

Définition

Le terme botnet, contraction de l'anglais robot+net, se définit par l'ensemble des programmes, machines, serveurs connectés à Internet ayant un ou plusieurs processus communs de communication. Placé sous le contrôle d'un opérateur humain, appelé botmaster, le botnet recrute des machines en exploitant les vulnérabilités, failles, infections afin d'étendre son réseau à travers l'utilisation de canaux de Command and Control (C&C). Avec l'Internet of Things et ses appareils connectés, le réseau s'étend de plus en plus au sein de notre société. L'actuelle faiblesse en matière de sécurité liée aux objets connectés représente une menace majeure et croissante dans notre environnement. Historique

Le concept, inventé en 1988 à l'université de Oulu en Finlande, fut développé à l'origine pour gérer les services associés au protocole IRC (Internet Relay Chat), un protocole de communication textuelle. Le premier bot "iGM" assistait ainsi l'utilisateur dans la gestion des connexions IRC. Cette gestion automatisée, permettant à distance, de contrôler et de réaliser des opérations à très vite montrant un haut pouvoir malveillant. En Mai 1999, Pretty Park, un malware de forme trojan horse se propageant sur le net permettait de voler les mots de passe. Les premières drives furent notamment l'affrontement de botnet IRC (<https://www.eggheads.org/Eggdrop> en décembre 1993, puis GTbot en avril 1998). Motivations liées à la menace botnet énumérées

- L'aspect lucratif représente l'intérêt majeur pour l'utilisateur de botnet. L'automatisation d'une tâche contrôlée à distance permettant de rapporter facilement des revenus (revente d'information, fraude au clic, spam), surtout si celle-ci est réalisée de manière anonyme (réseau TOR (The Onion Routing), un réseau d'anonymisation).
- La motivation idéologique, comme par exemple, lors du conflit entre la Géorgie et la Russie en 2008 ou de nombreux sites critiques faisant l'objet de cyberattaques massives paralysaient les infrastructures.
- La motivation personnelle, à travers la vengeance ou le chantage, est également une finalité grâce notamment au caractère anonyme de l'attaque.