A louer : un botnet Mirai de 400 000 objets pour lancer des DDoS

Deux hackers affirment disposer d'un botnet Mirai de 400 000 objets infectés, un réseau qu'ils louent en ligne afin de mener des attaques par déni de service distribué (DDoS). Rappelons que le malware Mirai a récemment fait parler de lui en raison de sa capacité à infecter de très nombreux objets connectés (comme des caméras ou des enregistreurs numériques) et à les détourner de leurs usages pour lancer des DDoS massifs, les plus larges à ce jour. Les dernières victimes de Mirai incluent le Français OVH (1,1 Tbit/s, avec peu de conséquences pratiques), le prestataire DNS Dyn (taille de l'attaque inconnue, l'attaque a rendu de très grands sites clients de Dyn, comme Twitter ou PayPal, indisponibles) ou le blog du journaliste spécialisé dans la sécurité Bryan Krebs (620 Gbit/s, le site a lui aussi été submergé).

Suite aux attaques contre OVH et Brian Krebs, le code source de Mirai a été rendu librement disponible sur le Web, aboutissant à la création de multiples botnets à louer. Cette activé est suivie de près par deux chercheurs en sécurité sur le compte Twitter @MiraiAttacks. Selon ces derniers, la quasi-totalité de ces réseaux de machines zombies sont relativement petits. Mais il en existe un largement plus important que tous les autres. « Il compte plus de machines zombies que tous les autres botnets Mirai réunis », affirment les deux chercheurs dans les colonnes de *Bleeping Computer*.

3 000 $ pour 50 000 bots

Au point de réunir plus de 400 000 zombies ? Les chercheurs ne le confirment pas. Mais, dans une campagne de spam via Jabber, deux hackers (dont les pseudos sont BestBuy et Popopret) affirment qu'ils ont à leur disposition un réseau de cette taille, qu'ils présentent comme le « *plus grand* » botnet Mirai. « *Nous utilisons des exploits zero day pour corrompre les machines, et pas seulement des scanners Telnet et SSH* », ajoutent les deux pirates, pour expliquer la taille de leur réseau malveillant.

Selon Bleeping Computer qui a pu échanger avec les deux hackers, les tarifs des DDoS vendus au marché noir par ces deux pirates varient selon le nombre d'objets enrôlés, la période de pause entre deux attaques et la durée des attaques. A titre d'exemple, nos confrères expliquent que Popopret a fixé un tarif de 3 000 à 4 000 dollars pour 50 000 bots menant, pendant deux semaines, des attaques d'une heure, séparées par 5 à 10 minutes de pause. Une fois que l'acheteur a trouvé un accord financier avec les deux pirates, il accèderait à une URL Onion du réseau Tor lui offrant, via Telnet, une interface de contrôle de son botnet.

Un zero day pour faire grossir Mirai

Même si le chiffre de 400 000 objets détournés est difficile à vérifier, ce total marquerait une sérieuse inflation des capacités malfaisantes de Mirai. Le premier botnet bâti à partir du malware – celui ayant attaqué OVH notamment – aurait compté 200 000 objets détournés 'seulement'. Et la très efficace attaque contre Dyn a mobilisé quelque 100 000 bots, selon les éléments fournis par le prestataire DNS. Pour étendre les capacités de Mirai, BestBuy et Popopret expliquent avoir

multiplié les techniques d'infection des objets connectés. En plus de la prise de contrôle via Telnet (sur la base de crédences par défaut imprudemment laissés actives par les constructeurs), les deux hackers affirment avoir enrôlé d'autres terminaux via des attaques par force brute sur le protocole SSH ainsi que via l'utilisation d'une faille zero day affectant un certain type de terminal. Les pirates se sont évidemment refusés à donner le nom et la nature de ce dernier dans leurs échanges avec BleepingComputer.

Popopret affirme également que la version de Mirai que BestBuy et lui ont mise au point est capable de tromper certains systèmes anti-DDoS, en falsifiant l'adresse IP du botnet. Si ces arguments promotionnels restent à vérifier, plusieurs éléments tendent à conforter le sérieux des affirmations des deux pirates.

Sur la piste du Botnet #14

Leur profil tout d'abord : Popopret et BestBuy se trouvant, selon un rapport d'InfoArmor, derrière le malware GovRAT, une souche identifiée en novembre 2015 et qui a servi à dérober de nombreuses informations à des entreprises et administrations américaines du secteur de la défense. Ils figurent aussi parmi les membres actifs du Hell Forum, un forum de pirates de haut vol dont l'un des animateurs présumés a été arrêté au Canada en juin 2015. Par ailleurs, un chercheur en sécurité du nom de MalwareTech, qui anime un outil de suivi des attaques Mirai, a récemment confirmé sur Twitter qu'un botnet créé avec ce malware possédait une fonction permettant d'échapper à certains systèmes anti-DDoS.

De son côté, le compte @MiraiAttacks, dont MalwareTech est aussi un des animateurs, affirme que le botnet Mirai imposant qu'il a identifié –sous l'appellation 'Botnet #14' – est à l'origine d'attaques DDoS assez intenses mais brèves contre les infrastructures télécoms du Libéria. Comme si les pirates à la tête de ce réseau de zombies testaient les capacités de leur canon à requêtes illégitimes…

A lire aussi :

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

DDoS : le botnet IoT Mirai a bien participé au raid contre Dyn

Sécurité et IoT : pourquoi le pire est encore à venir

Crédit photo : Rusty Russ via VisualHunt / CC BY-NC-ND