Comprendre les attaques DoS et DDoS : leur impact, tendances et stratégies de mitigation

Bernard Sfez - 2024-11-11 15:07

Les attaques par déni de service (DoS) et déni de service distribué (DDoS) comptent parmi les menaces de cybersécurité les plus perturbatrices pour les entreprises et les gouvernements. Ces attaques consistent à saturer un système de requêtes afin de le rendre inaccessible, provoquant ainsi des interruptions de service importantes. Alors que les attaques DoS sont généralement lancées depuis une seule source, les attaques DDoS utilisent de multiples sources, ce qui les rend beaucoup plus difficiles à contrer.

Les récentes tendances révèlent une nette augmentation des attaques, illustrée par l'exploitation en 2023 d'une vulnérabilité critique du protocole HTTP/2. Cet incident a poussé des géants technologiques comme Google et Amazon à déployer des mesures de protection en urgence, comprenant des fermetures de passerelles et des investissements substantiels dans des systèmes d'atténuation pour maintenir la continuité de leurs services.

Cet article examine ces menaces et présente des stratégies clés pour réduire les risques, comme l'utilisation de services de protection DDoS, de protocoles de sécurité réseau, de méthodes d'authentification sécurisées et d'une surveillance proactive. En appliquant ces stratégies, les entreprises peuvent considérablement réduire leur vulnérabilité face à de telles attaques et protéger leurs infrastructures critiques.

Comprendre les attaques DoS et DDoS : leurs impacts et risques potentiels

Pour clarifier, une attaque par déni de service (DoS) ou par déni de service distribué (DDoS) consiste à rendre une machine ou une ressource réseau inaccessible pour ses utilisateurs. En termes simples, les attaques DoS visent à saturer un serveur cible avec un trafic excessif, le rendant inaccessible ou lent pour les utilisateurs légitimes. Une attaque DDoS diffère légèrement en ce qu'elle utilise plusieurs sources, qu'il s'agisse de personnes ou de bots, ce qui augmente exponentiellement son impact.

Source: wikipedia
En informatique, une attaque par déni de service (attaque DoS) est une cyber-attaque dans laquelle l'auteur tente de rendre une machine ou une ressource réseau indisponible pour ses utilisateurs en perturbant temporairement ou indéfiniment les services d'un hôte connecté à un réseau. Le déni de service est généralement réalisé en inondant la machine ou la ressource ciblée de demandes superflues .../...

Dans une attaque par déni de service distribué (attaque DDoS), le trafic entrant qui inonde la victime provient de nombreuses sources différentes. Des stratégies plus sophistiquées sont nécessaires pour atténuer ce type d'attaque ; tenter de bloquer une seule source est insuffisant car il existe de multiples sources...

Tendance des attaques DoS et DDoS (mise à jour 2023)

D’après CVE (catalogue des vulnérabilités et des attaques en cybersécurité), le nombre total d'incidents déclarés comme attaques DDoS a plus que doublé en 2023, passant de plus de 1 000 en 2022 à plus de 2 100 un an plus tard.

Une méthode d'attaque courante consiste à saturer le mécanisme cible avec des demandes de communication externes, à tel point qu’il ne peut pas répondre au trafic légitime, ou répond si lentement qu’il devient pratiquement indisponible. De manière générale, les attaques DoS sont mises en œuvre en forçant l’ordinateur ciblé à se réinitialiser, en consommant ses ressources pour qu’il ne puisse plus fournir le service prévu ou en obstruant le canal de communication entre les utilisateurs et la victime, de sorte qu’ils ne puissent plus communiquer correctement.

L’une des attaques DDoS les plus importantes de 2023 a impliqué l’exploitation d’une nouvelle vulnérabilité dans le protocole HTTP/2, exploitée par une technique appelée « Rapid Reset ». Des entreprises technologiques majeures, dont Google, Amazon et Cloudflare, ont observé des niveaux de trafic record lors de ces attaques en août 2023. Google a atténué une attaque culminant à un niveau sans précédent de 398 millions de requêtes par seconde (RPS), tandis qu’Amazon et Cloudflare ont enregistré des attaques massives similaires avec des pics de 155 millions et 201 millions de RPS, respectivement. World Economic Forum

Bien que les chiffres financiers exacts de cette attaque ne soient pas entièrement divulgués, des experts estiment des coûts potentiels en millions pour les entreprises affectées, couvrant la perte de revenus, les efforts d'atténuation et les dommages à l'infrastructure. Les coûts découlent également des interruptions de service et des réparations d’urgence, nécessitant des mises à jour et des ajustements de protocoles par de nombreux fournisseurs de services pour contrôler l’attaque.

Tactiques Courantes des Attaques DoS

Si la saturation d'un serveur cible par des demandes externes est l'une des méthodes les plus populaires, le simple fait de surcharger sa capacité pour bloquer l'accès légitime suffit souvent à perturber les services. En règle générale, les attaques DoS peuvent être menées en :

- Consommation de Ressources: Surcharge de la capacité du serveur, entraînant son ralentissement, son plantage ou une extinction préventive.
- Redémarrage des Ordinateurs Ciblés: Forcer le redémarrage de la machine cible, interrompant ainsi les services.
- Obstruction de la Communication: Bloquer les canaux de communication entre les utilisateurs et la cible, coupant effectivement l’accès.
- Scénarios Plus Avancés: Les attaques de grande envergure peuvent impliquer du code malveillant envoyé vers un sous-hôte, qui utilise ensuite un botnet—un réseau de robots automatisés—pour inonder la cible de millions de requêtes par seconde. Ce type d'attaque peut viser soit une adresse IP unique (pour des motivations commerciales) soit une plage d’adresses IP (pour des motivations politiques ou militaires).

Découverte de données via des attaques DoS : exploitation indirecte de vulnérabilités

Bien qu’une attaque DoS ne fournisse généralement pas un accès direct aux données, certaines situations peuvent conduire à une exposition involontaire d’informations :

- Cartographie du réseau : Lorsque des systèmes de sauvegarde se déconnectent, les équilibreurs de charge peuvent révéler des informations internes sur le réseau, comme des détails de sous-réseaux ou des noms de machines internes, que les attaquants peuvent utiliser pour cartographier l’infrastructure cible.
- Données des messages d'erreur : Si une attaque DoS interrompt une base de données, des messages d'erreur peuvent exposer des informations critiques, telles que le type de moteur de base de données, les noms d'utilisateur de connexion ou les adresses IP internes.
- Vulnérabilités des API et des logiciels web : Les API ou applications web mal conçues peuvent comporter un paramètre de “fail-open”, permettant un accès non autorisé si le serveur d’authentification unique (SSO) tombe en panne suite à une attaque DoS.
- Opérations de menaces persistantes avancées (APT) : Dans des scénarios APT sophistiqués, les attaquants peuvent lancer des attaques DoS contre les systèmes de détection pour échapper aux alertes de sécurité tout en recueillant des données du réseau.
- Interface d'administration du pare-feu : Une attaque DoS sur les interfaces d'administration du pare-feu peut ralentir les efforts de réponse de l'équipe de gestion réseau.
- Attaques de révocation de clés : Le ciblage des services de révocation de clés peut permettre aux attaquants d'utiliser des identifiants compromis sans être détectés.

Au-delà de la surcharge : le but secondaire des attaques DoS

Les attaques DoS ne visent pas uniquement à faire tomber un service. Souvent, elles servent de "leurre" pour détourner l'attention des équipes informatiques, pendant que d'autres violations plus invasives sont tentées. Cette approche d'attaque à deux volets peut préparer le terrain pour des phases ultérieures plus impactantes d'une attaque.

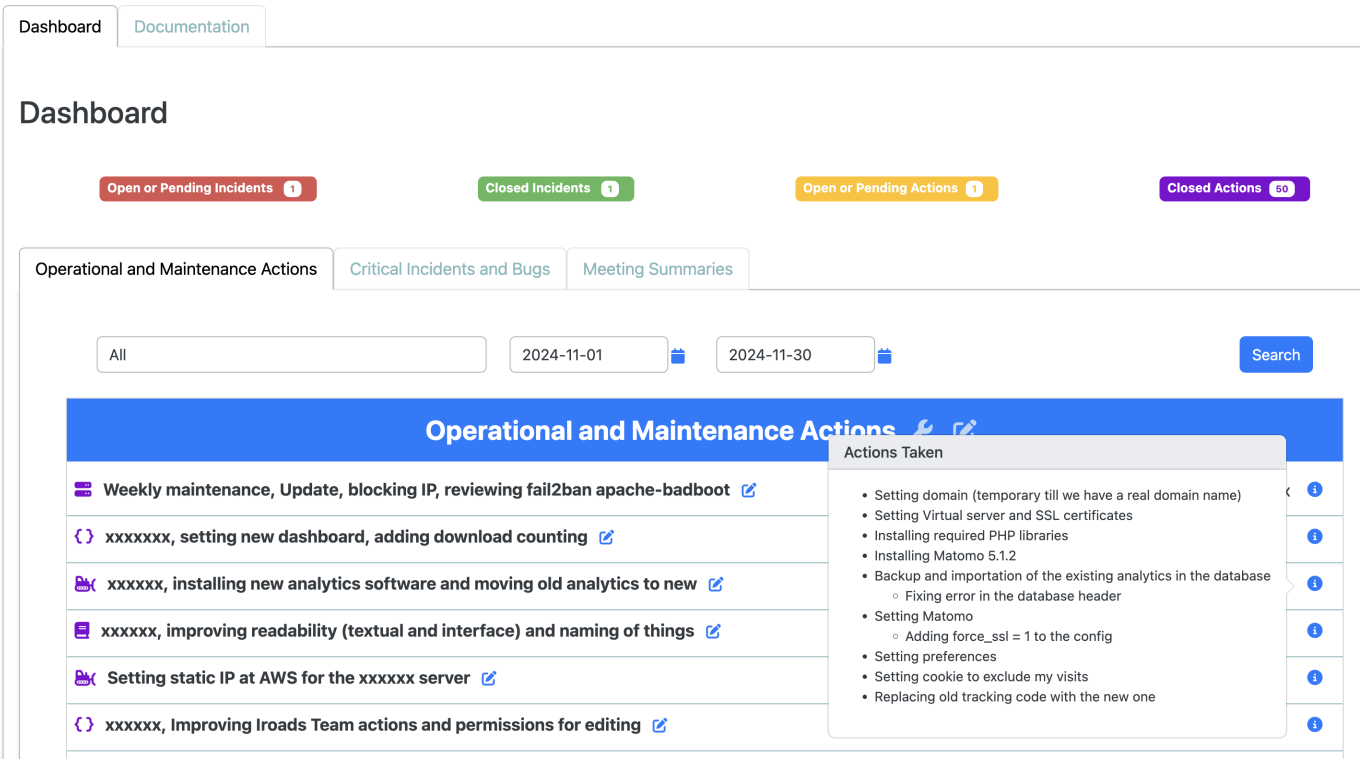
Atténuation des risques DoS : stratégies clés

Pour réduire la probabilité et l'impact d'une attaque DoS, il est essentiel de mettre en place une surveillance précise, une documentation constante et des mesures proactives.

Chez OpenSource Solutions, nous avons mis en place un protocole complet couvrant tous les aspects de la surveillance proactive et de la maintenance. Pour les projets d'envergure entreprise, nous utilisons des outils de surveillance active, accompagnés d'un protocole de maintenance hebdomadaire structuré. De plus, notre approche comprend un protocole de maintenance passé en revue tous les mois, axé sur les éléments clés suivants :

- Services de protection DDoS: Utilisation des systèmes de protection DDoS pour fournir une détection hors bande, une gestion des volumes de trafic élevés, ainsi qu'une identification et une réponse aux attaques.
- Protection du réseau: Nous configurons et ajustons les pare-feu et les règles de bannissement pour fournir une couche de défense cruciale contre les attaques DoS. En appliquant des contrôles d'accès stricts, nous filtrons le trafic malveillant et empêchons l'accès non autorisé aux services. Cette stratégie de contrôle d'accès comprend le blocage des tentatives redondantes d'accès à des ressources inexistantes, l'application du géo-bloquage, et la limitation du taux, avec des mesures adaptées à une analyse détaillée des besoins de sécurité et des contraintes spécifiques du projet.
- Mise à jour et amélioration des composants: Nous maintenons les listes des logiciels, bibliothèques et composants tiers qui permettent à un projet de remplir sa tâche, et nous veillons à ce qu'ils soient régulièrement mis à jour. Cela inclut le suivi des mises à jour des agences de cybersécurité, des organismes gouvernementaux ainsi que des organisations privées de sécurité pour intervenir immédiatement en réponse aux menaces émergentes.
- Authentification et autorisations sécurisées: Authentification à deux facteurs (2FA), mots de passe forts, noms d'utilisateur uniques, noms de groupes clairs et autorisations bien définies.
- Accès au contenu: Grâce à un audit régulier de l'accès aux pages, nous identifions et sécurisons les pages ou zones interdites (administration, pages de test, etc.), en nous assurant qu'elles sont soit supprimées, soit définies comme privées. De plus, nous gérons activement l'accès des crawlers et des robots de recherche, en les autorisant ou en les bloquant selon les besoins pour éviter une utilisation excessive des ressources et améliorer la sécurité.
- Revue des applications web: Les API et les logiciels web doivent être révisés et sécurisés avant d'être accessibles en ligne.
- Surveillance proactive et alertes: Nous utilisons des outils de surveillance avancés et d'alerte qui notifient les administrateurs informatiques des problèmes potentiels en temps réel. Ces outils permettent également d'analyser des comportements plus subtils et insidieux qui pourraient indiquer des vulnérabilités de sécurité ou une dégradation des performances.

Nous suivons et consignons les problèmes et les actions entreprises, en nous assurant que ces informations sont discutées et examinées avec nos clients et partenaires lors de nos réunions hebdomadaires ou mensuelles. Cette approche permet un suivi, de tenir tout le monde informé sur les progrès, les défis et les résolutions, favorisant une communication transparente et une collaboration active.


Dashboard
Documentation
Dashboard
Open or Pending Incidents 1
Closed Incidents 1
Open or Pending Actions 1
Closed Actions 50
Operational and Maintenance Actions
Critical Incidents and Bugs
Meeting Summaries
All
2024-11-01
2024-11-30
Search
Operational and Maintenance Actions
Weekly maintenance, Update, blocking IP, reviewing fail2ban apache-badboot
xxxxxxx, setting new dashboard, adding download counting
xxxxxx, installing new analytics software and moving old analytics to new
xxxxxx, improving readability (textual and interface) and naming of things
Setting static IP at AWS for the xxxxxx server
xxxxxx, Improving Iroads Team actions and permissions for editing
Actions Taken
Setting domain (temporary till we have a real domain name)
Setting Virtual server and SSL certificates
Installing required PHP libraries
Installing Matomo 5.1.2
Backup and importation of the existing analytics in the database
Fixing error in the database header
Setting Matomo
Adding force_ssl = 1 to the config
Setting preferences
Setting cookie to exclude my visits
Replacing old tracking code with the new one