Le ver/virus Mimail.L ré-attaque les sites anti-spam

La mode a changé. Avant, les virus s'en prenaient aux ordinateurs, aux disques durs ou aux systèmes de paiements en ligne. Aujourd'hui, les attaques virales sont politiques. C'est le cas du célèbre Mimail: sa variante L s'attaque, de nouveau, aux sites Internet qui luttent contre le spam.

« C'est la troisième variante Mimail qui en a après nous, mais celle-ci essaie d'aller plus loin », a déclaré, à Reuters, Steve Linford, fondateur de The Spamhaus Project, une association britannique qui traque les spammeurs et dont le site a été victime d'une attaque en début de semaine. *« Ils en ont après nous parce que nous essayons de stopper le cycle du spam »*, a expliqué Linford. Mais The Spamhaus Project n'est pas la seule victime. Selon, les éditeurs de logiciels de sécurité, huit associations anti-spam ont été attaquées par Mimail.L: www.spews.org, www.register.com, www.cardcops.com, www.carderplanet.net, www.spamcop.net, www.authorizenet.com, disney.go.com. **Procédé vicieux** Le mode de propagation du ver est au départ classique. Il est envoyé aux internautes via un mail intitulé « Re2 » posté par une certaine Wendy. Il contient un fichier **« wendy.zip »** qui contient lui même un fichier exécutable nommé **« for_greg_with_love.jpg.exe »**. En ouvrant ce fichier, le virus va alors se transférer de lui-même aux adresses électroniques enregistrées dans l'ordinateur contaminé. Ensuite, le système infecté pourra être utilisé comme ordinateur relais commandé à distance, afin de mener des attaques de déni de service distribué(ou DDOS, pour « distributed denial-of-service ») contre des sites pré-sélectionnés, ici des sites anti-spam. Mais si pour une raison quelconque Mimail-L ne parvient pas à se propager correctement, il envoie alors un autre mail (sans pièce jointe) informant l'utilisateur que sa commande d'un CD contenant des images pédophiles sera livrée à son adresse postale. Le message précise que l'internaute peut annuler la commande en écrivant à une adresse qui semble être celle d'un service de réclamations, ce que chacun s'empresse de faire. En fait, les messages des internautes sont redirigés vers les adresses électroniques des huit associations anti-spam. Vicieux!