

# Mydoom -A actif jusqu'au 3 février. Traque en Russie?

**(Mise à Jour)** La traque à Mydoom (ou Novarg-A et Mimail-R.) est lancée. Le ver virus poursuit son attaque à grande échelle en inondant les réseaux. Selon Mikko Hypponen, directeur de la recherche en anti-virus chez F-Secure Finlande, plus d'un million d'ordinateurs étaient déjà touchés ce dimanche 1er février dans le monde entier. Conséquence, « *Mydom a dépassé Sobig.F et est devenu la plus importante attaque virale jamais connue* », ajoute-il. « *Ce truc ne veut pas mourir, il continue à s'étendre au même rythme qu'au cours des derniers jours, ce qui nous semble assez surprenant* », ajoute Mikko Hypponen. Les experts en sécurité informatique ont averti jeudi que les vers allaient perturber les messageries électroniques pour un certain temps, au moins jusqu'aux attaques programmées des sites Internet des éditeurs de logiciels SCO et de Microsoft prévues respectivement ce dimanche 1er février et ce mardi 3 février. D'ailleurs, les experts ont prévu un 'crash' complet du site de SCO. « *Il y aura une grosse attaque ce 1er février contre www.sco.com, qui sera durement touché. Nous pensons que le site va planter* », explique Mikko Hypponen. Mydoom est probablement d'origine russe, ont indiqué vendredi les experts d'une société russe d'antivirus. « *Les premiers 'spams' infectés par le virus l'ont été en Russie, ce qui laisse penser que Mydoom est originaire de ce pays, même si ce n'est pas encore une certitude* », a déclaré Alexandre Gostiev, expert de la société Kaspersky Labs, dans une conférence de presse. Ce mercredi, le FBI annonce qu'il prenait les choses en main. « *Nous sommes activement en train d'enquêter* » sur le nouveau virus, a déclaré un porte-parole du FBI, Paul Bresson. **3 niveaux d'attaque**

**Rappel des faits:** Mydoom-A se propage à grande vitesse en utilisant les messageries e-mail mais également les réseaux d'échange « peer-to-peer » type Kazaa. Comme d'habitude, ce ver/virus se propage via toutes les adresses trouvées sur les ordinateurs affectés. Il est véhiculé par un e-mail comprenant un attachement de fichier. L'objet comporte différentes accroches : test, hi, hello, Mail Delivery System, Mail Transaction Failed, Server Report, Status Error. Le corps du message contient: « Test », « *The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment* ». Ou encore « *The message contains Unicode characters and has been sent as a binary attachment* ». « *Mail transaction failed* ». « *Partial message is available* ». Les pièces jointes sont « document », « readme », « doc », « text », « file », « data », « test », « message », « body » avec les extensions : .pif, .scr, .exe, .cmd, .bat. Il s'installe sur le système sous le nom de '**taskmon.exe**'. Une fois la machine infectée, il active Windows Notepad et installe une porte-dérobée (ou « backdoor ») en créant un fichier **SHIMGAPI.DLL** sur le système 32 de Windows. Il l'exécute ensuite à travers un processus de IEPLOR.EXE. Mydoom.A ouvre le port TCP 3127 sur l'ordinateur infecté, autorisant ainsi le contrôle à distance dudit ordinateur. Ceci signifie qu'un pirate peut accéder, dérober, modifier ou détruire, toute information présente sur l'ordinateur. **Vocation politique** Une fois que le virus a infecté un ordinateur, il se met à la recherche du programme de partage de fichiers en réseau Kazaa. Si ce dernier est détecté, un fichier est alors copié dans le répertoire de partage, autorisant sa diffusion via ce système de 'peer to peer'. Ce n'est pas tout. Non content d'inonder les réseaux et d'ouvrir une « back door », ce ver a également une vocation politique. Une sorte de fonction « double lame »... Il est programmé pour conduire une **attaque par « déni de service »** sur le site Internet de l'éditeur **SCO**. **Microsoft** est aussi visé par la variante B de Mydoom (voir notre article).

Après le 1er février, Mydoom s'activera à chaque redémarrage ('boot') de la machine et tentera d'ouvrir la page de l'éditeur de solutions Unix, SCO [www.sco.com](http://www.sco.com) et essaiera de s'y connecter chaque seconde à partir de chaque machine infectée à travers le monde. Le requête, très simple « GET / HTTP/1.1 », est programmée pour surcharger le serveur web de SCO! Basé dans l'Utah, le groupe SCO a confirmé s'attendre à une attaque virale de grande ampleur: « *Nous ne connaissons pas les origines et les raisons de cette attaque, bien que nous ayons des soupçons. C'est un acte délictueux auquel il doit être mis fin* ». L'éditeur Unix a décidé par ailleurs d'offrir une **prime de 250.000 dollars** à toute personne qui fournira des informations permettant d'arrêter et d'inculper le ou les auteurs du virus-ver. SCO a récemment engagé un bras de fer contre plusieurs acteurs de la communauté Linux qu'il accuse de violation de propriété intellectuelle. Son attitude irrite particulièrement les utilisateurs de l'Open-source (Linux)... Comme Bagle et autres Sobig, ce ver/virus est programmé pour s'auto-détruire le 12 février.