Botnet Mirai : Un gamer mécontent derrière l'attaque DDoS contre Dyn

Les experts en sécurité avaient déjà émis des doutes sur le niveau de perfectionnement de l'attaque en déni de service (DDoS) qui a touché le prestataire DNS Dyn, le mois dernier. Et le responsable de la sécurité de Level 3 Communication, Dale Drew, semble leur donner raison. Devant un parterre d'élus américains, il s'est ouvert des résultats de l'enquête menée par sa société sur cette attaque.

Pour rappel, plusieurs sites web dont Amazon, Netflix, Twitter, Reddit, Imgur, Twitter, GitHub , Soundcloud, Spotify, PayPal et autres ont été inaccessibles pendant quelques heures le 22 octobre dernier. En réalité, cette attaque ciblait un prestataire commun à tous ces grands noms, Dyn, qui assure des services de DNS. Ce dernier a expliqué que cette agression avait pour origine un botnet, connu sous le nom de Mirai, capable d'enrôler 100 000 objets connectés (principalement des caméras de vidéo-surveillance). Une attaque spectaculaire par ses répercussions et par le volume de trafic envoyé vers le prestataire.

Pour autant, selon le RSSI de Level 3, il ne faut pas voir là l'œuvre d'un Etat ou d'un groupe de hackers particulièrement bien structuré. « *Nous croyons, en ce qui concerne Dyn, qu'il s'agissait d'un pirate amateur qui cherchait à mettre hors ligne un site de jeux vidéo avec qui il avait un contentieux personnel* », a expliqué Dale Drew. Qui a refusé de donner le nom du site de jeux en question, mais le *Wall Street Journal* croit savoir qu'il s'agit de Playstation Network de Sony.

Mirai, un botnet de 2 millions d'objets connectés « zombies »

Selon Level 3, l'attaquant aurait simplement « *loué* » un botnet Mirai pour mener à bien son offensive. Selon Dale Drew, il a réussi à accéder à un réseau de 150 000 objets connectés « zombies ». Pour le RSSI, il y a quelque chose de rassurant dans le fait que ce piratage ne soit pas le fait d'un attaquant averti. Les premiers soupçons s'étaient tournés vers un Etat au regard du volume de trafic envoyé pour faire tomber Dyn.

Mais, dans le même temps, Dale Drew considère comme très inquiétant la faible sécurité des objets connectés. Pour lui, ces objets disposent de « *mots de passe relativement faciles à pirater, y compris des mots de passe en dur que les propriétaires ne peuvent pas modifier* ». Et d'indiquer que le botnet Mirai a réussi en quelques semaines à contaminer plus de 2 millions d'objets connectés. Une armée gigantesque capable de faire des dégâts importants dans les mains de cybercriminels plus déterminés. Y compris contre des infrastructures considérées aujourd'hui comme bien protégées.

A lire aussi :

Le botnet IoT Mirai s'essouffle victime de son succès

Un botnet Mirai teste sa capacité de nuisance sur le Liberia

crédit photo © Peter Bernik – shutterstock