BOTNET, machine "Zombie" sur internet

par Pascal Couturiaux, dimanche 11 septembre 2011, 11:20

En sécurité informatique, une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un cracker (pirate informatique). Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité.
Un zombie est souvent infesté à l'origine par un ver ou cheval de Troie.

Un réseau de machines zombies peut être constitué et contrôlé par une ou plusieurs personnes, afin d'obtenir une capacité considérable et d'avoir un impact plus important.
Des « armées de zombies », c'est-à-dire de grandes quantités d'ordinateurs compromis, sont utilisées dans les attaques de type « déni de service DoS» ou des tâches diverses comme les envois en masse de courriers non sollicités (spam).
Certains groupes de crackers en contrôleraient plusieurs centaines de milliers au sein de réseaux de zombies, qu'on appelle **botnets** à l'instar des réseaux de robots IRC du même nom. Ces botnets peuvent être utilisés pour commettre des délits comme le vol de données bancaires et identitaires à grande échelle. Les botnets sont plus à l'avantage d'organisations criminelles (mafieuses) que de hackers isolés, et peuvent être même loués à des tiers peu scrupuleux.
Un réseau de machines zombies peut aussi être utilisé afin de fournir aux hackers une puissance de calcul phénoménale, leur permettant de déchiffrer un code en un temps considérablement plus court que sur une machine.