L'Internet des objets au service des attaques DDoS

Lancer des attaques DDoS à l'aide d'une armée d'objets connectés à la solde de cybercriminels n'est plus une fiction Le laboratoire de recherche de menaces de l'opérateur Level 3 et la société de sécurité Flashpoint ont travaillé de concert pour traquer les malwares qui visent les objets connectés (via Internet) dans l'objectif de lancer des attaques par déni de service. Attaques qui peuvent impacter n'importe quel serveur en ligne et pas uniquement d'autres éléments propres à l'Internet des objets (IoT).

Ces malwares permettant d'échafauder des bots se nomment notamment Lizkebab, BASHLITE, Torlus ou encore gafgyt. La détection de leur existence remonte même à début 2015, quand leur code a commencé à circuler. Depuis, il a donné naissance à plus d'une douzaine de variantes. Écrits en C, ces logiciels sont conçus pour être facilement compilables et touchent différentes architectures processeurs sous Linux. *« Cela en fait une bonne option pour tourner sur des appareils IoT et autres systèmes embarqués qui utilisent souvent différentes architectures de processeurs pour se conformer aux exigences de coût et de puissance »*, remarque Level 3 sur son blog. Quand un terrain est propice au développement d'un bot, les pirates ne cherchent pas à identifier l'architecture de l'objet, mais lance l'exécution de plusieurs variantes du malware (une douzaine, rappelons-le) en espérant qu'il y en aura une qui se fera comprendre de leur hôte involontaire.

Des attaques à plusieurs centaines de Gbit/s

Systématiquement, le malware implémente un module client/serveur standard. Ensuite, chaque botnet tente de conquérir d'autres objets en cherchant et en exploitant leurs failles de sécurité pour installer les souches infectieuses. Deux modes opérationnels sont utilisés. Le premier, classique, part à la recherche d'un serveur Telnet – administrant légitimement des objets – qu'il tente de pénétrer par force brute (une attaque du couple login/mot de passe). Le second, qui se généralise rapidement, passe en revue le réseau pour repérer de nouveaux objets 'zombies'. *« En dépit d'un manque de sophistication, beaucoup de ces botnets sont capables de produire de puissantes attaques »*, avance Level 3. Qui a pu constater des tsunamis de plusieurs centaines de Gbit/s lancées depuis ce type de botnets.

Plusieurs groupes de cybercriminels, comme Lizard Squad ou Poodle Corp, exploitent ou commercialisent déjà des botnets d'objets connectés pour lancer des attaques par déni de service distribué. Les réseaux de caméras de surveillance, et plus particulièrement les systèmes d'enregistrement numériques des vidéos (DVR), sont particulièrement prisés. Notamment parce que nombre d'entre eux sont déployés avec les identifiants de connexion fournis par défaut et que ces objets sont facilement détectables. Ensuite parce que la bande passante nécessaire au service de communication vidéo offre une capacité d'attaque intéressante aux DDoS

Un million de DVR enrôlés dans un botnet

De fait, Level 3 et Flashpoint ont observé une attaque qui s'est emparée de plus d'un million de DVR, principalement à Taïwan, au Brésil et en Colombie. Dont une large majorité fournie par le constructeur Dahua Technology (que Flashpoint a bien évidemment alerté). Parmi les appareils enrôlés dans ce botnet, les deux partenaires ont déterminé que près de 96% étaient des objets connectés (dont 95% de caméras et DVR), tandis que les routeurs résidentiels ne représentaient environ que 4% des victimes ; les serveurs Linux pesant moins de 1%. *« Cela constitue un changement radical dans la composition des botnets par rapport aux botnets DDoS composés de serveurs et routeurs résidentiels que nous observions par le passé »*, s'inquiète Level 3. La majorité des attaques déclenchées par ces réseaux zombies utilise classiquement les flux UDP et TCP pour noyer leurs victimes (particulièrement des sites et plates-formes de jeux en ligne) sous les requêtes. De plus, la plupart des attaques sont de très courte durée, à peine 2 minutes pour la plupart et moins de 5 minutes dans 75% des cas.

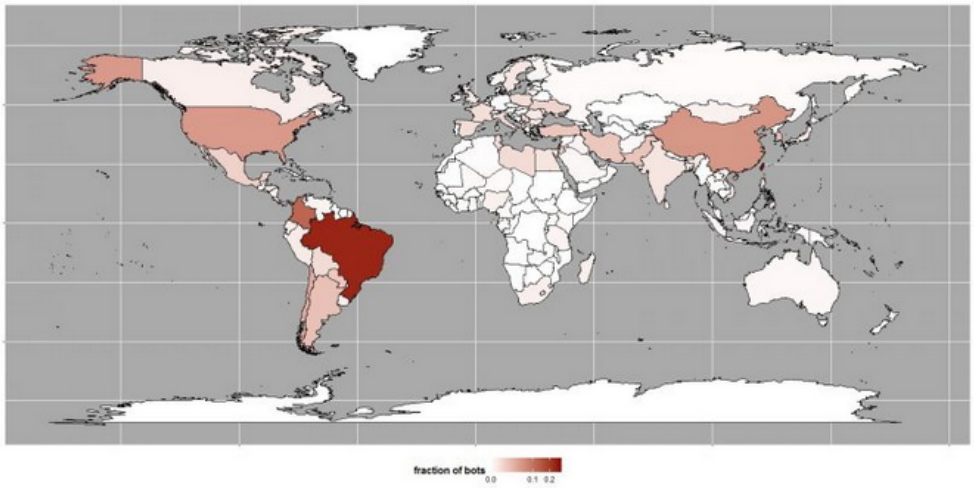

Figure 1 – Global Distribution of gafgyt Bots (Source: Level 3 Threat Research Labs)

« Nous avons vu une variété de mises en œuvre de différents acteurs qui profitent du libre accès au code source [des malwares]. Nous nous attendons à ce que les vecteurs d'infection, les méthodes d'analyse et la sophistication générale continuent à évoluer », préviennent Level 3 et Flashpoint. D'autant que les attaquants profitent aujourd'hui du faible intérêt que les constructeurs, mais aussi les utilisateurs, portent à la sécurisation des objets connectés. Autrement dit, il faut s'attendre à une multiplication des attaques DDoS depuis l'Internet des objets dans les mois et années qui viennent. Un nouvel Eldorado pour les cybercriminels.

Lire également

DDoS : 9 attaques sur 10 sont lancées depuis des services à la demande
Bientôt un Bitcoin pour rémunérer les attaques DDoS ?
Les attaques DDoS en hausse de 40% au 4e trimestre 2015

crédit photo © Duc Dao – shutterstock