

# MARC BLANCHARD VIRUS DOCTEUR

## [Définition&Explications] Les serveurs Web ZOMBIES

Les technologies et des process de fonctionnement évoluent de jour en jour.

Voici une technique qui, certes, est un peu compliquée à comprendre, mais qui est cependant de plus en plus utilisée par les pirates cyberdélinquants aujourd'hui.

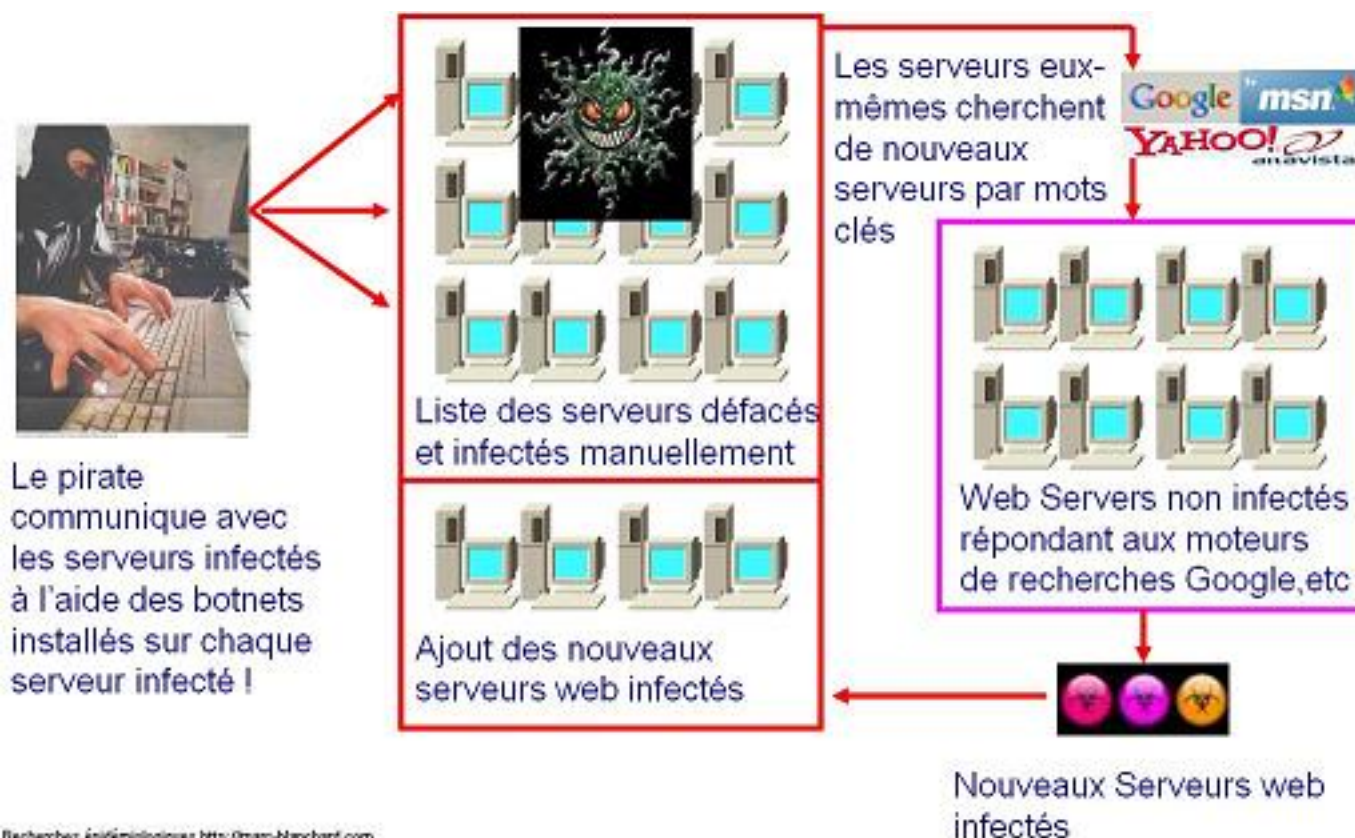
Je vous renvoie sur ce post afin que vous puissiez mieux appréhender la technologie Storm Worm et Storm Botnet.

Post Marc Blanchard : StormWorm et Storm Botnet

Comme je l'avais déjà expliqué dans ce post, les pirates vont utilisées des méthodes de defacing de serveurs web afin de pousser leurs storm worms sur des sites web commerciaux, informationnels, de paris en ligne, de casino, ou même de jeux.

Afin de renforcer la longévité de leurs réseaux zombies, ils ont imaginé deux techniques via des tentatives de pénétrations de serveurs web via du PHP Injection ou du SQL Injection, attaques devenues aujourd'hui très courantes. Voici, après analyses de codes malicieux trouvés sur des serveurs Web, le principe de fonctionnement.

### **Méthodologie 1 : Les serveurs WEB zombies autonomes**

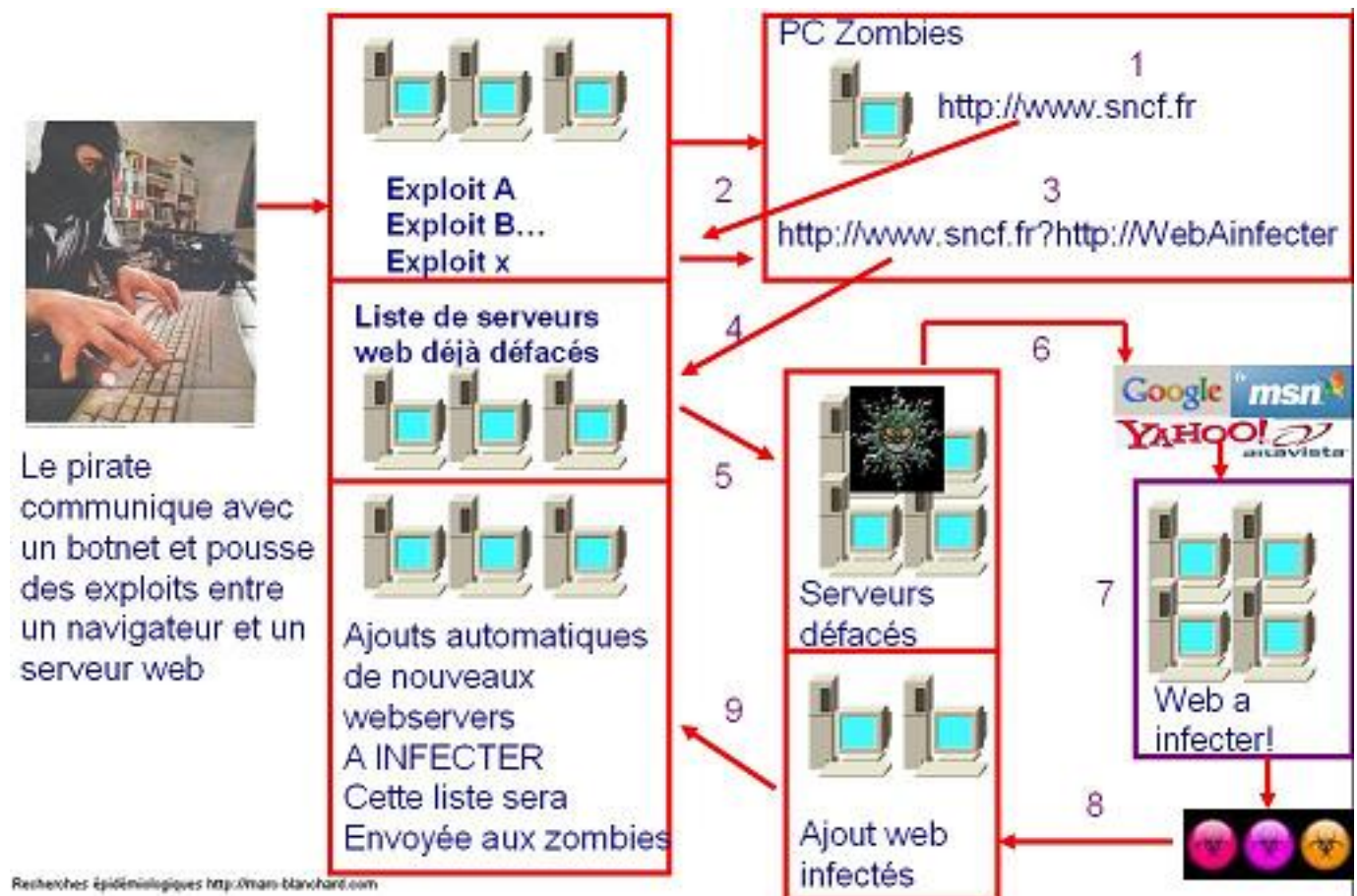


Le Principe est le suivant :

- Le pirate exploite manuellement un certain nombre de serveurs internet
- Sur ces serveurs, un botnet est installé par le délinquant.
- Ce botnet a pour mission d'aller sur différents moteurs de recherches (google, yahoo search, msn, altavista, etc) et font faire ressortir une liste de serveurs web par thématique (sport, politique, jeux, etc)
- les serveurs web contaminés vont alors tenter d'infecter ces nouveaux serveurs trouvés par les moteurs de recherches. Les nouveaux serveurs web seront alors exploités via des exploits PHP et/ou SQL afin de pouvoir pousser un botnet sur ces serveurs
- Une fois infecté, ces nouveaux serveurs web sont insérés dans une liste de serveurs infectés et prêt alors d'utiliser, à leurs tours, les moteurs de recherches..... La boucle est bouclée !

L'internaute, quand à lui, lorsqu'il arrivera sur ces serveurs web zombies, verra son navigateur exploité par un storm worm hébergé par ces serveurs web zombies afin que la machine victime fasse partie intégrante du réseau parallèle zombies.

**Méthodologie 2 : Les machines zombies des internautes qui enrichissent les serveurs WEB zombies**



Le Principe est le suivant :

- L'internaute infecté (utilisant sa machine zombifiée ultérieurement) utilise son navigateur pour aller sur un site.
- Le storm worm présent sur la machine de l'internaute télécharge un à deux exploits

c. Le site web que l'internaute demande se verra alors exploité par un des serveurs web zombies par l'intermédiaire du navigateur de l'internaute.

d. Une fois ce nouveau serveur web défectueux et infecté, un botnet a pour mission d'aller sur différents moteurs de recherches (google, yahoo search, msn, altavista, etc) et font faire ressortir une liste de serveurs web par thématique (sport, politique, jeux, etc)

Les serveurs web contaminés vont alors tenter d'infecter ces nouveaux serveurs trouvés par les moteurs de recherches. Les nouveaux serveurs web seront alors exploités via des exploits PHP et/ou SQL afin de pouvoir pousser un botnet sur ces serveurs

e. Une fois infecté, ces nouveaux serveurs web sont insérés dans une liste de serveurs infectés et prêt alors d'utiliser, à leurs tours, les moteurs de recherches..... La boucle est bouclée !

L'internaute, quand à lui, lorsqu'il arrivera sur ces serveurs web zombies, verra son navigateur exploité par un storm worm hébergé par ces serveurs web zombies afin que la machine victime fasse partie intégrante du réseau parallèle zombies.

### **CONCLUSION**

Il faut impérativement veiller à ce que l'antivirus soit bien à jour aux niveaux des bases de signatures, et l'analyse heuristique doit être OBLIGATOIRE.

## Commentaires

2008-04-14 11:27:50 - Alexis Markov - alexis@kov.ch - <http://blog.kov.ch>

Merci pour cette explication très claire.

J'ai rassemblé ma collection de samples de scripts et batchs que mon intercepteur d'injection bloque.

Je t'envoie tout ça par email. Dis-moi si ça t'est utile...

A bientôt

Copyright : Blanchard [Virus Docteur] Marc - 2008-04-10 13:18:03  
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/>