



Éditorial

# La prolifération des Botnets

Guillaume Lehembre 

Un quart des ordinateurs connectés à Internet appartiendrait à un *Botnet*. Ce constat alarmant – peut être un peu exagéré mais au fond pas si étonnant – a été fait par Vinton Cerf, l'un des pères fondateurs d'Internet, lors du forum économique mondial de Davos en Janvier 2007. Un *Botnet* est un réseau de machines compromises qu'on appelle zombies (*bots*), servant à des tâches malveillantes diverses : envoi de SPAM, *phishing*, dénis de service répartis, scanneur de ports, exploitation de vulnérabilités, etc. L'ensemble de ces machines est contrôlé de manière centralisée par un groupe d'individus au travers de canaux de communication de type IRC, ou plus récemment au travers de HTTP ou de canaux cachés pour tenter de s'affranchir des limites des firewalls. L'existence des *Botnets* remonte au ver PrettyPark apparu en 1999 qui introduisit le concept de canal de contrôle via IRC. Ce mécanisme fut alors repris et amélioré par différentes générations de vers dont les plus connus actuellement appartiennent à la famille AgoBot, SDBot et PhatBot. Leur modularité en fait des outils très hétérogènes capable d'exploiter de multiples vulnérabilités, de scanner des cibles potentielles, d'utiliser des portes dérobées (*backdoor*), de voler des informations sensibles (*keylogger*, sniffeur réseau), etc. Ce qui les différencie des vers est leur capacité à être contrôlés à distance. Les méthodes d'infection utilisées pour compromettre de nouvelles machines sont similaires à celles utilisées par d'autres malwares tels que les virus ou les vers : ingénierie sociale dans l'envoi massif d'emails malicieux, exploitation de vulnérabilités distantes, transmission dans les réseaux de partages, etc.

Le canal de contrôle (*Command & Control*) – principal élément les différenciant des autres malwares – est basé essentiellement sur deux modèles. Le premier modèle est dit centralisé, une machine unique est le point de contact de tous les *bots*. L'ensemble des *bots* se connectent alors à ce point central et attendent des instructions. Ce modèle a l'avantage d'être simple à implémenter et de présenter des temps de réponse rapides pour un grand nombre de *bots*. Son principal inconvénient est le rôle crucial joué par ce serveur central, rendant la survie du *Botnet* fortement lié à cette machine. Son choix est donc vital pour l'attaquant (connexion permanente, bande pas-

sante élevée, etc.). Le second modèle, encore marginal aujourd'hui, est basé sur le modèle P2P afin d'assurer une résilience du réseau. L'inconvénient de ce modèle réside dans les temps de réponse parfois élevés et dans les difficultés pour supporter un nombre de *bots* élevés (plusieurs milliers). Ce type de modèle risque de se développer en intégrant de nouveaux protocoles P2P plus efficaces. Il n'y a qu'un pas à franchir pour que votre Skype soit utilisé comme canal de contrôle au vu de sa facilité à contourner les mécanismes de filtrage.

La détection de *Botnets* peut se faire à différents niveaux. Au niveau réseau, l'analyse du trafic de contrôle (IRC, interrogations DNS suspectives, tunnels HTTP, etc.) ou du trafic lié à des attaques (DDoS, envoi massif de SPAM, scans réseaux, etc.) peut révéler la présence de machines compromises au sein d'un *Botnet*. Une détection peut évidemment être faite directement sur la machine compromise car les mécanismes de dissimulation sont sensiblement identiques à ceux utilisés dans le monde des virus, vers, *rootkits* et autres *malwares*. Depuis quelques années, des *Botnets* servent à des extorsions de fonds massives sur des sites à forte visibilité sous la menace d'attaques par déni de service répartis (DDoS), et certains sites avouent, à mots couverts, avoir payé plusieurs milliers d'euros pour ne pas subir un arrêt de leurs services (cas des bookmakers anglais par exemple). Encore un exemple qui démontre que le piratage actuel tend vers l'appât du gain alors qu'il s'agissait plus de «challenge» et de besoin de reconnaissance par le passé.

Référence : <http://www.honeynet.org/papers/bots/>

## À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants – <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles, dont un article dans le numéro 14 de hakin9 intitulé *Sécurité Wi-Fi – WEP, WPA et WPA2*. Guillaume peut être contacté à l'adresse suivante : [Guillaume.Lehembre@hsc.fr](mailto:Guillaume.Lehembre@hsc.fr)