

# MARC BLANCHARD VIRUS DOCTEUR

## [Zombie] Cas qui peut nous arriver à tous...



Un webmaster m'a fait part d'une attaque d'un réseau zombie qu'il a subi dernièrement sur ses serveurs web. Je vais essayé de vous l'expliquer le plus simplement possible.

### **Perception de l'attaque :**

**a. Coté utilisateur :** Très grosses lenteurs d'accès aux pages web du site, voire impossibilité d'affichage de la page d'index (la page de bienvenue du site)

**b. Coté serveur internet :** Le microprocesseur est à 100% d'utilisation, des milliers de processus du serveur web/http surchargent la mémoire

**c. Coté administrateur / webmaster :** Vérification des règles de parefeux : Rien d'anormal, vérifications auprès du provider internet : rien d'anormal...

### **Que se passe-t-il ?**

1. Après investigation du webmaster et de l'administrateur, des milliers d'ordinateurs sont en train de télécharger un fichier présent au téléchargement sur le site web attaqué.
2. Ces milliers d'ordinateurs téléchargent le fichier du site web attaqué avec une toute petite bande passante.

### **Que peut-on constater dans ce cas :**

1. On s'aperçoit, sur le serveur web attaqué, qu'une multitude de processus de serveur http sont chargés en mémoire, visant à faire tomber la machine via un 100% CPU (micro-processeur) et qu'une saturation mémoire et swap sont proches

2. Que ces processus de serveur http ne s'arrêteront pas tant que le fichier n'est pas totalement téléchargé, ne libérant ainsi le serveur que dans quelques heures.

### **Différentes théories de palliatifs contre cette attaque de denis de service (appelé D.O.S) :**

1. Imposer des limites de processus au système, mais elles peuvent nuire à la production habituelle du nombre de pages web visitées au quotidien
2. Filtrer les adresses IP : Mais certaines IP peuvent avoir un incident de blocage de connexion pour l'utilisateur non perturbateur, car son adresse IP peut être filtrée

### **Solution :**

Partant de ce constat, il s'est avéré que la seule méthode, la plus efficace, était de capturer (blacklister) ces IP perturbatrices, non pas en les annulant, car l'attaquant pourrait attendre que toutes les adresses IP de son réseau zombie changent, mais de lui faire croire que son attaque fonctionne sans pour autant perturber le système.

Pour ce faire, une solution de 'pot noir' en linux existe qui consiste à répondre à la requête d'une adresse IP mais la diriger vers 'rien'

Après une fantastique saisie des adresses IP, et une recherche de géolocalisation des adresses IP, il s'est avéré que l'attaque venait d'Asie. Par conséquent, un 'pot noir' temporaire des adresses IP venant de ce pays s'est avéré la solution la plus efficace, sans trop de perte de productivité commerciale pour l'entreprise.

### **Conclusion :**

Les hackers qui contrôlent les réseaux zombies peuvent provoquer un cyber-désordre d'une entreprise, d'un grand groupe international, juste en télécommandant des attaques programmées, par pays, par région sous forme de denis de services (D.O.S.), pour ensuite effectuer des chantages financiers ....un arrêt de l'attaque contre une somme d'argent...

Les machines zombies ne sont, en fait, que des ordinateurs que nous utilisons au quotidien, mais qui ont été infectés par une backdoor (porte dérobée) et d'un BOTNET (qui envoie régulièrement l'adresse IP de la machine au hacker). Le hacker peut ainsi prendre le contrôle du poste en entrant dans le système via la porte dérobée.

La seule solution aujourd'hui, pour éviter que notre ordinateur n'entre dans un réseau zombie, est une protection antivirale équipée d'un module proactif de défense, une analyse heuristique qui complète une mise à jour des bases antivirale (la plus fréquente possible), et une analyse en temps réel qui analyse TOUT TYPE de fichiers.

Les hackers d'aujourd'hui ne sont plus les hackers que nous avons, il y a 10 ans encore (qui ne montraient que des preuves comme quoi les systèmes pouvaient être vulnérables)... Non! les hackers d'aujourd'hui sont bel et bien de réels businessmen, et là .....

Où s'arrêteront leurs limites? Dans ce cas, est-ce que la limite est celle qu'un homme peut attendre dans sa quête de richesse ou de pouvoir ?

## Commentaires

2007-09-29 11:03:34 - svart - <http://www.carantec-pc.com>

"La seule solution aujourd'hui, pour éviter que notre ordinateur n'entre dans un réseau zombie, est une protection antivirale équipée d'un module proactif de défense, une analyse heuristique qui complète une mise à jour des bases antivirale (la plus fréquente possible), et une analyse en temps réel qui analyse TOUT TYPE de fichiers."

Malheureusement c'est insuffisant. La seule solution qui vaille, c'est un utilisateur averti, qui ne télécharge pas n'importe quoi du moment qu'il est écrit "gratuit" ou "super" dessus, et qui ne visite pas n'importe quel site. Le discernement est la seule arme possible contre le black hacking.

Aucun antivirus n'est fiable à 100%, les modules dit "proactif" sont largement incompetents, et à chaque fois que l'antivirus ou le parefeu tombe sur un cas litigieux, il va demander l'opinion de son propriétaire... lequel, s'il ne comprend ou même ne lit pas la question qui lui est posée, va répondre "autoriser" sans savoir de quoi il retourne.

Enfin, une telle fréquence d'analyse ne sera pas sans conséquence sur les performances de l'ordinateur (essayez de faire tourner régulièrement un NIS sur un Vista avec 1Go de RAM et 128 de GRAM, comme c'est fréquemment le cas) et sur la durée de vie du disque dur.

Je pense que se reposer sur une solution automatisée est une illusion. L'antivirus est indispensable, mais l'éducation est le premier rempart contre ce genre d'épidémie.

2007-09-29 23:12:02 - Marc Blanchard [Virus Docteur] - [marc.blanchard@fr.kaspersky.com](mailto:marc.blanchard@fr.kaspersky.com)

Votre prompt mot "c'est un utilisateur averti" qui m'interpelle un peu, sans vous froissez. En fait, statistiquement, il y a très peu d'utilisateurs avertis, et là est le problème. Quel utilisateur d'un pc atour de vous n'a pas installé de petits freeware ou shareware, dites moi ? Personnellement, je n'en connais pas, même ma mère installe des petits outils :-). ...car on ne peut pas tout acheter!!! Je viens de visiter votre site, et votre réaction ne me surprend pas, car vous êtes un professionnel de l'informatique....oui, je suis d'accord que une information auprès de l'utilisateur est primordiale, et personnellement, je properais même le "permis d'internet", un peu comme le permis de conduire, avec examen pour avoir sa licence ;-) mais c'est impossible. Beaucoup d'utilisateurs utilisent le net pour des téléchargements de musiques, films, les 'chats' 'claviotages' en canadien, donc le problème des interdictions attisent les curiosités, et vous ne pourrez rien contre les interdits des interdits :-). et...il faut impérativement aider les utilisateurs à contrer leurs erreurs (erreurs qui, en fait, ne le sont pas forcément pour eux) en les protégeant au mieux avec des antivirus et parefeux...un assistanat, me direz vous ? oui et non, car des logiciels de sécurité sont un peu comme la ceinture de sécurité dans une voiture, avec maintenant des protections pro-actives comme les airbags, les ABS, les ALB et autres protections.... cela n'empêchera pas l'accident, mais l'incident sera éviter.... Le problème, avec les codes malicieux d'aujourd'hui, est qu'ils travaillent dans la transparence la plus complète, en

s'attaquant aux systèmes, mais également au niveau des logiciels installés sur le poste de l'utilisateur, comme Firefox, ou Thunderbird pour ne citer que les plus utilisés, et ces vers essaient, à l'insu de l'utilisateur, de pénétrer la machine via des exploits, car ces logiciels ne sont pas, en général, les dernières versions ou builds installés sur les postes de nos utilisateurs, maheureusement :-). Le problème avec les attaques d'aujourd'hui, est la transparence des attaques. Vous lirez bientôt sur ce blog, un compte-rendu épidémiologique qui traite des problèmes des worms et botnet en ayant une vue globale du problème, et non une vue uniquement au niveau des ordinateurs personnels ou professionnels...et là, on s'aperçoit de l'ampleur de la problématique... Par conséquent, la meilleure protection, certes pas à 100%, mais une protection à 100% n'existe pas, sinon cela ce saurait, reste encore la protection avec un bon antivirus à jour, et un bon parefeu, lui aussi, à jour... Au plaisir de vous lire sur ce blog :-)

2007-09-30 00:16:05 - Souplounite - <http://www.carantec-pc.com>

Nous ne sommes pas en désaccord. Aurais-je donné l'impression de suggérer de ne pas utiliser d'antivirus ? Si c'est le cas, j'ai mal exprimé ma pensée. Il est absolument nécessaire d'avoir un antivirus à jour, et un parefeu correctement configuré.

Ce que je veux souligner, c'est qu'il ne faut pas donner aux utilisateurs l'impression qu'ils sont en sécurité \*parce qu'ils\* ont un parefeu et un antivirus. C'est un maillon essentiel de la chaîne de sécurité, mais le maillon primordial, c'est eux-même. C'est un point sur lequel les éditeurs de sécurité (et pour être honnête, je n'avais pas remarqué votre lien avec Kaspersky avant de vous répondre, voyez comme je suis tête en l'air) n'insistent pas assez - voire pas du tout. Je ne pourrais compter le nombre de fois où j'ai entendu un utilisateur héberlué d'avoir un ordinateur infecté s'écrier "mais pourtant j'ai un antivirus !".

C'est là que commence la pédagogie, et pour être franc, il y a un immense travail à réaliser. Il y a même une frange d'utilisateurs pour lesquels aucune solution n'existe, pour la simple raison qu'ils prennent des risques, sciemment.

Ma conclusion aurait dû être : "Je pense que se reposer \*uniquement\* sur une solution automatisée est une illusion.

Et je suis grandement d'accord avec vous que le problème majeur aujourd'hui est que la plupart des infections aujourd'hui sont le fait de codes assez discrets qui n'éveillent pas systématiquement l'attention des utilisateurs. Le cas le plus fréquent que je rencontre, à part les évidents HotBar et autres soi-disant "WeatherChose", c'est le rootkit Navipromo. Encore heureux qu'il soit assez frustré pour être facilement éradiqué. Je m'inquiète du futur et de codes plus élaborés.

Mais une autre partie du problème repose aussi sur la façon commerciale dont les produits sont vendus, insistant une évasive garantie de sécurité - laquelle, si elle n'est jamais prononcée contractuellement, est perçue comme telle.

En revanche, une question : pourquoi citer Firefox et Thunderbird comme vecteur de failles les plus courantes, alors que dans mon expérience, et statistiquement également, c'est surtout Internet Explorer et Outlook Express qui sont le plus utilisés ?

2007-09-30 20:52:15 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Le problème de la prise de conscience des utilisateurs d'ordinateurs est un accès majeur de mon métier (que je sois chez Kaspersky ou des éditeurs AV pour qui j'ai travaillé antérieurement). Je suis d'accord sur le fait que cette prévention doit être utilisée au quotidien, mais ce n'est pas évident pour un utilisateur d'appliquer de fortes recommandations de mises à jour, changement de versions de produits, et là, nous, éditeurs, nous avons encore de très gros progrès à faire. Nous travaillons au quotidien dans ce sens, mais parfois nous sommes techniquement bloqués pour des automatisations à 100%. Pourquoi je cite Thunderbird ou Firefox, ou autre freeware tout aussi performant, voire même plus que des outils proposés par notre big brother quotidien ;- ) est que ces produits doivent être mis à jour très régulièrement afin d'éviter que des attaques exploitent des failles connues... Et je rencontre très souvent des utilisateurs qui utilisent encore même des versions bêtas alors que des versions définitives sont très 'sécures' et installables sans aucun problème.... et l'on reste toujours sur le même débat des mises à jours automatiques ou pseudo automatiques, car il n'y a pas seulement les antivirus ou parefeux à maintenir à jour, mais également les outils du quotidien !!!

2007-09-30 21:34:47 - Souplounite

Compris :)

2007-10-02 02:43:17 - Noizette -

<http://blog.eurnet.fr/index.php/2007/10/01/224-les-aventures-de-noizette-l-cureil-roux-des-chnes-rouvres>

Il ne faut pas oublier que l'informatique est un outil et que les risques liés à cet outil sont "jeunes". Cela ne fait que quelques années que l'on parle de Cyber Criminalité, même si le côté obscur a toujours existé. De nos jours les utilisateurs veulent utiliser leurs Pc's et autres sans réfléchir. On clique on installe et hop... Ils ne veulent souvent ne pas réfléchir ni comprendre ce qu'ils ont pu faire comme erreur. Il faudra du temps pour que les gens arrivent à comprendre qu'il peut y avoir des risques et qu'il faut parfois avoir une "hygiène" de vie sur internet et dans l'informatique. Trop souvent cela n'arrive qu'aux autres, jusqu'au jour où l'on se fait résilier son abonnement par son ISP à cause d'une machine détectée comme Zombie....

Les gens veulent une solution simple qui fait tout un clic et hop pas de questions à poser, le souci est que l'informatique est vaste et variée, peut-être faudrait-il restreindre certaines fonctions et revenir sur des "plateformes" verrouillées et propriétaires pour limiter la casse...

Pour qu'il existe une infection et où un risque il faut respecter trois règles, en supprimer une revient à limiter les risques....

En tout K vaste débat ...

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-23 00:28:05  
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/>