Nouvelle bataille remportée par les spammeurs

Les spams devraient faire leur retour, si ce n'est pas déjà fait. Certains éditeurs de sécurité ont relevé que de nouveaux et nombreux pourriels étaient en circulation ces derniers jours. C'est un élément nouveau dans la bataille entre spammeurs et éditeurs puisque la **fermeture récente** d'une plate-forme populaire chez ces derniers avait entraîné une baisse sensible du nombre de spams.

Après quatre mois d'enquête, le quotidien américain *The Washington Post*, a découvert que la **fermeture d'un hébergeur situé en Californie a abouti à tarir le flot de spams à travers le monde.**

McColo Corp, basé à San Jose en Californie servait de plate-forme à de nombreux spammeurs, et serait **responsable de l'émission de plus de 75 % des pourriels** diffusés dans le monde, à en croire le quotidien. Pour preuve, seulement deux jours après la fermeture du site, il fut constaté une **baisse du nombre d'envois de spams d'environ 35 à 50%.**

C'était sans compter avec leur force de riposte. On apprend aujourd'hui que le botnet (réseau d'ordinateurs zombie) appelé **Srizbi** a repris du service. Quelqu'un aurait remis à jour ses réseaux pour qu'il puisse envoyer de nombreux messages pollueurs. Il faut savoir que ce **botnet était jusqu'à présent hébergé chez… McColo Corp**. Il semblerait donc que ces botnets aient trouvé de nouveaux chemins pour opérer pendant que les serveurs étaient fermés un à un.

Les chercheurs de FireEye, société qui s'est fait une spécialité de l'analyse des botnets et de leur protection ont découvert que les hackers ont introduit un **algorithme qui génère automatiquement de nouveaux noms de domaines** à un ordinateur lorsqu'on lui attribue de nouvelles instructions. Les botnets ont alors pu s'héberger autre part… Selon les premiers résultats, les **serveurs de contrôles seraient désormais installés en Estonie** et le nom de domaine a été acheté depuis un 'registrar' russe.

La vague pourrait donc s'étendre à nouveau sur le Web. D'autant que selon certaines informations, **Srizbi contrôlerait environ 450.000 postes** et serait l'instigateur de la moitié de ces messages envoyés sur la planète. Sans aller jusque là, le mouvement pourrait être important si l'on considère les **trois autres botnets majeurs** (Rustock, Asprox et Cutwail), eux aussi autrefois hébergés chez McColo.

Si, depuis le fermeture des serveurs, le nombre de pourriels a bien diminué, il reste que l'activité demeure lucrative. Selon l'éditeur G Data, un spam aurait un **coût de 500 euros par an et par employé**. Multiplié par les 130 milliards (environ) envoyés chaque jour. Faites le calcul.