Ces géants nommés Botnet!

Joe Stewart, directeur de la recherche en vulnérabilités pour RSA a présenté une étude lors de la RSA conférence qui s'est ouverte à San Francisco. Ce document se penche sur les dix plus grands réseaux de botnets du monde.

L'étude s'intéresse à la taille de ces réseaux underground. Par extrapolation, Steward estime que **l'ensemble de ces botnets contrôle plus d'un million de machines**. Ils sont capables d'envoyer plus de **100 milliards de messages de spams par jour**.

D'après les conclusions de Stewart, le plus important de ces botnets est le réseau **Srizbi**. Ce dernier dispose de plusieurs noms, on le nomme également Cbeplay ou Exchanger. Il totalise pas moins de **315.000 bots** et peut diffuser **60 milliards de spams par jour.** Un chiffre qui donne des frissons dans le dos.

Srizbi n'est pas aussi célèbre que le réseau Storm pourtant il est encore plus actif. A titre de comparaison, Storm ne totalise que 85.000 machines dont seulement 35.000 diffusent du spam. D'ailleurs, sur le Top 11 de Stewart, Storm n'apparaît qu'à la 5e position. Reste que le réseau « Tempête » serait constitué de 230.000 membres actifs.

« Storm n'est plus un réseau très actif. Qui plus est, Microsoft a ajouté Storm a sa liste de code malveillant à détecter depuis septembre 2007. Du coup ce réseau est sur le déclin » estime Stewart.

Le deuxième plus grand réseau de machines zombies est nommée Bobax. Selon l'étude de RSA, Bobax contrôle près de **185.000 machines**. Une jolie collection qui lui permet d'envoyer **9 milliards de spams par jour.** Bobax est un botnet HTTP géré par près de 24.000 membres.

Comme Rbot, un réseau qui compterait **40.000 membres actifs**, ce botnet commence à dater.

Ce dernier dispose également d'une collection d'alias. C'est d'ailleurs pour cette raison que d'autres éditeurs de sécurité le classent à la première place des réseaux de bot les plus actifs. L'éditeur Damballa estime ainsi que le premier réseau botnet est nommé Kraken, et contrôle près de **400.000 machines.**

Pour RSA, Kraken est en réalité l'ancien nom de Bobax. Il dispose d'autres noms comme « Bobic », « Oderoor », « Cotmonger » et « Hacktool.Spammer. »