

# MARC BLANCHARD VIRUS DOCTEUR

## [Interview] Le Journal du Net par Christophe Auffray

### JDN Solutions - Interview

**Marc Blanchard (Kaspersky) :** "On peut décompter 20 à 30 millions de bots dans le monde" Le chercheur de Kaspersky revient sur l'évolution des modes de propagation multiplateforme des réseaux zombies. Technologie P2P et consoles d'administration complexifient la lutte antivirale.

### **JDN Solutions : Pourquoi cette enquête sur les réseaux de PC zombies ?**

Ce qui m'y a poussé, c'est la déclaration du 13 juin dernier faite par le FBI et qui faisait état d'un million de victimes potentielles. De source non-officielle, je pense qu'en 2007, on peut en décompter entre 20 et 30 millions. Bien que ce désordre numérique ne soit pas une épidémie - cela fait désormais quelques temps que ce ne l'est plus -, il m'inquiète.

Le spam envoyé depuis des ordinateurs infectés existait déjà, mais en 2007 nous avons remarqué la multiplication des faux serveurs Web et des blogs fictifs, référencés dans les moteurs de recherche. Or, tous ces services sont hébergés sur des machines contrôlées par un bot, c'est-à-dire un robot.

En ce qui concerne le mode de fonctionnement, on reste sur des techniques connues, avec notamment des backdoors et des rootkits. Mais ce que les pirates recherchent, c'est uniquement la multiplication du nombre de machine zombies. En 2003, le temps moyen d'un développement suite à l'apparition un nouvel exploit était de 15 minutes avec propagation sur le net. En 2007, ce temps est seulement de 4 minutes.

### **JDN Solutions : Quelles évolutions avez-vous notées en ce qui concerne les bots ?**

On s'aperçoit que le taux d'utilisation d'une machine contaminée par un bot ou un ver - non Storm - est de l'ordre de 100% du CPU. L'utilisateur va donc vraisemblablement s'apercevoir de la contamination, ne serait-ce que parce que son ordinateur souffre d'importants ralentissements.

J'ai ainsi remarqué que les pirates analysaient désormais le nombre de mégaflops de la machine et divisaient par 2 ou 3 le taux d'utilisation du CPU. Lors de mes tests, j'ai ainsi exécuté Storm Worm sur un ordinateur disposant de 337 mégaflops. Avec ce bot, c'était non plus 100% du CPU qui étaient exploités, mais 47%.

"Il suffit désormais de se rendre sur un site Web pour être contaminé"

Cette prise de contrôle d'ordinateurs vulnérables permet aux pirates de bénéficier d'une puissance de calcul extraordinaire. A titre de comparaison, le supercalculateur du centre de météorologie français, le Cray, dispose d'une puissance de 101 téraflops. Si on ne retient que la moitié du nombre de victimes comptabilisées par le FBI, soit 500 000, et que l'on attribue à chacun une puissance de 210 mégaflops, on peut se faire une idée de la puissance représentée par les botnets.

### ***JDN Solutions : Quel est le mode de propagation des bots ?***

Aujourd'hui, les méthodologies de propagation et de contrôle à distance des machines sont différentes. Dans un premier temps, on va essayer de vous pousser une enveloppe vide de toute attaque, en fait une backdoor. Cette porte dérobée va permettre d'accéder à un point d'entrée afin de propager une ou plusieurs attaques : serveur de mail, faux blog, faux DNS, etc. Le robot activé - le bot -, enverra de façon automatisée votre adresse IP au pirate à chacun de ses changements.

Les plates-formes de propagation ont elles aussi changé. Avant, le mode de contamination était essentiellement l'e-mail. Désormais, il suffit d'aller sur un site Web. Il faut savoir qu'un script inséré dans le code d'une page Web permet de modifier en temps réel une clef de registre.

Ainsi, les pirates viennent ajouter du code dans les pages d'origine des serveurs, soit un script ou un iframe, qui va pointer vers un autre serveur. Ainsi, un internaute visitant le site et n'ayant pas un système à jour, comme cela est fréquent, téléchargera le code du programme malveillant.

Les attaques de script - VBS, Javascript, PHP, iframe, etc. - vont de pair avec la montée en puissance de Storm Worm. Depuis août, la base de signature des scripts malveillants a ainsi progressé de 300%.

"Les consoles d'administration permettent de géolocaliser les victimes par pays"

### ***JDN Solutions : Quelles sont les particularités de Storm Bot ?***

En plus d'une grande force de calcul, il permet aux pirates de géolocaliser l'ensemble des zombies et repose sur une technologie de P2P. Storm Botnet se compose ainsi de machines hôtes mâles qui vont essayer de trouver 1.000 à 2.000 femelles prêtes à accéder au code géniteur du programme. En outre chaque femelle sera reliée à au minimum 3 machines hôtes. Le maillage est très rapide car les femelles vont essayer également de propager des enveloppes vides à 1.000 à 2.000 autres machines.

Les consoles d'administration permettent quant à elles désormais de géolocaliser les victimes par pays. Un pirate peut même établir des rapports statistiques par pays et télédiffuser une attaque à l'échelon national ou international. Ce mode opératoire permet d'ailleurs de remettre en cause l'implication des autorités chinoises dans les attaques contre la France. Les machines zombies peuvent en effet se trouver en Chine, mais le commanditaire, via ces consoles d'administration évoluées, peut être dans un autre pays.

Autrefois, un botnet était facilement géolocalisable car il reposait sur quelques machines poussant l'attaque. Il suffisait alors d'examiner les traces sur un ordinateur zombie pour

retrouver l'identité de ces serveurs hôtes. Une fois ces derniers désactivés, le réseau zombie s'écroulait.

***JDN Solutions : Un tel maillage signifie-t-il qu'il est désormais impossible de déconnecter un botnet ?***

Ce serait comme essayer d'arrêter un réseau P2P type Kazaa. Trop de machines sont à la fois clientes et serveurs pour qu'il soit possible de faire s'écrouler le réseau de partage. Pour venir à bout de Storm Botnet, il faudrait parvenir à nettoyer l'ensemble des ordinateurs contaminés. Or, il y aura toujours des machines vulnérables.

De vieux programmes comme Blaster, Sasser, Mydoom continuent par exemple d'être au Top 5 des attaques sur le câble. Cela signifie qu'il y a toujours des postes vulnérables qui véhiculent le code sur les réseaux. Avec une propagation multiplate-forme, les pirates s'assurent de toujours disposer d'un nombre de bots suffisant. Et ils y ont tout intérêt puisque leurs profits en dépendent directement.

L'intégrale de l'interview sur le Journal du Net

## Commentaires

2009-01-10 19:41:19 - dodo - alpha@yahoo.fr - <http://www.chermou.org>

on peut plus vivre sans pc :)

2010-10-02 23:58:03 - medical billing - mivpljaipur@gmail.com -  
<http://www.medicalbillers.org/medical-billing-and-coding-as-related-skill-sets/>

effet se trouver en Chine, mais le commanditaire, via ces consoles d'administration évoluées, peut être dans un autre pays.

Copyright : Blanchard [Virus Docteur] Marc - 2007-10-22 10:55:08  
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/>