Leet : un botnet IoT plus effrayant que Mirai arrive

Le monde à découvert cette année le côté obscur de l'Internet des objets sous la forme d'un botnet dénommé Mirai capable de mener des attaques massives en déni de services. On se souvient des offensives menées contre le site Krebsonsecurity et contre OVH (qui a observé des pointes jusqu'à plus de 1 Tbps). Et bien évidemment le plus emblématique, le prestataire de DNS Dyn dont l'attaque par saturation avait mis hors service pendant quelques heures des sites comme Netflix, Twitter ou Spotify aux Etats-Unis.

Si le botnet IoT Mirai a depuis évolué avec différentes variantes, la société de sécurité Imperva a déniché, au hasard d'une attaque, un concurrent à Mirai que les experts ont nommé **Leet**. Le 21 décembre dernier, la firme a contré un assaut de 650 Gbps avec plus de 150 millions de paquets par seconde. Selon le blog d'Imperva, l'attaque a été menée en deux vagues sur son réseau. La première a atteint 400 Gbps pendant 20 minutes. Puis après une pause de 5 minutes, le botnet est revenu à la charge avec un niveau de trafic de plus de 650 Gbps pendant 17 minutes. Voyant ses essais repoussés, le botnet a ensuite cessé son activité.

Leet, un botnet distinct de Mirai

Les spécialistes d'Imperva n'ont pas pu tracer ou géolocaliser le botnet Leet car il utilise des adresses IP usurpées. Par contre, ils ont été capables d'analyser la charge utile et quelques indices sur le *modus operandi* du botnet. Concernant l'ampleur du volume de trafic, les soupçons de se trouver en face d'une émanation de Mirai étaient forts. Mais en analysant ce trafic, ils ont trouvé que seulement 0,01% des paquets montrés des similitudes avec Mirai.

Mais les experts constatent d'autres différences. Ainsi, le botnet Leet dispose de deux sortes de payload de type SYN. Le premier comprend des paquets de taille normale soit de 40 à 60 octets, mais le second comprend des paquets de taille moins courante allant de 799 à 936 octets. Mirai lui n'était pas conçu pour mener de grandes attaques SYN. D'autre part, les options TCP comme MSS, SACK, TSVAL, WSS présentes dans Mirai ne le sont pas dans Leet.

1337 comme signature

C'est d'ailleurs dans les options TCP que les experts d'Imperva ont découvert la signature du botnet. Dans le payload SYN de taille normale, plusieurs en-têtes TCP étaient organisés de manière à retrouver les caractères 1337, soit le langage de l'élite (Leet en anglais) en mode ASCII.

Si Imperva n'a pas réussi à déterminer que le botnet utilise des objets connectés pour mener à bien ses assauts, il ne fait aucun doute que c'est bien le cas comme Mirai. Reste que la firme de sécurité estime que ce nouveau botnet ne sera pas le dernier et que 2017 devrait être le théâtre d'attaques beaucoup plus élevées qu'en 2016.

A lire aussi :

DDoS : le code du botnet IoT Mirai mis en libre-service

Rakos, un nouveau botnet IoT en constitution

Photo credit: Jason A. Samfield via VisualHunt / CC BY-NC-SA