Groupe de travail sur la messagerie, les logiciels malveillants et les anti-abus mobiles

Recommandations initiales du M3AAWG : Armer les entreprises contre les attaques DDoS

Mars 2017

L'URL de référence pour ce document : www.m3aawg.org/DDoS-Recommendations-Business

Table des matières

Introduction 1
Attaques DDoS 1
Se préparer avant que les attaques ne se produisent 2
Pendant une attaque 5
Après une attaque 5
Conclusion 6
Références 6
Glossaire 7

Introduction

Les attaques par déni de service distribué continuent d'être une préoccupation majeure pour les entreprises qui dépendent d'Internet pour le courrier électronique, le marketing, le commerce et le stockage des données. Les perturbations causées par les attaques par déni de service distribué (DDoS) vont de la perte de revenus et de l'augmentation des coûts à l'atteinte dramatique à la marque. Ce guide fournit des concepts et des idées pour aider les entreprises à se préparer aux attaques DDoS. En outre, certaines de ces techniques peuvent également aider les entreprises qui constatent soudainement une forte augmentation du trafic de clients légitimes sur leurs sites Web.

Attaques DDoS

Les attaques par déni de service distribué (DDoS) englobent une grande variété de techniques et peuvent aller des attaques volumétriques de la couche 3 de l'IP aux attaques applicatives de la couche 7. Les sources de ces attaques vont des systèmes compromis qui envoient directement du trafic d'attaque aux sources réfléchies non compromises qui répondent à des paquets IP usurpés.

Les attaques DDoS peuvent être réparties en quatre grandes catégories :[1]

- Volumétrique
- Application
- Épuisement de l'État
- Plan de contrôle

Il existe des dizaines de types d'attaques au sein de ces quatre grandes catégories. La grande majorité des attaques DDoS s'appuient sur des systèmes informatiques compromis, placés sous un système central de commande et de contrôle. Ces

1 Fonash et Glenn 2014

Les ordinateurs infectés sont généralement appelés "bots". Un réseau de robots placés sous un seul système de commande et de contrôle est appelé "botnet". Des organisations de sécurité à but non lucratif recensent des milliers de botnets opérant sur Internet à tout moment. [2]

Les **attaques DDoS volumétriques** peuvent provenir soit de sources directes, soit d'un service réflectif où l'IP source du paquet est falsifiée avec l'adresse IP de la victime. En général, les mécréants exploitent les services réflecteurs pour amplifier le trafic d'attaque et augmenter considérablement la taille de l'attaque. Jusqu'à récemment, les plus grandes attaques volumétriques observées sur l'internet étaient des attaques DDoS à amplification réflective. Cependant, les attaques directes provenant d'un grand nombre de dispositifs IoT non sécurisés ont fait passer les plus grandes attaques DDoS au-dessus du seuil de 1 Tbps. [3]

Les attaques peuvent également être classées comme **directes** ou **indirectes**. Les attaques directes visent une victime (différente des sources directes décrites ci-dessus), tandis que les attaques indirectes visent les services réseau critiques dont la victime a besoin pour que son service fonctionne. Un exemple de ce type d'attaque est que le mécréant cible le service autoritaire ou récursif DNS que la victime utilise.

En général, les **attaques au niveau des applications** sont des attaques de faible volume ; elles s'appuient sur des ordinateurs compromis pour envoyer des demandes au niveau des applications aux systèmes afin de surcharger la victime avec des demandes d'apparence légitime. Les attaques peuvent se dérouler en avant ou en arrière. Une attaque de type applicatif peut tenter de submerger un serveur web en envoyant au site web un grand nombre de requêtes de recherche exigeantes en termes de CPU et de mémoire, tandis qu'une attaque de type inverse peut effectuer un grand nombre de requêtes pour des documents de grande taille situés sur le site web afin de consommer toute la bande passante disponible en amont du site web.

Un nouveau type d'attaque de haut volume au niveau des applications a récemment été observé à partir du 18 mars 2015.[4] Surnommée le " Grand Canon ", il s'agissait d'une attaque de type " man-on-the-side ". Après la modification du code JavaScript analytique du moteur de recherche chinois Baidu, des requêtes de sites Web légitimes sont entrées dans les réseaux chinois et ont envoyé des requêtes d'attaque depuis des ordinateurs non compromis utilisant le code modifié. Ce type d'attaque est inhabituel ; il doit être réalisé soit par un opérateur de réseau, soit par une organisation ayant accès à la plupart du trafic réseau transitant par les réseaux des opérateurs.

Une autre forme d'attaque indirecte vise le service DNS d'un FAI. Les serveurs récursifs ou faisant autorité peuvent être ciblés, ce qui peut provoquer des interruptions de service à grande échelle. L'interruption du service DNS peut avoir un impact considérable sur la clientèle d'un ISP ou d'un fournisseur DNS.

Préparation avant que les attaques ne se produisent

Les entreprises doivent prendre des mesures pour se préparer aux attaques DDoS qui pourraient avoir un impact important sur leurs activités. Ces mesures comprennent des préparatifs internes pour leurs réseaux et leurs serveurs, ainsi que des services supplémentaires d'atténuation des attaques DDoS fournis par leur fournisseur d'accès Internet ou par une société spécialisée dans ce domaine. Les mesures énumérées ci-dessous sont des directives générales et varient en fonction de la taille de l'entreprise, de la taille du réseau de l'entreprise (y compris la capacité de la liaison Internet montante) et du niveau de compétence des employés en matière de DDoS.

Soutien à la gestion

La première étape la plus importante de la préparation à une attaque DDoS est probablement d'obtenir l'adhésion de la direction. Estimez l'impact commercial qui se produirait si une attaque DDoS touchait les opérations de l'entreprise. Combien de temps les services peuvent-ils être interrompus avant que différents niveaux d'impact sur les clients ne se produisent ? Que se passe-t-il si les clients ne peuvent pas

2 https://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts

3 "Mapping Mirai : A Botnet Case Study", 2016.

4 "Utilisation de Baidu pour diriger des millions d'ordinateurs afin de lancer des attaques par déni de service", 2015.

de payer leurs factures ou de commander des produits ? Quel est l'impact d'une interruption de la connectivité Internet et du courrier électronique des employés pendant une période prolongée ? L'entreprise dispose-t-elle de communications hors bande ? N'oubliez pas que lors d'une attaque DDoS, le service téléphonique VoIP fonctionnant sur le même circuit Internet ne fonctionnera pas.

Évaluer les services dépendant de l'Internet
L'étape suivante pour une entreprise consiste à évaluer tous ses services dépendant d'Internet. Examinez l'impact et la perte de revenus potentiels que l'entreprise subirait si ces services devenaient indisponibles. Les services typiques comprennent :

- Portails web de commerce électronique orientés vers le client - pour de nombreux secteurs, ces sites peuvent avoir un impact significatif sur les revenus de l'entreprise s'ils ne sont pas accessibles aux clients.
- Systèmes de messagerie d'entreprise
- Systèmes DNS d'entreprise orientés vers l'Internet
- Systèmes d'accès à distance des employés
- Réseaux VPN qui pourraient être touchés par des attaques DDoS sur Internet

Les entreprises doivent évaluer l'impact que la perte de ces systèmes aurait sur les revenus et la productivité des employés.

Mettre en place des systèmes de surveillance des attaques DDoS
Pour les services importants ou critiques tournés vers l'Internet, des systèmes doivent être mis en place pour surveiller les attaques DDoS et effectuer la journalisation et la capture des paquets lorsque les attaques se produisent. Au cours des premiers stades d'une attaque, les informations relatives à l'attaque peuvent contribuer aux efforts d'atténuation. La possibilité de voir les requêtes web, les demandes de connexion, les journaux de pare-feu, les journaux IPDS et d'effectuer des captures de paquets complets sur le trafic entrant permettra à l'entreprise et à son fournisseur de services d'atténuation des attaques DDoS d'avoir un aperçu du trafic d'attaque. En outre, la surveillance des attaques DDoS par le fournisseur de services de l'entreprise peut être très utile.

Points clés à retenir :
1. Capturez la date et l'heure pour tous les journaux et les captures de paquets.
2. Exécutez un client NTP sur vos systèmes pour vous assurer que vous avez des heures précises.
3. Capturez les adresses IP sources des paquets incriminés.
4. Dans la mesure du possible, effectuez une capture de paquets complets du trafic d'attaque.

Préparation du site de commerce électronique
Les organisations susceptibles d'être touchées de manière significative par une attaque sur leur infrastructure web de commerce électronique doivent préparer le site à une attaque DDoS. Cette préparation comprend :

- Priorité aux fonctions les plus importantes du site
- Création d'un plan dans lequel le site peut fonctionner dans un état de fonctionnalité minimale pour servir les fonctions les plus importantes tout en supprimant des fonctionnalités pour rendre le site Web plus résistant aux attaques DDoS ou aux attaques par épuisement des ressources.

Les attaques DDoS se présentent sous de nombreuses formes. Les choses à prendre en compte pour un site web minimisé :

- **Réduction ou élimination des fonctionnalités dynamiques**. Les fonctions de recherche, les pages Web générées dynamiquement et toute fonctionnalité nécessitant un accès à des ressources dorsales telles que des bases de données permettent à un attaquant d'épuiser facilement les ressources du processeur, du disque ou de la mémoire. Même un site Web conçu pour être amélioré par des réseaux de diffusion de contenu (CDN) ou un service d'atténuation des attaques DDoS ne fonctionnera pas si l'attaquant trouve une URL qui ne peut être servie que par une seule ressource dorsale dynamique. Dans la mesure du possible, présentez aux clients un contenu web statique qui continuera à être servi en cas d'attaque, en particulier la page principale.

- **Réduction des graphiques. Des** graphiques de plus petite taille ou l'élimination de la plupart des graphiques peuvent aider les serveurs Web à fonctionner plus efficacement pendant une attaque.

- **Limitez l'accès aux documents ou fichiers volumineux.** Un type d'attaque DDoS consiste à envoyer des milliers de demandes de documents volumineux à partir du site Web. Cela peut inonder le lien en amont du site web et interférer avec d'autres trafics légitimes.

- **Limiter le nombre de connexions entrantes autorisées sur le site Web.**

Tous les événements à fort volume ne sont pas des attaques DDoS. L'établissement d'un lien entre un site Web largement diffusé et le site Web d'une organisation peut également ressembler à une attaque. [5]

Comme avantage inattendu, toute cette préparation peut également aider les entreprises à gérer les fortes augmentations soudaines du trafic *légitime*.

Préparation du réseau et du serveur

Des travaux préparatoires supplémentaires doivent être envisagés, notamment :

1. Ajout d'une plus grande capacité locale (bande passante ou serveurs) au service attaqué.

2. Déployer des dispositifs d'atténuation des attaques DoS/DDoS sur site et/ou utiliser les capacités anti-DoS du matériel local. Il peut s'agir d'équilibreurs de charge, d'épurateurs de données DDoS locaux, de serveurs DNS dotés de capacités d'atténuation DDoS et d'autres dispositifs spécialisés.

3. Coordination avec les fournisseurs de logiciels et de matériel pour obtenir des conseils sur la configuration optimale des appareils.

4. L'utilisation de réseaux de diffusion de contenu (CDN) pour aider à atténuer les attaques en distribuant les volumes d'attaques sur une vaste infrastructure CDN.

5. Envisagez un serveur de messagerie secondaire ou tertiaire hors site pour stocker le courrier électronique pendant une attaque et pour le récupérer hors site.

6. Veiller à ce que le trafic du plan de contrôle du réseau soit prioritaire par rapport au trafic DDoS.

7. Veiller à ce que le trafic de gestion de l'administration du site Web soit transmis sur un réseau hors bande et une ou plusieurs interfaces de serveur qui ne seront pas affectés par le trafic des attaques DDoS, ou à ce qu'une hiérarchisation de la qualité de service (QoS) et des listes de contrôle d'accès (ACL) du trafic de gestion soient en place pour garantir que le site Web puisse être géré pendant une attaque.

8. Diminuer les TTL des DNS de l'entreprise afin que les adresses IP puissent être rapidement changées si elle prévoit d'utiliser des techniques de blackhole pour atténuer une attaque.

Ne faites pas partie du problème. Trouvez les serveurs NTP ou DNS et les autres services basés sur UDP qui ne devraient pas être exposés à l'extérieur et supprimez-les du réseau ou localisez-les sur un réseau interne afin que ces services ne participent pas aux attaques DDoS réfléchies.

5https://en.wikipedia.org/wiki/Slashdot_effect

Fournisseurs tiers d'atténuation des DDoS
La préparation sur site ne permet pas de se défendre contre les attaques volumétriques à grande échelle qui sont plus importantes que la bande passante de la connectivité de votre réseau à Internet. Ces attaques doivent être atténuées par votre FAI en amont, votre fournisseur d'hébergement ou un fournisseur tiers de services d'atténuation des attaques DDoS. Anticipez et mettez en place un service d'atténuation avant une attaque réelle. En outre, certains services d'élimination du trafic d'attaque fonctionnent mieux si le trafic normal est isolé avant l'attaque. Il est préférable de négocier les contrats juridiques et tarifaires avant une attaque.

Coordination avec les ressources centrales
Les entreprises doivent identifier de manière proactive les points de contact appropriés dans les organisations externes et les avoir contactés avant une attaque DDoS, notamment :

- ISP en amont
- Fournisseur tiers d'atténuation des DDoS
- Organisme chargé de faire respecter la loi
- Équipe nationale d'intervention d'urgence communautaire (CERT)
- Fournisseur d'hébergement
- Autres organisations qui peuvent aider avant, pendant et après une attaque DDoS.

Tester la préparation de l'entreprise
Testez la préparation de l'entreprise pour voir si elle a été bien planifiée. Commencez par un exercice sur papier pour voir si l'entreprise est réellement prête à faire face à une attaque. Comment vont-ils contacter les clients ? Le groupe de communication sera-t-il prêt à diffuser un communiqué de presse sur le sujet ? Quelles mesures d'atténuation seront déployées pour arrêter ou réduire l'attaque ?

Pendant une attaque

- **Capture du trafic d'attaque**
  Soyez prêt à capturer le trafic pendant l'attaque. Les captures de paquets complets peuvent donner un bon aperçu de l'attaque et de sa nature changeante.
- **Mettre en œuvre des stratégies d'atténuation**
  En fonction des caractéristiques de l'attaque, mettre en œuvre des stratégies d'atténuation prédéfinies. Celles-ci peuvent inclure :
  - modifications du site web
  - holing noir
  - le filtrage et les modifications des entrées DNS
  - nettoyage en amont avec le FAI de l'entreprise ou un service tiers d'atténuation des DDoS
  - le nettoyage des données sur place.

Après une attaque

Partager le code, les tactiques, les techniques, les sources d'attaque et les procédures d'attaque capturés avec d'autres organisations susceptibles d'être confrontées à des types d'attaques similaires et avec des organisations de coordination centrale telles que les organisations CERT nationales, les organisations de partage d'informations et éventuellement les forces de l'ordre, le cas échéant. Travailler avec l'opérateur du réseau, le fournisseur d'hébergement, l'organisation de partage de l'information ou le CERT national pour identifier les ordinateurs attaquants et nettoyer les machines du côté distant afin de minimiser la possibilité de futures attaques.

Conclusion

Les attaques DDoS continueront d'affecter de nombreuses entreprises et utilisateurs d'Internet dans un avenir prévisible. Les entreprises qui ne se préparent pas aux attaques pourraient subir un impact important sur leurs opérations, leurs clients et, en fin de compte, une perte de revenus. Les entreprises qui se préparent aux attaques DDoS peuvent réduire considérablement ces impacts. Une planification et une préparation adéquates en coordination avec les fournisseurs de services peuvent non seulement contribuer à atténuer les attaques, mais aussi préparer les entreprises à mieux gérer les augmentations légitimes du trafic sur les sites Web.

Références

Fonash, Peter, et Michael Glenn. "Remediation of Server-Based DDoS Attacks Final Report". Rapport du groupe de travail du Conseil de la sécurité, de la fiabilité et de l'interopérabilité des communications (CSRIC) IV, FCC, Washington DC : FCC. http://docplayer.net/16237406-September-2014-working-group-5-remediation-of-server-based-ddos-attacks-final-report.html

"Mapping Mirai : Une étude de cas de botnet". 3 octobre 2016. Consulté le 7 octobre 2016. https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fiflield, Sarah McKune, Arn Rey, John Scott-Railton, Ronand Deibert et Vern Paxson. 10 avril 2015. "Le grand canon de la Chine". *Citizen's Lab.* Université de Toronto. Consulté le 3 septembre 2015. https://citizenlab.org/2015/04/chinas-great-cannon/

" Utilisation de Baidu pour diriger des millions d'ordinateurs afin de lancer des attaques par déni de service ". 25 mars 2015. Consulté le 3 septembre 2015. https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1.h

Glossaire

AntiDoS	Techniques et dispositifs utilisés pour atténuer les attaques DoS/DDoS.
Blackhole/Blackholing	Également connu sous le nom de "routage nul", le blackholing du trafic réseau permet d'éliminer le trafic malveillant au niveau d'un routeur correctement configuré. Le FAI ou le client envoie une annonce de route qui identifie l'adresse IP de destination à supprimer. Cette annonce peut interrompre le trafic à travers un groupe de routeurs configurés comme des trous noirs. Une variante de cette technique permet de supprimer le trafic en fonction de l'adresse IP source.
Bot	Un dispositif infecté par un logiciel malveillant qui peut être contrôlé à distance.
Botnet	Un groupe de bots qui sont contrôlés à distance par une seule entité.
CERT	Computer Emergency Response Team.
Réseaux de diffusion de contenu (CDN)	Un système de serveurs géographiquement distribués qui répliquent les fichiers et le contenu et fournissent ce contenu aux utilisateurs finaux à partir du serveur le plus proche ou le meilleur. Un CDN peut aider à distribuer et à minimiser l'impact des attaques DDoS, notamment sur le trafic web.
Épuration des données	Activité au cours de laquelle un serveur fait la différence entre le trafic légitime et le trafic d'attaque illégitime, en abandonnant le trafic illégitime et en permettant au FAI d'acheminer le trafic légitime vers la destination appropriée.
Déni de service (DoS) Attaque	Trafic malveillant qui tente de refuser l'accès aux ressources du réseau, du serveur ou de l'application.
Attaque par déni de service distribué (DDoS)	Une attaque DoS dans laquelle le trafic d'attaque provient de (est distribué sur) plusieurs sources, qui peuvent être n'importe quoi, des ordinateurs aux smartphones en passant par les appareils connectés à l'IoT.
Système de noms de domaine (DNS)	Un service internet essentiel qui traduit les noms alphanumériques en adresses IP.
Fournisseur de services Internet (ISP)	Une entreprise ou un organisme qui fournit un accès à l'internet à ses abonnés.
Protocole Internet (IP)	Le principal protocole utilisé pour transmettre des paquets sur Internet.
Internet des objets (IoT)	Terme utilisé pour décrire l'ajout de la connectivité réseau à une variété d'objets physiques pour la communication locale ou la communication à travers l'internet. Parmi les exemples de dispositifs, citons les ampoules électriques, les réfrigérateurs, les machines à laver, les appareils de fitness à domicile, les véhicules, les feux de signalisation, les capteurs d'humidité du sol et bien plus encore. Les principales catégories d'appareils IoT comprennent les appareils grand public, les villes intelligentes, les appareils industriels, les appareils de santé, les appareils gouvernementaux, les appareils financiers, etc.
Système de détection d'intrusion (IDS)	Un système de détection d'intrusion (IDS) surveille les réseaux ou les systèmes pour détecter toute activité malveillante ou inhabituelle.
Système de prévention des Intrusions (IPS)	Un système de prévention des intrusions (IPS) a la capacité d'arrêter, de bloquer ou de répondre aux paquets identifiés. Un IPDS (ou IDPS) combine un IDS et un IPS.

Protocole de temps réseau (NTP)	Protocole utilisé pour synchroniser les horloges sur Internet et sur d'autres réseaux à commutation de paquets. les réseaux commutés.
Amplification par réflexion Le déni de service distribué Service (DDoS)	Une attaque DDoS dans laquelle l'adresse source des paquets IP est modifiée par rapport à l'adresse de l'expéditeur. l'expéditeur réel à l'adresse IP de la victime. Les paquets IP sont ensuite envoyés à un service sur l'internet qui amplifie leur effet. Les paquets IP d'origine sont "réfléchis" Le service légitime est coupé et la réponse est envoyée à la victime de l'attaque DDoS, qui est inondée de paquets IP qu'elle n'a pas demandés. Les protocoles vulnérables les plus courants sont DNS, NTP, SSDP, SNMP et une dizaine d'autres. Certaines des plus grandes attaques DDoS observées sur Internet ont utilisé cette technique.
Tbps	Terabits par seconde
Temps de vie (TTL)	Un champ dans l'en-tête du paquet IP. Le champ TTL est normalement décrémenté à chaque fois que l'IP routeur. Lorsque le TTL du paquet IP atteint zéro, le routeur rejette le paquet. Cela permet d'éviter les boucles de routage où le paquet tourne en boucle.
Contrôle de la transmission Protocole (TCP)	Protocole de réseau qui s'exécute au-dessus du protocole IP afin de fournir un service fiable. méthode de livraison de paquets de données ordonnés.
Protocole de datagramme utilisateur (UDP)	Protocole réseau qui s'exécute au-dessus du protocole IP pour fournir des paquets de données. pour les applications tolérantes aux pertes. Un exemple d'application est une diffusion flux de télévision.
Voix sur IP (VoIP)	Groupe de technologies et de protocoles permettant de transmettre la voix et le multimédia. les communications à travers un réseau à commutation de paquets comme l'internet.
Réseau privé virtuel (VPN)	Réseau privé qui isole les paquets transitant par un réseau public tel que l'Internet. internet. Un VPN peut faire croire que l'utilisateur ou le système est connecté à une réseau privé.

Comme pour toutes les meilleures pratiques que nous publions, veuillez consulter le site Web du M3AAWG (www.m3aawg.org) pour connaître les mises à jour de ce document.

M3AAWG108