La taille du botnet Storm est-elle surestimée ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 janvier 2009

https://www.bortzmeyer.org/taille-de-storm.html

Quelle est la taille du plus célèbre des "*botnets*", Storm ? Selon un article de chercheurs à l'UCSD, elle serait moins importante qu'annoncée.

Les "*botnets*" inquiètent beaucoup, et à juste titre, les praticiens de la sécurité des réseaux informatiques et notamment de l'Internet. Ces réseaux pirates de dizaines ou de centaines de milliers de machines Windows enrôlées de force sont responsables de la très grande majorité du spam, ainsi que de beaucoup d'attaques DoS. Il y a donc une activité de recherche intense sur les "*botnets*", notamment pour évaluer leur taille.

Comme les gérants de "*botnets*" ne publient évidemment pas de statistiques fiables, les chercheurs ne doivent donc compter que sur des heuristiques diverses. Le plus célèbre botnet actuel, Storm, est normalement facilement mesurable puisqu'il utilise, pour enregistrer ses machines, une DHT, avec protocole connu, Kademlia, au sein du réseau Overnet. Plusieurs études ont donc annoncé des chiffres sur la taille de Storm, estimée quelque part entre 100 000 machines et bien plus d'un million.

L'article de Kanich, Levchenko, Enright, Voelker et Savage, "*The heisenbot uncertainty problem : challenges in separating bots from chaff*" <http://www.cse.ucsd.edu/~savage/papers/LEETHeisenbot08.pdf> a un point de vue plus nuancé. Selon eux, Storm serait en fait plus petit qu'annoncé, en raison d'un certain nombre d'erreurs systématiques commises dans la mesure. D'abord, Storm partage le réseau Overnet avec des applications légitimes comme mldonkey et toutes les machines enregistrées dans la DHT ne sont donc pas forcément des zombies.

Ensuite, les "*botnets*" attirent justement beaucoup de monde : chercheurs en sécurité, concurrents (puisque les "*botnets*" sont surtout utilisés dans le cadre d'une économie criminelle) et « justiciers » qui essaient de perturber le "*botnet*". Une partie des machines recensées comme faisant partie de Storm sont donc en fait des parasites qui infectent le "*botnet*" pour l'étudier ou l'attaquer (un autre article des mêmes chercheurs, plus facile d'accès, "*When researchers collide*" <http://www.cse.ucsd.edu/~savage/papers/login08.pdf>, détaille ce problème).

En résumé, excellent article, très détaillé sur le fonctionnement du botnet, un domaine bien plus riche qu'on ne pouvait le penser au début.

Donc, sans relativiser la considérable menace que représentent les "*botnets*", il vaut se rappeler que la mesure d'un phénomène clandestin est difficile et que la plupart des chiffres publics sont fournis par... des vendeurs de solutions de sécurité, qui ont tout intérêt à gonfler les chiffres. Le phénomène est donc le même que pour la délinquance classique.

Un bon article sur ce problème de comptage est « "*Lies, Damn Lies, and Botnet Size*" <http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100705> ».