin des prédiction sur une Implémentation probable via une modularité de code

On finira notre recherches par des Etudes de Comportements :

- Taux de redépart de l'attaque
- Taux de dégradation (détection AV, blocage FW, etc)
- Stabilité du réseau

Les attaques évoluant chaque jour, nous adaptons ces nouvelles recherches épidémiologiques en fonction des nouvelles technologies des codes malicieux.

Commentaires

2007-09-12 18:59:19 - Jean 32

Bonjour,

Je découvre avec le forum de Kaspersky(merci Thierry) toutes ces infos qui donnent le frisson au profane que je suis.

Chapeau pour ce magnifique travail de pédagogie, même si beaucoup, beaucoup de termes m'échappent. Pour rester dans l'esprit du forum je ne laisse que le pseudo.

Avec mes amitiés et mes félicitations, car à 76 ans les neurones s'affolent vite.....

Encore merci

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-11 11:35:45
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/>