

MARC BLANCHARD VIRUS DOCTEUR

[Avis des internautes] Vos réactions intéressent tout le monde !

Cette rubrique vous est destinée !

Pour tout commentaire ou demande d'information ou tout simplement des curiosités sur le sujet des virus et codes malveillants, cette rubrique est pour vous !

Postez vos commentaires, et je vous répondrais soit par cette rubrique, soit par un sujet scientifique explicatif.

Je parts sur le principe que l'information et la connaissance doivent être partagé par tous.

La question est rarement Pourquoi, mais très souvent Comment Cela permet d'avancer épidémiologiquement :-)

*PS : Ne vous inquiétez pas si votre demande n'est pas de suite publiée, je modère les posts, car je ne souhaite pas publier des SPAMs de blog générés par les robots. Votre post sera publié !
Merci pour votre compréhension !*

Commentaires

2008-01-02 21:33:19 - guibou56 - guibou_56@hotmail.fr

Bonjour ! J'aimerais dès que possible me lancer dans une carrière dans l'informatique et pourquoi pas dans la lutte anti-virus, quelles sont les études à faire pour travailler dans une entreprise comme la votre, et quels sont les différents métiers et tâches dans le domaine ?

Sinon j'apprécis votre BLOG ;)

2008-03-16 11:47:09 - atoure85 - atoure85@yahoo.fr

bonjour! J'apprécie beaucoup votre blog meme si je ne suis pas très calée coté technique, étant juste une utilisatrice ordinaire. J'ai installé Kaspersky Internet Security V.6 d'abord puis à l'expiration, j'ai renouvelé mais avec la V 7.

Le problème est qu'en dépit de tous les analyses et malgré le fait que tous les tests soient positifs, Kaspersky semble ne pas avoir été en mesure d'éliminer ce qui semble être un virus. Cela apparait sous forme d'une fenêtre qui s'ouvre systématiquement au démarrage, intitulée :C:\WINDOWS\SYSTEM 32\neOkS.exe. Cette fenêtre contient un message: Hello BO2k Press any key to continue.

kaspersky semble avoir détecté un virus dénom :virus.VBS.Autorun.ac dans le fichier C:\windows\SYSTEM 32\neOkS.dll.wsf

Et malgré cela et l'ordre de le supprimer, la fenêtre continue à s'afficher à chaque démarrage e qui semble attester de la présence de ce virus.

Je ne sais plus quoi faire et la recherche de ce virus sur le site n'a rien donné.

Pouvez vous m'aider? Merci d'avance

2008-05-06 15:16:12 - cain - postmaster@localhost

Bonjour,

Je visite de temps en temps ce blog qui est assez informatif. Cependant j'ai une remarque à faire et j'aimerais avoir votre avis.

Pratiquement tous vos posts ont pour conclusion l'installation et la configuration d'antivirus. Je suis assez contre ce principe car il est basé sur un mauvais principe sécuritaire, celui de l'énumération des choses négatives. Le "enumerating badness" de Marcus Ranum (1)

Les attaques d'aujourd'hui sont de plus en plus ciblées, de plus en plus spécifiques et les codes malveillants ressemblent de moins en moins aux virii tels qu'on les trouvait en code asm il y a 10 ou 15 ans. Le système de signatures antivirales n'est-il pas un modèle de sécurité voué à l'échec ? Ne pensez vous pas qu'une politique stricte au niveau du poste de travail (prise en charge ou non par le système d'exploitation) serait beaucoup plus efficace qu'un antivirus ? Attention ! je ne dis pas qu'avec un tel système l'utilisateur est parfaitement

protégé de toutes les attaques possibles. Chaque jour des chercheurs trouvent des failles dans les systèmes et les éditeurs corrigent souvent ces failles (ou pas ! cf. Oracle (2))

Si on ajoute à ceci les failles que génère tout programme supplémentaire (et d'après secunia il y en a eu 9 pour les produits Kaspersky en 2007 (3)), on peut se demander pourquoi tant de précipitation pour installer un antivirus alors qu'il va nous ralentir l'ordinateur pour une sécurité toute relative.

Pourquoi ne pas privilégier un système comme l'extention <noscript> pour Firefox, ou de limitation des applications exécutables dans Windows ? Les menaces seraient grandement réduites.

1. [hxxp://www.ranum.com/security/computer_security/editorials/dumb/](http://www.ranum.com/security/computer_security/editorials/dumb/)

2.

[hxxp://securite.reseaux-telecoms.net/actualites/lire-gros-courants-det-x92-air-dans-oracle-11642.html](http://securite.reseaux-telecoms.net/actualites/lire-gros-courants-det-x92-air-dans-oracle-11642.html)

3. [hxxp://secunia.com/search/?search=kaspersky](http://secunia.com/search/?search=kaspersky)

2008-05-14 16:23:08 - Fill - Le-site-de-Fill@orange.fr - <http://pagesperso-orange.fr/Le-site-de-Fill/>

Merci pour ces explications à la fois techniques et concrètes. J'ai particulièrement apprécié la vidéo tissant des liens entre l'approche juridique et l'approche technique dans les différents modes d'infections, à travers notamment le regard d'un juriste.

Je crois que le crime informatique n'a pas fini de se développer, malheureusement.

2009-01-22 14:47:03 - David G. - david.grenard@bluewin.ch

Merci pour vos explications, elles me sont très utiles pour mieux comprendre l'étendue de la menace.

Bien que travaillant dans l'informatique je suis loin de m'y connaître en sécurité.

Votre explication décrivant l'installation d'un rootkit a attiré mon attention et j'ai une question à ce sujet.

Vous dites que ce processus doit absolument ouvrir une porte dérobée pour pouvoir permettre une connection entrante depuis l'extérieur. Pour cela il doit corrompre ou tromper le firewall. Cela se comprend aisément dans le cas ou le firewall se trouve localement sur le PC, mais si un autre firewall veille au grain à l'extérieur, sur un router/nat par exemple? C'est majoritairement le cas actuellement. Le mien est fermé à toute tentative de connection depuis l'extérieur et je le vérifie de temps à autre. De plus il me prévient par mail en cas de tentative d'intrusion. Même dans le cas ou une porte est ouverte dans mon pc comment un rootkit ou autre pourrait-il permettre de prendre les commandes de mon pc depuis l'extérieur malgré ça?

J'imagine qu'il pourrait aller charger des instructions depuis une adresse quelconque et les

exécuter mais il s'agirait d'un mode batch et pas interactif dans ce cas.
Merci et très bonne journée.

Copyright : Blanchard [Virus Docteur] Marc - 2007-10-11 13:17:19
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/>