Thingbots : 4 choses à savoir sur les menaces qui pèsent sur l'IoT

Dans la sixième édition de son rapport The Hunt for IoT, F5 Labs pointe la recrudescence des thingbots, ces objets connectés « zombies ».

Entre octobre 2018 et janvier 2019, ses experts ont relevé l'existence de 26 thingbots contre seulement 6 en 2017 et 9 en 2016. Avec l'émergence de l'Internet des Objets (IoT), de nombreux objets et appareils risquent de se transformer, si ce n'est déjà fait, en thingbot .

« Le nombre de menaces liées à l'IoT continuera d'augmenter tant que les clients n'exigeront pas des stratégies de développement plus sûres de la part des fabricants. Il faudra plusieurs années avant que de nouveaux équipements IoT sécurisés, réduisant la surface d'attaque, aient un impact notable. » indique Sara Boddy, directrice de recherche au F5 Labs.

Toujours à l'oeuvre depuis fin 2016, le botnet Mirai a généré une grande quantité de variantes qui expose plus particulièrement l'Europe.

« 88 % de tous les thingbots connus ont été découverts après le lancement de Mirai, conséquence de l'attention qu'il a suscitée et de la disponibilité de son code source. 46 % de ces découvertes sont des variantes de Mirai, et bon nombre d'entre elles ne se contentent pas de lancer des attaques DDoS : elles sont notamment capables de déployer des serveurs proxy, de miner des crypto-monnaies et d'installer d'autres bots. » détaille F5 Labs.

Dans son rapport, le spécialiste détaille aussi quatre observations importantes sur l'évolution des menaces qui pèsent sur les dispositifs d'objets connectés. Nous les publions dans leur intégralité.

– Les types d'équipements concernés

Les routeurs pour les microentreprises, les caméras IP, les enregistreurs vidéo numérique, les enregistreurs vidéo en réseau et les systèmes de vidéosurveillance en circuits ouverts demeurent les principaux types d'équipements IoT compromis par les thingbots.

Les hackers ne les ciblent pas pour lancer des attaques spécifiques, mais plutôt pour des tests de tentatives de piratage. Compte tenu du volume considérable d'équipements accessibles publiquement, ils sont la cible privilégiée des cybercriminels mais également des experts à la recherche de vulnérabilités de l'IoT.

Les vulnérabilités découvertes seront souvent exploitées par la suite par des acteurs malveillants contrôlant des botnets.

– L'évolution des méthodes d'attaque

Les thingbots visent de plus en plus les équipements IoT utilisant le protocole HTTP, ainsi que les protocoles UPnP, HNAP et SSH exposés publiquement (mais qui ne devraient pas l'être). Parmi les derniers thingbots découverts 30 % ciblent les vulnérabilités et expositions courantes (CVE) des équipements IoT.

– Des attaques peu coûteuses et des possibilités infinies

Une fois un programme malveillant installé sur un équipement IoT, le bot contacte le serveur de

Command and Control et télécharge ses instructions (des attaques DDoS dans la plupart des cas). Par ailleurs, ces thingbots déploient des serveurs proxy pour lancer des attaques, collecter des données à partir de dispositifs liés au trafic, chiffrer le trafic, miner des cryptomonnaies et lancer des attaques d'applications web. Il faut souligner que la vente de services de botnets sort de l'ombre du Dark Web pour s'afficher sur des plateformes grand public comme Instagram.
Certains abonnements à des services de botnets sont proposés pour la modique somme de 5 dollars par mois.

– Un manque d'informations

Peu d'informations sont disponibles au sujet des derniers thingbots découverts. Auparavant, la majorité des thingbots étaient découverts en étudiant le trafic des attaques : le bot, les types d'attaques et les équipements infectés étaient alors identifiés à postériori. Heureusement, aujourd'hui, la communauté de la sécurité découvre les bots *avant* qu'ils ne passent à l'attaque. Toutefois, la communauté de la sécurité a encore plusieurs trains de retard sur les hackers.
Pour véritablement cerner le comportement des pirates, il est nécessaire de pouvoir accéder aux équipements infectés.