IoT : les botnets Mirai ont doublé en quelques jours

Fort de ses travaux publiés en août dernier sur les botnets d'objets connectés pour lancer des attaques DDoS (Distributed Denial of Service), l'opérateur Level 3 Communications a poursuivi son étude du malware vedette en la matière, j'ai nommé Mirai. Ce malware qui infecte principalement des DVR (enregistreurs numériques de caméras de surveillance ou de consoles de jeux), mais aussi des serveurs Linux, est d'autant plus intéressant à étudier que son code source a été publié début octobre. Depuis, le nombre de réseaux d'objets connectés à la solde des pirates n'a cessé de croitre, comme on pouvait le craindre.

Près de 500□000 botnets Mirai

Ainsi, avant que le code de Mirai ne soit disponible au plus grand nombre, Level 3 avait recensé 213□000 bots exploitant les méthodes d'infection et d'attaques du malware. Depuis la publication de son code, le nombre des bases de lancement des attaques DDoS a progressé de 280□000. Soit un total de bots Mirai qui frôle les 500□000 aujourd'hui ! Et *« le nombre réel de bots est peut être plus élevé ; nous nous basons sur une vue incomplète de l'infrastructure »*, souligne l'opérateur. Ces réseaux sont capables de lancer des attaques massives par déni de service distribué. Fin septembre, OVH a reconnu avoir essuyé des pics de charge de 1,6 Tbit/s pour protéger plusieurs de ses clients. Et le site du journaliste spécialisé en sécurité Brian Krebs n'a pas tenu la charge, après avoir perdu la protection d'Akamai. Dans le cas de Krebs, la moitié des bots attaquant étaient sous le contrôle de Mirai, confirme Level 3. D'autres malwares s'attaquant aux objets connectés sont également très actifs, dont Gafgyt (Bashlite).

Les Etats-Unis recensent 29% des réseaux d'objets connectés pilotés à distance à des fins malveillantes. Suivis du Brésil (23%) et de la Colombie (8%). L'Europe et la France ne sont pour autant pas épargnées, mais avec des taux d'activité plus faibles. Pour le moment. Mais cela pourrait bien ne pas durer. Car la prolifération grandissante de Mirai risque d'intensifier son action dans de nouveaux territoires. *« Peu de temps après [la] libération [du code de Mirai], le 2 octobre, nous avons commencé à observer des robots se connecter à un autre domaine du serveur de commande et contrôle »*, indiquent les équipes de sécurité de l'opérateur. Entre le 2 et le 5 octobre, Level 3 a repéré 4 nouveaux domaines de serveurs de C&C contre 1 seul constaté avant le 14 septembre. Avec des réseaux qui, derrière, affichent *« des comportements légèrement différents par rapport à la variante originale de Mirai »*.

Nouveaux DDoS en perspectives

Ce qui laisse supposer une déclinaison du code source initial pour de nouvelles formes d'exploitation. *« Avec l'introduction récente et fréquente de nouvelles variantes de Mirai, nous nous attendons à voir progresser l'activité DDoS des botnets Mirai*, prévient Level 3. *La structure de ces botnets évolue au fil des différentes adaptations. Dans certains cas, nous voyons les nouvelles variantes s'exécuter depuis un ou*

deux hôtes, par opposition au Mirai original qui avait de nombreux hôtes différents et changeait souvent d'adresse IP pour éviter la détection ou les attaques. Nous voyons aussi différents mécanismes de distribution de malware, comme dans le cas de swinginwithme.ru. »

Pour limiter les surfaces d'infection et, donc, d'attaques, Level 3 recommande aux constructeurs d'objets connectés de supprimer les services inutilisés sur ces derniers (Telnet en premier lieu) et d'inviter les utilisateurs à en changer les mots de passe. Ce sont généralement en exploitant les identifiants fournis par défaut que les malwares parviennent à s'introduire dans les appareils pour, potentiellement, les transformer en lanceurs d'attaques DDoS.

Lire également

L'Internet des objets au service des attaques DDoS
DDoS : le code du botnet IoT Mirai mis en libre-service
DDoS et IoT : Mirai s'en prend aux objets connectés de Sierra Wireless

crédit photo © Gajus- shutterstock