Introduction

Une attaque par déni de services ou DDOS est une attaque qui vise à saturer le réseaux internet de l'entreprise ou d'un site internet pour le rendre inutilisable par les utilisateurs réels.

1. Fonctionnement des attaques DDoS , qui peut être ciblé?

Les attaques DDoS exploitent généralement un réseau de machines infectées, appelé "botnet", pour submerger une cible de requêtes, rendant ses services indisponibles pour les utilisateurs légitimes. Il y a 3 techniques principales afin d'effectuer une attaque DDoS

-Attaques par saturation de bande passante: Elles inondent la cible avec un volume massif de données, dépassant la capacité du réseau.

-Attaques par épuisement de ressources : Elles visent à épuiser les ressources spécifiques, telles que la mémoire ou les processeurs, d'un serveur ou d'un réseau.

-Attaques au niveau applicatif : Ces attaques ciblent les applications, en envoyant des requêtes légitimes, mais en grand nombre, pour provoquer une surcharge des serveurs.

Qui peut être victime d'une attaque DDoS ?

Les attaques DDoS peuvent cibler un large éventail de victimes, des petites entreprises aux grandes multinationales. Voici quelques catégories de victimes potentielles :

-Entreprises de commerce électronique : Les plateformes de vente en ligne, telles qu'Amazon ou eBay, peuvent être ciblées, causant des pertes financières significatives.

-Fournisseurs de services internet (ISP) : Les fournisseurs peuvent être attaqués, perturbant l'accès à Internet pour des milliers d'utilisateurs.

-Gouvernement et institutions publiques : Les sites web gouvernementaux sont souvent pris pour cible lors de manifestations politiques ou pour exercer des pressions.

-Startups et petites entreprises : Bien que les grandes entreprises soient souvent ciblées, les petites structures peuvent également subir des attaques, n'ayant pas les moyens de déployer des protections robustes.

-Sites web d'activisme ou de médias : Ces sites sont souvent la cible de cyberattaques, particulièrement lorsqu'ils diffusent des informations controversées.

2.Conséquences et impacts des attaques DDoS

Les conséquences des attaques DDoS sont multiples et peuvent avoir un impact significatif sur l'activité d'une organisation :

-Chaque minute d'indisponibilité peut représenter un grand nombre d'argent en pertes de revenus, surtout pour les entreprises qui dépendent fortement de leurs plateformes en ligne.

-L'indisponibilité prolongée d'un service peut entacher la confiance des clients et nuire à l'image de marque.

-Les utilisateurs finaux, qu'ils soient clients ou employés, ne peuvent accéder aux services essentiels pendant l'attaque, ce qui peut perturber des activités critiques.

- En plus des pertes directes, les entreprises doivent souvent dépenser des sommes considérables pour atténuer les effets de l'attaque et renforcer leur infrastructure contre de futures menaces.

-Les attaques DDoS peuvent également servir de couverture pour d'autres attaques plus graves, comme des intrusions visant à voler des données sensibles.

3. Mesures de prévention et de protection

Bien qu'il soit difficile d'éliminer totalement le risque d'une attaque DDoS, plusieurs mesures peuvent être mises en place pour en limiter l'impact :

-Installer un pare-feu et systèmes de détection d'intrusion, ces systèmes peuvent filtrer le trafic anormal et bloquer les attaques en amont.

-Utiliser des réseaux de diffusion de contenu ces réseaux dispersent le contenu d'un site sur plusieurs serveurs géographiquement distribués, diluant ainsi l'impact d'une attaque.

-Les serveurs peuvent être configurés pour limiter le nombre de requêtes qu'un utilisateur peut effectuer dans une période donnée.

-Passer par des Scrubbing centers : Ces centres redirigent le trafic vers une infrastructure spécialisée pour nettoyer le trafic malveillant et renvoyer le trafic légitime à la cible.

-Des services comme Cloudflare ou Akamai proposent des solutions de protection DDoS, en s'interposant entre l'attaquant et la cible pour absorber l'impact de l'attaque.

4. Exemples réels d'attaques DDoS

L'attaque DDoS de 2016 contre Dyn : Cette attaque est l'une des plus célèbres. Les attaquants ont paralysé les serveurs DNS de Dyn, affectant des géants du web comme Twitter, Netflix et Reddit pendant plusieurs heures.

L'attaque de GitHub en 2018 : GitHub a subi une attaque DDoS qui a été atténuée grâce à des mesures avancées de protection DDoS mises en place par Akamai Prolexic.

L'attaque sur les banques françaises en 2020 : Plusieurs banques françaises ont été victimes d'attaques DDoS, perturbant leurs services en ligne pendant plusieurs heures. Ces attaques ont souligné la vulnérabilité des services financiers face à ces menaces.

Conclusion

Les attaques DDoS représentent une menace sérieuse pour l'écosystème numérique mondial. De par leur simplicité d'exécution et leur capacité à causer des dommages massifs. Cependant, grâce aux avancées technologiques, de nombreuses solutions existent pour prévenir, détecter et atténuer ces attaques.Il est donc primordial pour les entreprises de se renseigner dessus afin de s'en prévenir.