Le monde de l'Antispam lance une offensive contre les Botnets

Le groupe de travail contre les abus de messagerie a rendu ses observations. A l'occasion d'une réunion organisée en Allemagne, un guide des bonnes pratiques, notamment destiné aux FAI, a été édité. Principaux vecteurs de spams, les *Botnets* ou ordinateurs zombies sont au centre des préoccupations.

A la base de cette réunion, se dresse un constat. De nombreuses personnes font suivre des mails sur leurs différentes boîtes de réception (en particulier celles de votre fournisseur Internet). Dès lors, pour éviter les spams, une des recommandations serait de pouvoir bloquer la boîte si un volume trop important de messages vient à être reçu. Risque, certains mails valides seront aussi bloqués. Pour autant, Richard Cox, PDG de Spamhaus commente la mesure : » *Si trop de spams proviennent d'AOL, les gens eux mêmes vont pouvoir les bloquer automatiquement*« . Les serveurs faisant alors la différence entre les courriers reçus et ceux qui ont été suivis.

La seconde recommandation de l'organisation porte sur les *botnets*. Les ordinateurs zombies sont souvent d'importants pourvoyeurs de spams à travers le monde. La technique est alors simple, les spams sont envoyés à partir de postes générant des adresses IP dynamiques. La parade consistant à bloquer ces adresses est en passe de devenir obsolète. Pour cause, **des programmes permettent désormais de redémarrer l'ordinateur pour qu'il s'identifie sous une nouvelle adresse**.

En attendant de connaître les dernières techniques en vogue chez le pirates, les sociétés ont pu s'échanger durant ce sommet leurs listes noires de DNS (*Domain Name Server*) pour mutualiser leurs efforts.

De leur côté, tous s'accordent pour noter la présence de plus en plus importante des *botnets* présents sur la Toile. Le jeu de cache-cache entre éditeurs de sécurité et zombies spammeurs semble loin d'être terminé.