Sécurité : FireEye traque les réseaux botnets

A en croire le récent rapport de l'éditeur McAfee baptisé *Rapport sur le paysage des menaces*, le bilan au premier trimestre 2009 constate une **nouvelle hausse de l' activité des botnets** . Ces « réseaux zombies » capables selon certains spécialistes d'envoyer plus de **100 milliards de messages** de spams par jour à l'insu de leurs utilisateurs iraient jusqu'à **dépasser le million de machines contrôlées par les cybercriminels.**

De même d'autres chercheurs se sont penchés sur la piste des ordinateurs zombies. Les botnets semblaient, après enquête **se servir de la société McColo comme tremplin aux spammeurs** afin d'envoyer des messages non-sollicités par dizaines de milliers. Un réseau en constellation qui peut même servir à orchestrer des attaques contre des Etats.

L'attaque cybernétique retentissante contre l' Estonie en 2007 a ainsi laissé une trace dans les esprits. Véritable nouveauté pour certains, elle incarne la **réalité du contexte géopolitique mondial.**

Rappel, l'**Etat balte reconnu comme étant le plus connecté d'Europe** (90 % des transactions bancaires sur la Toile) a vu lors d'une attaque tous ses sites officiels tomber un par un sous les coups de boutoir des *botnets*. Un groupe d **'activistes pro-russes ont annoncé plus tard être les initiateurs de l'attaque** contre les réseaux de l'Estonie. Une responsabilité qu'à toujours contesté le Kremlin…

Se basant sur ses constats, la société FireEye qui édite une solution promet d **'identifier et lutter contre les fuites et attaques d'informations sensibles** venant notamment des botnets. Une solution qui ne fait pas appel à la traditionnelle méthode des signatures de sécurité, explique le directeur des ventes Stéphane Depasse. « ***L***

es professionnels doivent s'attendre à un 11 septembre numérique. La technologie utilisée par les botnets existe depuis que la technologie du grid computing existe. Le botnet dirigé contre une entreprise va avoir la capacité non seulement de voir, mais aussi analyser le système de sécurité d'une société tout en envoyant massivement des spams« .

Une position certes alarmiste mais qui montre **combien la question des ordinateurs zombies va devenir de plus en plus prégnantes** dans les années à venir.

En France, la solution FireEye est diffusée par la société Exprimm'IT, intégrateur de services (voix, données, images) pour les professionnels. Olivier Breger, ingénieur technico-commercial explique : « ***L***

es solutions actuelles ont des limites car elles sont obligées d'engranger un nombre très important de signatures. Cela oblige les utilisateurs à avoir un bon comportement de protection ce qui n'est pas souvent le cas« .

Depuis la fermeture de certains serveurs de l'entreprise californienne McColo, il semblerait donc

que les éditeurs aient pu capter une partie des signalements d'ordinateurs zombies. A en croire FireEye, grâce à une redirection de flux, pas moins de **450.000 adresses IP destinataires de botnets auraient été relevées. Un mois plus tard, le chiffre s'élevait à 2 millions…** Reste à savoir qui de la solution ou du botnet est le plus rapide ou le plus malin.