

# Virus: Netsky.R se fait passer pour un 'soft'

## Panda

La saga Netsky continue. Toujours aussi virulent, la version R du ver est très vicieuse. Comme tous ses grands frères, il se propage à haute vitesse par e-mail.

Le sujet du mail est: *Re: Document* (nombre aléatoire) et le contenu du message: *Excuse me, the important document is attached, Yours sincerely*. Enfin, le ver comporte un fichier joint intitulé *Document ( nombre aléatoire) .pif*. Si le fichier est exécuté, le ver est envoyé à toutes les adresses qu'il trouve dans les fichiers portant les extensions suivantes : .eml, .txt, .php, .asp, .wab, .doc, .sht, .oft, .msg, .vbs, .rtf, .uin, .shtm, .cgi, .dhtm, .adb, .tbb, .dbx, .pl, .htm, .html, .jsp, .wsh, .xml, .cfg, .mbx, .mdx, .mht, .mmf, .nch, .ods, .stm, .xls, et .ppt. Mais surtout Netsky.R crée également dans le répertoire Windows un fichier nommé **PandaAVEngine.exe**, qui contient une copie du ver. Il s'agit d'une démarche des créateurs du virus qui consiste à essayer de tromper les utilisateurs en leur faisant croire qu'il s'agit d'un composant d'un des produits de Panda Software. Il ne faut surtout pas exécuter ce fichier. Par ailleurs, dans la déjà longue tradition des attaques politiques, Netsky.R a pour objectif de paralyser, via une attaque par déni de service, les sites [www.emule.de](http://www.emule.de), [www.cracks.am](http://www.cracks.am), [www.emule-project.net](http://www.emule-project.net), [www.kazaa.com](http://www.kazaa.com) et [www.keygen.us](http://www.keygen.us). Ces attaques auront lieu entre le 12 et le 16 avril prochain. Elles pourront provoquer la fermeture temporaire de ces sites, à l'image du site de l'éditeur SCO, crashé par MyDoom.