Les botnets, une (r)évolution des usages

Les acteurs malveillants créent toujours de nouvelles astuces pour rendre les botnets de plus en plus multifonctionnels et extrêmement volatiles.

A titre d'exemple, le botnet « TheMoon », qui existe depuis 2014, exploite les failles de sécurité et prends le contrôle de routeurs vulnérables et de périphériques IoT pour lancer des attaques DDoS.

Mais dernièrement, un nouveau module a été ajouté au botnet, permettant à l'auteur du botnet de vendre ou de louer son réseau proxy comme un service et ainsi donner la possibilité à d'autres acteurs malveillants de l'utiliser pour lancer des attaques par force brute, obfusquer le trafic ou pour déployer un système de fraude publicitaire vidéo.

Nous avons pu constater que pendant une période de 6 heures, le botnet donnait l'impression que des milliers de personnes cliquaient sur des annonces vidéos sur la plateforme vidéo YouTube grâce à un seul serveur ayant impacté 19000 URLs sur 2700 domaines.

L'heure est à l'émergence d'une nouvelle tendance et d'un nouveau modèle économique avec la monétisation grandissante de botnet-as-a-service.

Les botnets ciblent en priorité l'IoT

L'IoT est aujourd'hui devenu une cible prioritaire, ils sont souvent configurés de manière non sécurisée par défaut. Les cibles sont des routeurs ou des caméras connectées car les constructeurs ne les dotent généralement pas de systèmes d'authentification forte.

En raison du grand nombre d'appareils IoT connectés à Internet, cela crée un surface d'attaque massive.

Gartner estime à 20 milliards le nombre d'objets connectés en 2020, les attaquants peuvent facilement et rapidement rechercher des appareils vulnérables et accumuler de vastes réseaux de zombies. Il devient primordial d'intégrer une dimension de sécurité dès la création de l'objet connecté « security by design ».

Les utilisateurs, quant à eux, doivent s'astreindre à une première étape basique : changer le nom d'utilisateur et le mot de passe par défaut du périphérique connecté à Internet, ces derniers doivent être suffisamment complexes pour être difficilement identifiables.

IDC prévoit 745 milliards de dollars de dépenses IoT dans le monde en 2019, soit une progression de 15,4 % par rapport à 2018.

Les pays les plus friands d'IoT sont les Etats-Unis, la Chine, le Japon, la Corée, l'Allemagne, la France ou encore le Royaume-Uni. A la lumière de ces chiffres, veiller à la sécurité de l'IoT est donc devenue indispensable.

Les cyberattaquants, toujours plus innovants, compétents et mieux financés

Bien entendu, l'évolution de l'usage des botnets n'est pas la seule à dynamiser le secteur des cyberattaques.

Comme l'indique l'Anssi (Agence nationale de la sécurité des systèmes d'information), la menace est croissante et les pirates toujours plus innovants, compétents et mieux financés.

La majorité des attaques demeure encore invisible, ce qui constitue peut-être la plus grosse inquiétude pour les professionnels de la cybersécurité.

En outre, il reste difficile de disposer d'une connaissance complète des attaques, de leur nature et de leur ampleur car ni leurs auteurs ni les victimes ne souhaitent se faire connaître.

Un cybercriminel n'a besoin que d'une attaque précise pour avoir un impact négatif voir dévastateur sur votre entreprise.

Pour se prémunir et se protéger au mieux, les entreprises ont besoin d'une plus grande visibilité globale sur les menaces internes et externes, la mise en place d'un processus de gestion de crise, d'un programme de gouvernance adapté aux réglementations et aux besoins spécifiques de chaque secteur d'activité prenant en charge l'agilité informatique, les réseaux hybrides, la mobilité, le cloud et sensibiliser et former les collaborateurs à l'hygiène informatique.

La collaboration, élément vital pour lutter contre les botnets en constante évolution

Le botnet « Necurs » est actuellement le deuxième plus gros botnet de spam, il est actif depuis au moins 2012 et a été impliqué dans des campagnes massives propageant des programmes malveillants tels que le ransomware Locky, le ransomware Scarab et le cheval de Troie bancaire Dridex.

Necurs emploie un algorithme de génération de domaine (DGA) permettant aux serveurs de commande et de contrôle (C2) et aux réseaux zombies de trouver un autre C2 en cas d'indisponibilité du serveur actuel, ce qui lui a permis de s'étendre à plus de 570,000 robots répartis dans le monde entier.

Grâce à leur capacité à identifier les réseaux de commande et contrôle qui organisent le lancement des attaques, notamment via des botnets, les opérateurs de télécommunication globaux joue un rôle critique dans la lutte contre les cyberattaquants et la protection de l'internet mondial.

L'ampleur de la cybermenace incite les opérateurs globaux à travailler de concert avec d'autres acteurs clés de la cybersécurité pour améliorer constamment le niveau de visibilité sur les acteurs

malveillants et prendre des actions concrètes pour stopper les réseaux C2 qui communiquent avec les réseaux de botnets.

Pour profiter pleinement des avantages de la transformation numérique avec l'adoption du cloud, de l'IoT, de l'Intelligence Artificielle, les entreprises doivent s'assurer qu'elles se transforment en toute sécurité en adoptant une stratégie proactive pour déctecter, prédire et anticiper les cybermenaces actuelles et futures.

En collaborant avec un opérateur global MSSP (Managed Security Service Provider), les entreprises pourront utiliser la visibilité étendue sur les cybermenaces de ce dernier, s'appuyer sur ses équipes d'experts en sécurité et de data scientists qui utilisent l'Intelligence Artificielle et le Machine Learning afin de traiter une grande quantité de données transitant par ses réseaux, analyser les risques, superviser les logs, produire des informations sur les menaces exploitables en temps réel et automatiser la gestion et la réponse aux incidents.

Avec l'arrivée de nouveaux usages liés à la 5G, aux smart cities, aux voitures autonomes, l'élaboration d'une véritable stratégie de défense efficace est pirmordiale afin de renforcer la sécurité de demain.

crédit photo © F.Schmidt – shutterstock