Ver /virus: encore une version de MyDoom: Q

Tout l'alphabet va bientôt y passer! Les experts constatent que si cette dernière souche est avérée comme nouvelle, elle porte dès lors la référence MyDoom-Q. Car elle est similaire aux précédentes: elle se transmet via les e-mails en réutilisant des listes d'adresses avec une variété de dénominations pour les « objets » ou « sujets » des messages, aléatoirement affichées. Certains de ces messages font référence à un fichier .zip attaché (fichier comprimé, qu'il ne faut surtout pas ouvrir). S'il est ouvert, le fichier va se copier automatiquement sur le repertoire de Windows, « winlibs.exe ». La partie exécutable du fichier contient une liste d'une douzaine de noms ou sobriquets en expéditeur. Ce ver semble s'être propagé à l'origine via la fonction « Recherche de personnes » de Yahoo. Il s'insinue également dans les fichiers des postes infectés à partir desquels il va en contaminer d'autres. Cette pénétration dans les moteurs de recherche est l'un des points communs avec les variantes « M » et « O » des semaines passées. Outre Yahoo, ce sont Alta Vista, Lycos et Google qui ont été touchés. C'est ce dernier qui aurait été le plus affecté: fort ralentissement du site, et blocages dans la recherche Les requêtes sur Yahoo en revanche ne semblent pas avoir été très perturbées. Cette variante serait moins dévastatrice que les précédentes. Son classement est au niveau: »

medium risk« . Le ou les auteurs de MyDoom et de ses variantes n'ont toujours pas été cernés, malgré les fortes récompenses promises par Microsoft et SCO. _____ Avec **Vulnerabilte.com**

Commentaire de Sophos: plagiat de virus

«

Le plagiat de virus existants est à la mode dans le monde du cybercrime, et il ne fallait pas être grand devin pour prédire l'apparition de nouveaux vers capables de récupérer des adresses e-mail à partir des moteurs de recherche. Nous pouvons malheureusement nous attendre à en voir d'autres du même type dans l'avenir», constate Annie Gay, dg de Sophos France.