

MARC BLANCHARD VIRUS DOCTEUR

Confiker ... Petits conseils récapitulatifs avec les produits BitDefender...

Nombre d'entre vous me contacte pour me demander conseils de nettoyage pour ce botnet.

Je vous propose donc d'effectuer les procédures suivantes qu'il vous faut suivre scrupuleusement.

1. L'installation du patch est obligatoire sur tous les postes clients et serveurs du réseaux windows (OBLIGATOIRE).

Installer le patch Microsoft (KB958644) disponible sur le lien ci-dessous:

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

<http://www.microsoft.com/technet/security/Bulletin/MS08-068.msp>

2. Il vous faut bloquer temporairement les accès aux périphériques usb de votre réseaux afin d'éviter aux utilisateur de se faire réinfecter en connectant un périphérique disque usb.

Allez dans BitDefender management console, "**créer un script WMI**" Sélectionner "**désactivez la mémoire de masse usb**"

3. Modifier la politique "**paramètres antivirus**", et basculez le niveau de protection par défaut en mode **PERSONALISE** en cochant toutes les options sauf analyse reseau et analyse des archives

Il faut, pour toutes les options en cas de detection malware, passer les actions que BitDefender doit entreprendre en cas de détection, **METTRE EN QUARANTAINE**

Assurez vous également que les mise à jour antivirus soient à jour la plus récente en appliquant la politique de "**demande de mise à jour**"

4. Modifier la politique "**Politique d'Analyse**",

5. Basculez le niveau de protection par défaut en mode **PERSONNALISE** en verifiant si toutes les options sont cochées.

6. Vérifier que dans l'option Analyse sur fichier que l'Analyse tous les fichiers soit cochée .

7. Dans Action d'analyse, positionner toutes les premières et secondes actions soit programmées en Mise en 40aine
8. Lancer une analyse sur chacun des postes du réseau
9. Si vous avez des **OS Microsoft NT ou Windows Seven**, même protégés, déconnectez **PHYSIQUEMENT** ces ordinateurs du réseau, ils sont **vulnérables à ce jour, et Microsoft n'a pas encore sorti de hotfix** sur la faille décrite sur le KB958644.
10. Si l'infection continue, prendre quelques postes remontés dans la console comme infecté.
 - 10.1 Déconnecter ce poste physiquement du réseau local (retirer la prise réseau)
 - 10.2 Lancer une analyse manuelle sur tout le disque

Si ce poste est contaminé offline, vérifiez si le patch Microsoft (KB958644) a été installé par le biais d'ajout et Suppression de programmes

Si il n'est pas contaminé, refaire la procédure du **point 10** sur quelques postes et / ou serveur. Cela implique qu'un des postes ou serveurs de votre réseau est encore contaminé et ne possède pas le patch Microsoft.

Si il est contaminé (offline), il vous faudra alors **IMPERATIVEMENT le déconnecter physiquement (retirer la prise RJ45)**

Il faut le patcher et l'éradiquer avec BitDefender.

Nota : Tant que ce poste n'est pas patché et que l'antivirus n'a pas fini son analyse, ne pas le reconnecter sur le réseau.

Si l'infection continue, cela implique qu'un des postes ou serveurs de votre réseau est encore contaminé et ne possède pas le patch Microsoft.

Il vous faudra le(s) trouver et appliquer la procédure à partir du point 10

CONCLUSION : Ce type d'infection représente un travail fastidieux à la désinfection. Appliquez les procédures à la lettre, et vous gagnerez votre temps.

Bon courage

Commentaires

2009-08-26 11:23:22 - Poppy - adinboley@yahoo.com - <http://www.ms-jewelry.com>

Comment installer un patch? J'ai lu de nombreux articles et des recommandations, mais ne peut toujours pas moi!

2009-09-16 23:21:43 - depannage informatique - hypocamp@gmail.com - <http://www.pcpourlesnuls.com>

merci bcp pour l'astuce, je ne la connaissais pas mais je vais pouvoir la donner à mes clients :)

Copyright : Blanchard [Virus Docteur] Marc - 2009-08-18 15:40:33
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/>