

Les attaques par botnets : modus operandi d'un cybercriminel

Internet

Posté par : JulieM

Publié le : 9/11/2022 13:00:00

Selon le dernier Data Breach Investigations Report (DBIR) publié par Verizon, en 2022 les attaques DDoS restent l'un des principaux types d'incidents identifiés avec les attaques par botnets.

Mirai, Emotet, LemonDuck sont autant de noms qui, hors contexte, pourraient faire sourire, mais qui, dans le monde de la cybersécurité, donnent du fil à retordre aux équipes informatiques des organisations du monde entier, et ce avec des méthodes d'attaques somme toute très simples.

Pour Philippe Alcoy, spécialiste sécurité chez NETSCOUT, bien qu'il semble plus facile de considérer les cybercriminels comme des « gârnies maléfiques », ils ressemblent en réalité à n'importe quel individu lambda cherchant une méthode lucrative qui soit la fois simple et rapide.

C'est pourquoi penser comme eux et remonter à l'origine de ces attaques est nécessaire.

« Les cybercriminels se sont non seulement banalisés aujourd'hui n'importe qui peut s'improviser hacker, grâce aux outils disponibles sur le darkweb mais ils ont également amélioré leurs méthodes d'attaque, pour la plupart établies de longue date, en y apportant de nouvelles modifications et stratégies. C'est le cas des botnets, qui existent depuis les années 1980.

En effet, un rapide historique de ces réseaux de bots informatiques des programmes connectés à internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches, met en évidence la manière dont, en l'espace de 20 ans, les hackers ont modifié leur façon de les utiliser.

Les premiers du genre ont été déployés sur des ordinateurs de type serveur. Par la suite, les attaquants ont commencé à créer des botnets capables de mener des attaques par déni de service distribué (DDoS) en compromettant des ordinateurs personnels (PC) ; ils continuent d'ailleurs aujourd'hui à les utiliser afin de créer des botnets et lancer des attaques DDoS.

À l'heure actuelle, les botnets de l'internet des objets (IoT) sont monnaie courante, les cybercriminels lançant généralement des attaques DDoS par l'intermédiaire de dispositifs IoT, via une infrastructure commune de commande et de contrôle (C2). Ces botnets ont vu leur popularité monter en flèche après la fuite du code source du botnet Mirai en 2016.

Cependant, les acteurs malveillants ont à nouveau modifié leur stratégie en augmentant la taille des botnets IoT et en intégrant des serveurs puissants dans des botnets plus importants.

Les serveurs sont utilisés pour lancer des attaques DDoS ciblées contre des actifs de grande valeur. Toutefois, il est intéressant de remarquer que les attaquants font évoluer leur stratégie pour créer de puissants botnets Mirai.

De nouveaux botnets Mirai de type serveur sont désormais créés et utilisés pour lancer des attaques DDoS directes à fort impact. Ainsi, malgré un coût beaucoup plus élevé pour une

organisation malveillante, les cybercriminels privilégieront une attaque DDoS directe par botnet, pour s'assurer de dommages de très grande envergure, comme l'ont démontrés deux des attaques de plus de 2,5 Tbps détectées au deuxième semestre 2021.

Si ce type d'attaque est coûteux, il est accessible à toute personne ayant les moyens de le provoquer, ce qui en fait un outil redoutable.

Si différentes tendances fluctuent à travers le monde, les attaques DDoS par botnet ne doivent surtout pas être minimisées. Elles constituent bel et bien une menace de taille pour les entités gouvernementales, les établissements de santé et les entreprises, et ce sans distinction.

De plus, si on remarque une sophistication des techniques d'attaque, il est intéressant de noter que les profils des acteurs malveillants sont variés et parfois loin de la professionnalisation ; d'où la nécessité d'anticiper tout type de menace afin de mieux s'en prémunir. »