

Attaques DDoS : Penser comme un attaquant

Internet

Posté par : JulieM

Publié le : 23/5/2022 13:00:00

Le télétravail a considérablement changé les modes de fonctionnement en entreprise. En effet, selon l'Insee, 22 % des salariés français travaillent au moins une fois par semaine.

Cette pratique élargit les modes de communications entre collaborateurs, rendant les environnements numériques de travail accessibles depuis n'importe quel appareil connecté, professionnel comme personnel. Cette accessibilité augmente la surface d'attaque et donc les possibilités de corruption des cybercriminels.

Ces derniers s'appuient en effet désormais sur cette informatique de périphérie pour s'immiscer insidieusement dans les réseaux, soulignant ainsi la nécessité d'adapter les approches de protection des réseaux à ces nouvelles pratiques.

Pour Philippe Alcoy, spécialiste de la sécurité chez NETSCOUT, la part importante des salariés en télétravail nécessite des ajustements que l'informatique de périphérie est capable d'offrir. En revanche, cette dernière présente de nouvelles failles que les cybercriminels exploitent déjà dans les attaques par déni de service distribuées (DDoS) :

« L'adoption d'une architecture de périphérie à edge computing qui rapproche le traitement et le stockage des données de leur source, permet entre autres aux entreprises d'accroître les performances de leur réseau, tout en réduisant la nécessité de renvoyer les données recueillies à la périphérie du réseau vers un datacenter.

Ainsi, plus de la moitié des entreprises seraient susceptibles d'y recourir pour au moins six cas d'utilisation, d'ici fin 2023. Toutefois, si les entreprises se tournent de plus en plus vers la périphérie, les cyberattaquants s'y intéressent également de très près afin d'adapter leurs modes d'attaques aux pratiques en place.

Par ailleurs, outre la lutte contre les attaques par déni de service distribuées (DDoS) à la périphérie, il est également essentiel d'accorder une attention particulière aux attaques DDoS plus granulaires au niveau des applications, cibles de choix pour les cybercriminels qui peuvent bloquer les activités des utilisateurs par ce biais.

Il existe trois types d'attaques DDoS courantes de la couche applicative communément utilisées par les acteurs malveillants : Slowloris, Slow Post et les attaques par épuisement des tables d'état TCP.

Tout d'abord, Slowloris, une attaque de la couche applicative qui utilise des requêtes HTTP partielles pour ouvrir des connexions entre un seul ordinateur et un serveur web ciblé.

Son objectif est de garder ces connexions ouvertes le plus longtemps possible afin de submerger et de ralentir la cible. Ensuite, avec l'attaque de type Slow Post, le cybercriminel envoie des en-têtes HTTP Post itérativement à un serveur web.

Dans les en-têtes, les tailles du corps du message qui suivra sont correctement spécifiées. Cependant, le corps du message est envoyé à une vitesse très lente, avec pour but de ralentir

le serveur.

Enfin, les attaques par épuisement des tables d'état TCP cherchent à consommer les tables d'état de connexion présentes dans de nombreux composants d'infrastructure tels que les routeurs de charge, les pare-feux et les serveurs d'application eux-mêmes. Ces attaques peuvent même détruire des dispositifs de grande capacité permettant de maintenir l'état de millions de connexions.

Les attaques par déni de service distribuées sont de plus en plus courantes et sophistiquées, surtout depuis les changements amenés par le travail en distanciel. Les réseaux, encore soumis à des zones d'ombres en raison des multiples appareils, applications, accès et utilisateurs humains et machines qui y circulent sont toujours plus de vulnérabilités.

C'est pourquoi les équipes IT doivent rivaliser de précision et de réactivité afin de protéger au mieux la pérennité du réseau et ainsi garantir la disponibilité des applications critiques pour l'entreprise ; de même que les cybercriminels continuent de chercher à garder une longueur d'avance sur les entreprises, pour en dérober les informations et bloquer les accès, ces dernières doivent penser comme des attaquants et partir du principe qu'à chaque changement ou nouveauté, elles seront probablement ciblées. En anticipant ces potentielles attaques, elles seront ainsi plus à même de les contrer. »