Date de publication Vendredi 10 avril 2009 à 12:02:55 **par** colok
Catégorie Nouveautés

Conficker: Attention! Virus intelligent !

Source: SebSauvage Les auteurs de virus (ou vers) ont toujours joué au jeu du chat et de la souris avec les auteurs d'antivirus. Mais il faut bien dire que les dernières générations de virus sont particulièrement sophistiquées. L'exemple le plus frappant étant le virus Conficker. Voici ce qu'il est capable de faire: Il se répand par le réseau, recherchant des dossiers partagés Windows (partages réseau), exploitant une faille de sécurité pour outrepasser les droits d'accès. Si la faille n'est pas présente, il essaie des dizaines de mots de passe différents afin d'accéder malgré tout au disque. Une fois qu'il a accès au disque, il peut infecter la machine. Il se propage également par supports amovibles, se copiant sur tous les disques qu'il trouve (disques durs externes, clés USB, cartes mémoire...) et créé un autorun qui lance une copie du virus placé dans le répertoire poubelle du disque. C'est malin: le répertoire "RECYCLER" n'est jamais affiché par Windows, et l'autorun déclenche le virus dès l'insertion du disque. Il créé un service dans Windows (et n'apparaît donc pas dans la liste des processus en cours d'exécution). Il utilise un nom de service qui semble natif de Windows. Il désactive: Le centre de sécurité Windows (qui vous prévient que votre firewall ou antivirus n'est pas actif ou à jour). L'utilisateur n'est plus alerté. Les mises à jour WindowsUpdate (fûté, vu que Microsoft distribue par ce biais des détections et désinfections automatiques de virus) BITS, le système de distribution des mises à jour de Windows. WindowsDefender, l'antivirus standard de Windows Le service de rapport d'erreur (qui envoie des rapport à Microsoft sur le plantage d'applications) Et enfin, toutes les secondes, il recherche en mémoire tous les programmes dont le nom ressemble de près ou de loin à un antivirus, antispyware ou logiciel de sécurité, et les tue. (Impossible de lancer le moindre programme de désinfection, même en l'apportant sur clé USB). Lire la suite en cliquant ici

Billet issu du site internet Colok Traductions:
https://www.colok-traductions.com

URL du billet
https://www.colok-traductions.com/index.php?op=billet&bid=1360