Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

Se protéger des attaques par déni de service distribué (DDoS)

Gestionnaires

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

TLP:CLEAR

Canada

Avant-propos

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, veuillez communiquer par téléphone ou par courriel avec le Centre d'appel du Centre pour la cybersécurité :

contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 20 février 2024.

Historique des révisions

Révision	Modifications	Date
1	Première version.	20 février 2024.

ISBN 978-0-660-69851-9
CAT D97-4/80-110-2024F-PDF

Vue d'ensemble

À mesure que la technologie évolue, les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) deviennent de plus en plus répandues et sophistiquées. Ces attaques, couramment utilisées par les cybercriminelles et cybercriminels, peuvent entraîner de graves conséquences financières et opérationnelles, et porter atteinte à la réputation d'organisations dans le monde entier. Quel que soit le type d'attaque par DDoS, le principal objectif de ces attaques consiste toujours à saturer et à neutraliser les serveurs, les services ou les réseaux ciblés en les surchargeant de trafic malveillant provenant de dispositifs ou de réseaux compromis.

Pour être en mesure de se défendre efficacement contre ces menaces, il est essentiel de mettre en œuvre une stratégie de défense qui permettra d'accroître la résilience de votre organisation face aux attaques par DDoS. La mise en œuvre de solutions de protection multicouche évolutives et résilientes constitue un élément crucial de cette stratégie de défense. Pour les organisations ayant des ressources limitées en matière de cybersécurité, il est recommandé d'avoir recours aux services d'un fournisseur de services gérés (FSG). Les FSG spécialisés en cybersécurité offrent leur expertise, des technologies de pointe et une surveillance en tout temps pour détecter rapidement les menaces. Ils réagissent rapidement afin d'atténuer les attaques et d'ajuster les services selon les besoins réseau. La présente publication vise principalement à aider votre organisation à réduire la probabilité et les effets d'une attaque par DDoS ainsi qu'à améliorer votre solution de défense globale en mettant en œuvre des stratégies d'atténuation et en tirant des leçons des attaques par DDoS passées.

Les stratégies d'atténuation définies dans cette publication peuvent également contribuer à améliorer la posture de sécurité globale de votre organisation ainsi que sa résilience; elles peuvent également contribuer à défendre l'organisation contre d'autres types de menaces ou d'attaques.

Table des matières

1 Introduction 5

1.1 Qu'est-ce qu'une attaque par DDoS? 5

1.2 Répercussions potentielles sur l'organisation 5

1.3 Différence entre DoS et DDoS 6

2 Types courants d'attaques par DDoS 7

2.1 Attaques volumétriques 7

2.2 Attaques de protocole 7

2.3 Attaques de la couche application 7

3 Facteurs motivant une attaque par DDoS 9

4 Comment détecter une attaque par DDoS? 10

5 Stratégies d'atténuation pour les attaques par DDoS 11

5.1 Sensibiliser le personnel 11

5.2 Mettre en œuvre un routage par trou noir 12

5.3 Appliquer la limitation de débit 12

5.4 Installer un pare-feu d'applications Web 12

5.5 Assurer une surveillance continue du trafic réseau 12

5.6 Mettre en œuvre l'unidiffusion aléatoire 13

5.7 Mener une évaluation des risques 13

5.8 Élaborer un plan d'intervention en cas d'attaque par DDoS 14

5.9 Collaborer avec un fournisseur de services de protection contre les attaques par DDoS 14

6 Étapes à suivre à la suite d'une attaque par DDoS 16

7 Sommaire 17

8 Contenu complémentaire 18

8.1 Liste d'abréviations, d'acronymes et de sigles 18

8.2 Glossaire 18

8.3 Références 19

1 Introduction

Dans le contexte sans cesse croissant de la cybersécurité, les attaques par déni de service distribué (DDoS) continuent de représenter une menace persistante et grandissante. L'Évaluation des cybermenaces nationales 2023-2024 [1] décrit les attaques par DDoS comme étant un moyen d'extorsion en évolution dont se servent les auteures ou auteurs de menace pour compromettre les organisations canadiennes, quelle que soit leur taille. Ces attaques, menées par des individus ou des groupes dans l'intention de nuire, ont la capacité de perturber et de paralyser les services en ligne en causant des ravages au sein d'organisations, et même d'industries entières.

La présente publication décrit en détail les divers types d'attaques par DDoS, les facteurs qui motivent ces attaques, les moyens utilisés par les auteures ou auteurs de menace et, surtout, les stratégies d'atténuation que peut utiliser votre organisation pour améliorer vos capacités de défense et protéger votre présence en ligne. Afin de protéger votre infrastructure numérique, la première étape essentielle consiste à comprendre ce qu'implique une attaque par DDoS.

1.1 Qu'est-ce qu'une attaque par DDoS?

Une attaque par DDoS est une cyberattaque qui dirige un grand volume de trafic Internet malveillant vers une cible, souvent un site Web ou un service connecté à Internet, afin de la saturer et de la neutraliser. Les auteures ou auteurs de menace, notamment les pirates informatiques, les groupes criminels et les auteures ou auteurs parrainés par des États étrangers, mettent en œuvre leurs attaques afin de perturber les activités normales des réseaux, des services et des sites Web. Les attaques par DDoS entraînent une mauvaise performance ou une panne complète. Une attaque par DDoS peut résulter de l'effort coordonné d'un groupe d'auteures ou auteurs de menace, mais elle peut également être menée par une seule personne au moyen d'un réseau zombie. On entend, par réseau zombie, un grand réseau d'ordinateurs qui ont été compromis ou infiltrés par une ou un pirate informatique pour envoyer massivement à la cible des pourriels dans le but de perturber l'accès à des utilisatrices, utilisateurs ou systèmes légitimes. Ces attaques peuvent perdurer durant une période prolongée (quelques jours, voire des semaines) et s'avérer préjudiciables pour les organisations et les entreprises.

1.2 Répercussions potentielles sur l'organisation

Les attaques par DDoS pourraient avoir des conséquences néfastes pour votre organisation, notamment :

- **Ennuis financiers :** Une attaque par DDoS réussie peut entraîner une perte de productivité, des périodes d'indisponibilité, une perte de revenu et des dépenses importantes pour atténuer les répercussions de cette attaque et reprendre les activités par la suite.
- **Perturbation des opérations :** Les attaques par DDoS peuvent paralyser les activités principales de votre organisation ou empêcher la clientèle d'accéder aux services.
- **Atteinte à la réputation :** Les attaques par DDoS risquent de miner la confiance et la loyauté des clientes et clients. Si ceux-ci ne peuvent pas avoir accès au site Web voulu ou s'ils expriment des doutes quant à sa fiabilité, ils pourraient se voir obligés de privilégier des concurrents.

- **Risques accrus liés à la sécurité des systèmes :** Les attaques par DDoS peuvent révéler des lacunes existantes dans un réseau d'entreprise. Les auteures ou auteurs de menace peuvent tirer parti de ces lacunes pour mener d'autres attaques ou obtenir un accès non autorisé au système.

1.3 Différence entre DoS et DDoS

Bien que les attaques par DDoS et par déni de service (DoS) partagent des noms semblables et des objectifs visant à perturber la disponibilité des réseaux, des services ou des sites Web, elles se distinguent principalement sur le plan de l'envergure et de l'exécution.

Une attaque par DoS est réalisée par une seule source, ou une auteure ou un auteur de menace unique qui cherche à exploiter les vulnérabilités logicielles ou à surcharger un système ou un processus en envoyant à une cible une grande quantité de données ou de demandes. Tout comme pour une attaque par DDoS, elle vise à surcharger la cible dans une mesure telle qu'il lui devient impossible de traiter les demandes d'utilisatrices ou utilisateurs légitimes. Cette situation peut entraîner des retards ou des interruptions de service, ou encore provoquer l'arrêt complet du réseau ou des systèmes ciblés. Pour obtenir de plus amples renseignements sur les attaques par DoS et leurs répercussions sur votre organisation, veuillez consulter la publication Protéger son organisation contre les attaques par déni de service [2].

Contrairement à une attaque par DoS, une attaque par DDoS est plus sophistiquée et implique plusieurs dispositifs connectés qui travaillent ensemble à surcharger la cible. La puissance collective de ce réseau compromis de dispositifs fait en sorte qu'il est difficile de se défendre contre l'attaque, car elle peut arriver à surcharger l'infrastructure réseau et les mesures de sécurité les plus robustes. Non seulement une attaque par DDoS accroît-elle la puissance d'attaque, mais elle rend aussi plus difficile la tâche de déterminer la source réelle de l'attaque.

2 Types courants d'attaques par DDoS

Alors que l'objectif ultime d'une attaque par DDoS est de rendre inaccessible aux utilisatrices et utilisateurs un service en ligne, les méthodes utilisées pour y arriver peuvent varier. Les divers types d'attaques par DDoS ciblent différents éléments d'un réseau et sont classés en fonction des couches de connexion réseau qu'elles exploitent. Les trois types généraux d'attaques par DDoS sont les attaques volumétriques, les attaques de protocole et les attaques de la couche application.

2.1 Attaques volumétriques

Le type le plus courant d'attaque par DDoS est l'attaque volumétrique. Ce type d'attaque se concentre sur les moyens de surcharger le réseau à l'aide de fausses demandes de données et d'affaiblir la bande passante réseau et les capacités de traitement, ce qui rend inutilisables les services aux utilisatrices et utilisateurs légitimes. Cette attaque est souvent menée à l'aide de réseaux zombies. Une attaque volumétrique peut, par exemple, prendre la forme d'une amplification du système de noms de domaine (DNS pour *Domain Name System*), qui utilise des serveurs OpenDNS pour envoyer à la cible un grand nombre de requêtes DNS, occasionnant ainsi une surcharge de trafic. Une attaque par inondation UDP (protocole de datagramme utilisateur; User Datagram Protocol) est un autre type d'attaque par DDoS volumétrique qui consiste à inonder un serveur précis de paquets IP (protocole Internet; *Internet Protocol*) au moyen du protocole UDP. Étant donné que le serveur ne peut pas déterminer la destination ou l'application visée de ces paquets, il répond par des messages de « destination inaccessible ». Cette inondation de trafic UDP peut surcharger le serveur, ce qui entraîne des interruptions de service ou des périodes d'indisponibilité.

2.2 Attaques de protocole

Une attaque de protocole est un type d'attaque par DDoS ayant pour but de perturber un service en exploitant les vulnérabilités dans les protocoles utilisés pour le transfert des données. Elle vise à surcharger les ressources du serveur et/ou les ressources de l'équipement réseau, comme les pare-feu et les équilibreurs de charge. Heureusement, ce type d'attaque laisse des traces faciles à repérer.

L'attaque par inondation de paquets SYN (*Synchronize*) est un exemple d'attaque de protocole. L'auteure ou auteur de menace envoie une succession de requêtes de connexion TCP (protection de contrôle de transmission; *Transmission Control Protocol*) à la cible en se servant d'adresses IP provenant de sources usurpées. Les serveurs ciblés cherchent à traiter les requêtes de connexion, mais au lieu de connexions réussies, la cible se fait inonder d'un grand nombre de requêtes de connexion. Cette inondation de requêtes affaiblit les ressources de la cible en paralysant le système et en l'empêchant d'accepter les connexions légitimes.

2.3 Attaques de la couche application

Les attaques de la couche application ciblent les faiblesses d'une application. Ces attaques touchent surtout le trafic Web et peuvent être difficiles à détecter puisqu'un appareil peut avoir de la difficulté à les différencier du trafic Internet normal à haut volume.

L'inondation HTTP (protocole de transfert hypertexte; *HyperText Transfer Protocol*) est une forme courante d'attaque de la couche application qui rappelle une actualisation répétitive d'un navigateur Web sur de nombreux ordinateurs de manière simultanée. Ce nombre excessif de requêtes HTTP surcharge le serveur, entraînant ainsi un déni de service.

Un exemple d'inondation HTTP est l'attaque Slowloris, qui cible principalement les serveurs Web. Lors d'une telle attaque, l'auteure ou auteur de menace envoie des requêtes HTTP à un serveur Web, mais le traitement de ces requêtes n'est en fait jamais achevé. Périodiquement et lentement, l'auteure ou auteur de menace ajoute des en-têtes pour que la requête demeure active, mais le serveur n'est jamais en mesure de la terminer. Cette stratégie force le serveur Web à garder les connexions ouvertes pour ces requêtes HTTP partiellement achevées, ce qui l'empêche tôt ou tard d'accepter de nouvelles connexions.

Un autre exemple d'attaque de la couche application serait l'injection SQL (langage d'interrogation structuré; *Structured Query Language*). Cette forme d'injection SQL permet aux auteures ou auteurs de menace de manipuler les champs de saisie d'un site Web de façon à forcer la base de données à exécuter des requêtes SQL malveillantes, ce qui consommera la puissance du serveur Web et de la base de données et épuisera les ressources du serveur.

3 Facteurs motivant une attaque par DDoS

Des individus, des entreprises et même des États-nations peuvent être à l'origine des attaques par DDoS, chacun étant motivé par ses propres intérêts. Voici quelques motivations possibles qui sous-tendent les attaques par DDoS :

1. **Hacktivisme** : Les hacktivistes se servent des attaques par DDoS dans le but de sensibiliser à une cause sociale ou politique, ou de la défendre. Les cibles peuvent être autant des gouvernements que des politiciennes et politiciens, ou de grandes organisations.
2. **Extorsion** : L'extorsion est devenue une motivation populaire pour les attaques par DDoS. Les auteures ou auteurs de menace exigent une rançon aux victimes pour mettre fin à l'attaque par DDoS.
3. Convictions idéologiques : Un certain nombre d'auteures ou auteurs de menace qui lancent des attaques par DDoS le font en raison de leurs convictions idéologiques. Il peut s'agir d'individus qui cherchent à perturber des entreprises ou des organisations qu'ils jugent non éthiques, ou à leur causer un préjudice.
4. **Cyberguerre :** La cyberguerre est généralement associée aux États-nations qui parrainent des attaques par DDoS pour obtenir des avantages politiques et militaires. Leur objectif est de perturber les systèmes essentiels financiers, de santé et d'infrastructures au sein de pays ciblés. Ces stratégies demandent l'intervention d'expertes ou d'experts en technologie bien formés, et elles sont associées aux forces armées d'un gouvernement ou à des groupes terroristes. De nombreux gouvernements dans le monde ont investi des ressources considérables pour orchestrer des attaques visant à perturber les infrastructures en ligne et essentielles de leurs adversaires.
5. **Concurrence commerciale :** Les attaques par DDoS sont de plus en plus utilisées comme outil stratégique pour des entreprises concurrentielles. Le recours à de telles tactiques a comme principal objectif de causer des pertes financières ou une atteinte à la réputation de concurrents pour ainsi perturber leurs services et avoir un avantage concurrentiel sur le marché. Ces attaques peuvent se présenter sous diverses formes. Par exemple, elles peuvent empêcher un concurrent de prendre part à des événements en ligne ou perturber complètement ses activités en ligne pendant de longues périodes.
6. **Vengeance :** Des individus ou des groupes qui ressentent de la frustration en raison d'une injustice perçue peuvent lancer des attaques par DDoS à titre de représailles contre une personne ou une organisation.

4 Comment détecter une attaque par DDoS?

La détection d'une attaque par DDoS nécessite de reconnaître les signes pouvant indiquer que votre réseau est menacé. Les situations suivantes pourraient révéler une attaque par DDoS :

- **Augmentation subite et imprévue du trafic Web à partir d'un endroit précis ou d'une adresse IP précise**

  Dans la plupart des cas, ces requêtes de connexion ne peuvent pas être achevées étant donné que la source véritable des paquets IP est cachée.

- **Rendement lent ou irrégulier du réseau, comme des temps accrus de chargement des sites Web**

  Cette situation se produit quand l'auteure ou auteur de menace surcharge le serveur à l'aide d'un volume excessif de requêtes, entraînant ainsi un ralentissement visible du système.

- **Messages d'erreur du serveur inexpliqués, délais d'inactivité ou impossibilité d'accéder à votre site Web**

  Ces problèmes surviennent lorsque l'auteure ou auteur de menace inonde votre serveur en envoyant de nombreuses requêtes. Le serveur est alors surchargé, ce qui occasionne une erreur 503 « Service indisponible », généralement associée à des interruptions de service. Habituellement, cette situation se règle d'elle-même à mesure que diminue le trafic entrant. Toutefois, si le problème persiste, il y a lieu de croire que la situation pourrait être plus grave et qu'il pourrait s'agir d'une attaque par DDoS.

- **Le personnel se plaint de la lenteur de la connectivité**

  Ce point est particulièrement pertinent si le personnel partage avec votre site Web la même connexion réseau. Un tel scénario pourrait signifier que le rendement du réseau est compromis et qu'une attaque par DDoS pourrait en être la cause.

- **Baisse de rendement d'autres services partageant le même réseau**

  Ce problème est souvent dû aux requêtes de l'auteure ou auteur de menace qui surchargent la bande passante disponible du réseau, provoquant ainsi des ralentissements ou des perturbations dans d'autres services.

- **Notification provenant d'un fournisseur d'accès Internet (FAI), d'un fournisseur de services infonuagiques (FSI) ou d'un autre fournisseur de services**

  Vous pourriez recevoir une notification qu'une attaque potentielle par DDoS a été détectée par votre FAI, FSI ou d'autres fournisseurs de services.

5 Stratégies d'atténuation pour les attaques par DDoS

Le principal défi lié à l'atténuation d'une attaque par DDoS consiste à faire la distinction entre le trafic légitime et le trafic malveillant. Cette difficulté découle des différents types d'attaques par DDoS sur Internet. Ces attaques peuvent se présenter sous diverses formes, allant des attaques de source unique aux attaques complexes de sources multiples.

Les attaques par DDoS sophistiquées peuvent tirer parti de multiples voies d'accès pour surcharger une cible, tout en utilisant différents moyens pour détourner les efforts d'atténuation dans ces différentes voies. À titre d'exemple, une auteure ou un auteur de menace peut cibler simultanément de multiples couches de la pile de protocoles, comme en combinant une attaque par amplification DNS à une saturation du protocole HTTP. De façon générale, plus l'attaque est complexe, plus il est difficile de faire une distinction entre le trafic malveillant et le trafic légitime.

Les auteures ou auteurs de menace cherchent à passer inaperçus pour pouvoir contrecarrer les efforts d'atténuation. Afin de contrer efficacement ces attaques complexes par DDoS, vous devez mettre en œuvre une solution de défense multicouche pour tenir compte des différentes voies d'attaque. Votre solution doit être conçue aux fins d'extensibilité, avec des redondances intégrées, et elle doit offrir la possibilité de surveiller le trafic et de gérer efficacement les vulnérabilités. Outre les stratégies de défense contre les attaques par DDoS mentionnées ci-dessous, vous pouvez consulter le document intitulé DDoS Quick Guide [3] de la Cybersecurity and Infrastructure Security Agency pour obtenir des conseils sur les stratégies d'atténuation selon les différentes méthodes d'attaque.

5.1 Sensibiliser le personnel

La sensibilisation du personnel est une partie importante de la stratégie globale en matière de cybersécurité. Un réseau zombie DDoS est une tactique qu'utilisent les auteures et auteurs de menace pour compromettre un réseau de dispositifs en les manipulant à distance dans le but d'inonder une cible par l'envoi d'un volume trop élevé de trafic. Ces auteures ou auteurs peuvent exploiter les dispositifs d'employées et employés peu méfiants à l'aide de cette tactique. Il est important de sensibiliser le personnel afin qu'il comprenne comment protéger leurs dispositifs contre une telle exploitation.

Le personnel peut réduire de façon significative le risque d'être victime d'un réseau zombie en respectant les mesures préventives suivantes et en mettant en œuvre les recommandations décrites dans les documents d'orientation applicables indiqués ci-après.

- Assurez-vous de mettre régulièrement à jour vos dispositifs et logiciels : Application des mises à jour sur les dispositifs (ITSAP.10.096) [4]
- Utilisez l'authentification multifacteur pour protéger vos comptes : Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030) [5]
- Méfiez-vous des courriels suspects et de leurs pièces jointes : Reconnaître les courriels malveillants (ITSAP.00.100) [6]
- Utilisez un antimaliciel de confiance pour protéger vos dispositifs : Protéger votre organisation contre les maliciels (ITSAP.00.057) [7]
- Utilisez un réseau privé virtuel (RPV) reconnu : Les réseaux privés virtuels (ITSAP.80.101) [8]
- Sauvegardez vos dispositifs et vos informations : Sauvegarder et récupérer vos données (ITSAP.40.002) [9]

5.2 Mettre en œuvre un routage par trou noir

La mise en trou noir est une contre-mesure permettant d'atténuer une attaque par DDoS en rejetant le trafic entrant qui est destiné à une adresse IP précise. À l'aide de votre FAI, votre administratrice ou administrateur réseau peut établir une route de trou noir qui dirige tout le trafic réseau vers une route nulle. Toutefois, si le filtrage de trou noir ne comporte pas des critères de restriction précis, il peut acheminer tant le trafic légitime que le trafic malveillant dans le trou noir, retirant ainsi ce trafic du réseau de façon permanente. Cette mesure de prévention est loin d'être idéale, car elle permet essentiellement à l'auteure ou auteur de menace d'atteindre son objectif, soit de rendre le réseau inaccessible et de causer potentiellement des pertes commerciales. Par conséquent, elle doit être considérée en dernier recours lorsque d'autres techniques d'atténuation s'avèrent inefficaces. En dépit de sa capacité d'aider une auteure ou un auteur de menace à atteindre ses objectifs, le routage par trou noir peut quand même s'avérer utile lorsque la cible de l'attaque est un site plus petit au sein d'un réseau plus vaste. Dans de telles situations, le fait de détourner le trafic du site ciblé par la mise en trou noir peut protéger efficacement le réseau plus vaste contre les effets néfastes de l'attaque.

5.3 Appliquer la limitation de débit

La limitation de débit est une autre technique qui permet d'atténuer les attaques par DDoS. Cette technique nécessite la mise en œuvre de restrictions quant au nombre de requêtes qu'un serveur peut accepter provenant d'une adresse IP précise dans une période déterminée. Elle limite le trafic réseau et aide à empêcher les auteures et auteurs de menace de surcharger les ressources du système. La mise en œuvre de la limitation de débit est un moyen efficace de s'assurer que les utilisatrices et utilisateurs légitimes ont toujours accès aux ressources du système, sans entraver le rendement global de l'application. Même si cette approche ne peut à elle seule offrir une protection complète contre les attaques par DDoS de niveau avancé, elle peut quand même constituer un élément important d'une stratégie d'atténuation des attaques par DDoS plus complète.

5.4 Installer un pare-feu d'applications Web

Un pare-feu d'applications Web (WAF pour *Web Application Firewall*) est un outil de défense servant à atténuer les attaques par DDoS de la couche application. Il sert de mandataire inverse et crée un bouclier entre Internet et vos applications. Ce pare-feu aide les spécialistes en sécurité à repérer tout trafic malveillant qui tente de perturber vos services. Un WAF vous permet d'exercer un contrôle sur le trafic entrant, en autorisant ou en refusant l'accès en fonction d'un ensemble prédéfini de règles de sécurité. Vous pouvez commencer par un ensemble de règles de base que vous pouvez par la suite ajuster à mesure que vous détectez des tendances suspectes associées à des attaques par DDoS.

5.5 Assurer une surveillance continue du trafic réseau

La surveillance continue (CM pour *Continuous Monitoring*) et l'analyse en temps réel du trafic sur le réseau procurent plusieurs avantages permettant de repérer et d'atténuer des attaques potentielles par DDoS. La mise en œuvre de systèmes de détection d'intrusion (SDI) et de systèmes de prévention d'intrusion (SPI) pour la surveillance continue du trafic réseau contribue efficacement au repérage et au blocage des tendances suspectes suivies par le trafic et qui seraient liées à des attaques par DDoS. En tirant parti de ces outils d'analyse du trafic, il est possible de faire une détection précoce des attaques par DDoS pour ainsi intervenir rapidement avant l'intensification de ces attaques. La surveillance aide à créer une

base de référence des activités normales sur un réseau ou sur les systèmes informatiques. Cette base doit tenir compte des jours de trafic moyen et des jours de trafic élevé. Elle permet également de mieux comprendre les activités et les habitudes normales du trafic sur le réseau, pour qu'il soit plus facile de faire la différence entre le trafic légitime et le trafic malveillant, et de cerner les activités inhabituelles ou suspectes. Une surveillance ininterrompue permettra également de détecter une attaque imminente, même en dehors des heures normales d'ouverture et les fins de semaine.

5.6 Mettre en œuvre l'unidiffusion aléatoire

Le routage monodiffusion, utilisé largement dans les communications réseau en raison de sa simplicité et de sa polyvalence, sert différentes applications telles que la navigation Web, l'envoi de courriels et le transfert de fichiers. Dans un modèle de monodiffusion, chaque dispositif ou nœud de réseau se voit attribuer une adresse IP unique pour ainsi procurer une communication directe et efface dans tout le réseau. Toutefois, malgré sa simplicité, la monodiffusion n'est pas résiliente face à des attaques par DDoS. Étant donné que le trafic est dirigé directement vers un centre de données précis, une attaque par DDoS est susceptible de surcharger l'emplacement ou son infrastructure avoisinante au moyen de trafic excessif. Cette forte augmentation peut entraîner un déni de service, faisant en sorte qu'il devient difficile de répondre aux requêtes légitimes.

Contrairement au routage monodiffusion, l'unidiffusion aléatoire est plus résiliente en raison de son routage unique et de ses caractéristiques d'adressage. L'unidiffusion aléatoire disperse le trafic entrant sur un réseau de serveurs distribués dans divers emplacements, en utilisant la même adresse IP. Cette méthode permet d'accroître la couverture du réseau, empêchant ainsi qu'un emplacement soit aux prises avec une surcharge de requêtes malveillantes. Quand une adresse reçoit une grande quantité de trafic, comme c'est le cas lors d'une attaque par DDoS, le trafic est automatiquement réacheminé à l'emplacement réseau le plus proche de façon à réduire au minimum les répercussions sur l'infrastructure principale.

L'unidiffusion aléatoire permet d'accroître la résilience du réseau en rendant les attaques plus faciles à gérer, en réduisant les risques de perturbation et, par conséquent, en garantissant la disponibilité ininterrompue du service. En présence d'une configuration réseau à plus grande échelle, il est difficile pour les auteures et auteurs de menace de lancer des attaques par DDoS, car ces attaques nécessitent l'affectation de ressources importantes pour envoyer efficacement du trafic malveillant à l'aide d'un réseau zombie.

5.7 Mener une évaluation des risques

Une évaluation des risques vous permettra d'évaluer la vulnérabilité de votre organisation aux attaques par DDoS. Vous devriez effectuer régulièrement une évaluation des risques et des audits sur votre infrastructure réseau afin d'établir les vulnérabilités. Même s'il est impossible de garantir que vous n'aurez jamais à faire face à une attaque par DDoS, le fait de bien comprendre les ressources matérielles et logicielles de votre organisation, y compris leurs forces et leurs faiblesses, est essentiel pour assurer une protection adéquate. Il est en outre primordial de déterminer les zones les plus vulnérables de votre réseau pour adopter la stratégie la plus efficace qui permettra d'atténuer les répercussions d'une attaque par DDoS.

En effectuant une évaluation des risques, vous serez en mesure de réaliser ce qui suit :

- déterminer les actifs indispensables pour votre organisation et leur importance pour assurer le bon fonctionnement des opérations;

- analyser et évaluer les menaces pour les opérations de votre organisation;
- identifier les vulnérabilités du réseau de votre organisation, ce qui comprend les points faibles que les auteures ou auteurs de menace pourraient exploiter, et évaluer les répercussions et les probabilités d'une attaque par DDoS en fonction de données historiques, de renseignement sur les menaces et des tendances de l'industrie;
- déterminer les différentes voies d'accès que pourraient utiliser les auteures ou auteurs de menace pour lancer une attaque par DDoS, notamment des méthodes telles que la saturation UDP, SYN ou HTTP;
- accorder la priorité aux risques établis en tenant compte de plusieurs facteurs, notamment la probabilité que survienne une attaque, les conséquences possibles de l'attaque ainsi que la probabilité de détecter et d'atténuer l'attaque.

5.8 Élaborer un plan d'intervention en cas d'attaque par DDoS

Pour vous préparer efficacement à une attaque par DDoS, il importe particulièrement de mettre en place un plan d'intervention bien structuré. Ce plan doit comporter des étapes claires qui aideront à détecter et à atténuer une attaque, de même qu'à rétablir les activités. Votre plan doit chercher à réduire le plus possible les répercussions que pourrait subir votre organisation et à assurer le maintien des opérations ou une période minimale d'indisponibilité.

Dans ce plan, vous devez considérer les éléments suivants :

- définir et documenter clairement les rôles et les responsabilités de tous les membres de l'équipe qui vont intervenir à la suite d'une attaque par DDoS, y compris les parties prenantes internes, les leaders organisationnels, les administratrices ou administrateurs de réseau, ainsi que les fournisseurs de services impliqués;
- élaborer une liste de vérification complète qui définit les processus et les mesures à prendre en cas d'attaque par DDoS; préciser les outils et ressources nécessaires et déterminer les personnes qui devront être contactées;
- élaborer un plan de communication robuste qui présente une chaîne de communication prédéfinie à suivre en cas d'attaque par DDoS;
- procéder régulièrement à des exercices d'intervention en cas d'incident et vous assurer que le plan d'intervention en cas d'attaque par DDoS fait partie intégrante de la stratégie globale de reprise après sinistre et du plan de continuité des activités de votre organisation.

5.9 Collaborer avec un fournisseur de services de protection contre les attaques par DDoS

Si votre organisation dispose de ressources limitées pour gérer la cybersécurité, vous devriez envisager de collaborer avec des fournisseurs tiers pour accroître votre défense contre les cybermenaces. Ceux-ci peuvent proposer différents services de défense et de protection, notamment le nettoyage DDoS qui peut contribuer à protéger votre trafic Internet contre une attaque par DDoS. Le nettoyage DDoS consiste à filtrer le trafic entrant pour repérer et supprimer les données malveillantes afin que seul le trafic légitime soit en mesure d'atteindre le réseau ciblé. Votre organisation pourra ainsi maintenir une présence en ligne pendant les attaques, sans interruption de service.

La majorité des FAI et des FSI offrent une certaine protection contre les attaques par DDoS. Vous devez prendre connaissance des mesures de protection que proposent ces fournisseurs et passer en revue l'entente de service pour relever toute restriction potentielle dans leur couverture.

L'utilisation de solutions d'atténuation des attaques par DDoS basées sur l'infonuagique peut comporter également de nombreux avantages, notamment une équipe spécialisée qui peut intervenir plus rapidement en cas d'attaque et une bande passante réseau élevée pour accroître la résilience face aux attaques par DDoS basées sur le volume. Ces solutions peuvent également offrir des options automatisées de reproduction ou de sauvegarde, ce qui vous permet de fournir vos services sans que les utilisatrices et utilisateurs subissent une interruption.

S'il vous faut une solution de protection contre les attaques par DDoS encore plus robuste, pensez à contacter un fournisseur de services gérés (FSG) pour évaluer les solutions qui pourraient être adaptées aux besoins de votre organisation en matière de protection contre les attaques par DDoS. Ces services sont passés maîtres dans l'art de la surveillance du trafic sur le réseau. Ils détectent les signes précurseurs d'une attaque, identifient sa provenance et mettent en œuvre des mesures visant à détourner le trafic nuisible de votre réseau.

Avoir recours à une FSG pour se protéger des attaques par DDoS présente de nombreux avantages. Les FSG spécialisés en cybersécurité offrent leur expertise, des technologies de pointe et une surveillance en tout temps pour détecter rapidement les menaces. Ils réagissent rapidement afin d'atténuer les attaques et d'élargir les services selon les besoins réseau. Les FSG mettent à jour leurs systèmes continuellement afin de garder une longueur d'avance sur les nouvelles menaces et offrent une approche stratégique et efficace afin de préserver les services en lignes. En confiant la protection contre les attaques par DDoD à une FSG, vous permettez à votre équipe de TI de se concentrer sur les activités principales, au lieu de devoir constamment rester à l'affût de possibles cybermenaces et y réagir.

6 Étapes à suivre à la suite d'une attaque par DDoS

Gérer les séquelles d'une attaque par DDoS est une étape importante qui permet d'augmenter la résilience de votre organisation. Une fois l'attaque terminée, il est important d'en évaluer l'impact, de réévaluer votre stratégie de défense et d'améliorer votre planification générale pour pallier d'autres incidents futurs. Voici quelques mesures importantes qu'il est recommandé de prendre pour faciliter ce processus.

- Analysez l'attaque après l'incident en déterminant ce qui suit :
  - Quels actifs et quelle partie du réseau ont été ciblés?
  - Quelle méthode d'attaque par DDoS a été utilisée?
  - Combien de temps a duré l'attaque?
- Continuez à surveiller d'autres actifs réseau pour déceler toute activité inhabituelle ou suspecte qui pourrait indiquer la possibilité d'une attaque subséquente.
- Mesurez l'ampleur des dommages pour comprendre leurs répercussions sur votre organisation et être en mesure de déterminer les ressources nécessaires pour l'application de futures mesures préventives. Voici quelques questions à prendre en considération :
  - Quels services ont été touchés, dans quelle mesure et pendant combien de temps?
  - Quelles ont été les pertes financières encourues?
  - L'attaque a-t-elle nui à la réputation de votre organisation ou a-t-elle donné lieu à des plaintes de la part de la clientèle?
  - L'attaque a-t-elle eu un effet perceptible sur les utilisatrices et utilisateurs?
- Si vous utilisez un fournisseur de services tiers, vérifiez s'il a respecté ses obligations en ce qui a trait aux services d'atténuation d'attaques par DDoS, conformément à l'accord sur les niveaux de service (ANS).
- Maintenez une communication transparente et efficace en informant toutes les parties prenantes, y compris le personnel et la clientèle, de l'attaque, de ses répercussions et des mesures d'atténuation qui sont prises. Faites le point à intervalles réguliers sur l'état de la reprise et les délais prévus pour permettre à toutes et à tous d'être adéquatement informés. Continuez à informer les gens des mesures de sécurité additionnelles qui sont mises en œuvre pour renforcer les mécanismes de défense et prévenir de futures attaques, ce qui viendra confirmer l'engagement de votre organisation à l'égard de la protection des intérêts des parties prenantes.
- Déterminez des façons d'améliorer votre solution de défense contre les attaques par DDoS, ce qui comprend l'évaluation et le renforcement de votre plan stratégique de protection contre les attaques par DDoS en déterminant les causes fondamentales et les vulnérabilités exposées durant l'attaque. Vous devriez examiner des solutions pour renforcer vos mesures de défense, tant au niveau du réseau que des applications. Si vous devez avoir recours à un niveau supplémentaire de protection en raison du nombre limité de ressources internes, il serait bon d'explorer les options d'atténuation basées sur le nuage ou d'utiliser les services de protection contre les attaques par DDoS que peut offrir un fournisseur tiers. De plus, il est essentiel d'effectuer de façon systématique une évaluation des vulnérabilités et des tests de pénétration pour vous assurer de l'efficacité de votre solution de défense.

7 Sommaire

Dans le contexte de la cybersécurité, les attaques par DDoS représentent une menace persistante et croissante, orchestrée par des auteures et auteurs malveillants variés. Ces attaques ont pour objectif de perturber les services en ligne en les surchargeant de trafic Internet malveillant, pouvant potentiellement porter atteinte aux organisations. Les attaques par DDoS se présentent sous différentes formes, notamment les attaques volumétriques qui saturent la bande passante réseau, les attaques de protocole qui exploitent les vulnérabilités dans les protocoles de transfert de données et les attaques de la couche application qui ciblent les faiblesses des applications.

Il est donc essentiel que votre organisation comprenne les effets possibles des attaques par DDoS, comme le dévoilement des faiblesses existantes du réseau, des problèmes d'ordre financier et une atteinte à la réputation. Cette compréhension peut contribuer à mettre en œuvre des stratégies de défense efficaces pour protéger votre infrastructure numérique.
Ces stratégies devraient être régulièrement mises à jour pour s'attaquer aux menaces changeantes et aux changements dans les configurations réseau. Évaluer les conséquences d'une attaque par DDoS donne l'occasion de remettre en question les stratégies de défense, de les améliorer et ainsi de vous préparer à mieux réagir face à des incidents futurs.

8 Contenu complémentaire

8.1 Liste d'abréviations, d'acronymes et de sigles

Abréviation, acronyme ou sigle	Définition
CISA	Cybersecurity and Infrastructure Security Agency;
CM	Surveillance continue (*Continuous monitoring*)
FSI	Fournisseur de services infonuagiques
DDoS	Attaque par déni de service distribué (*Distributed Denial of Service*)
DNS	Système d'adressage par domaines (*Domain Name System*)
DoS	Déni de service (*Denial of Service*)
SDI	Systèmes de détection d'intrusion
IP	Protocole Internet (*Internet protocol*)
SPI	Système de prévention d'intrusion
FAI	Fournisseur d'accès Internet
FSG	Fournisseur de services gérés
OSI	Interconnexion de systèmes ouverts (*Open Systems Interconnection*)
SQL	Langage d'interrogation structuré (*Structured Query Language*)
SYN	Synchroniser
TCP	Protocole de contrôle de transmission (*Transmission control protocol*)
UDP	Protocole de datagramme utilisateur (*User datagram protocol*)
RPV	Réseau privé virtuel
WAF	Pare-feu d'applications Web (*Web Application Firewall*)

8.2 Glossaire

Terme	Définition
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Atout	Dans le domaine de la gestion de l'information, le terme « actif » s'applique, sans toutefois s'y limiter, à l'information sous toutes ses formes et quel que soit son support, aux réseaux, aux systèmes, au matériel, aux actifs immobiliers, aux ressources financières, à la confiance du personnel et du public, et à la réputation internationale. Dans ce contexte, le terme ne s'applique toutefois pas aux ressources humaines.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des biens d'information, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des biens contre les accès non autorisés et les compromissions.

Terme	Définition
Compromission	Divulgation intentionnelle ou non intentionnelle d'information mettant en péril sa confidentialité, son intégrité ou sa disponibilité.
Attaque par déni de service	Toute activité qui rend un système inaccessible aux utilisateurs légitimes ou qui provoque des retards dans les opérations et les fonctions du système.
Détection	Surveillance et analyse des événements d'un système en vue de relever les tentatives d'accès non autorisées aux ressources du système.
Attaque par déni de service distribué	Attaque dans le cadre de laquelle plusieurs systèmes compromis sont utilisés pour attaquer une cible en particulier. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé et l'interruption des services offerts aux utilisatrices et utilisateurs légitimes.
Pare-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre. Les ressources du système local sont ainsi protégées contre un accès de l'extérieur.
Pirate	Personne utilisant des ordinateurs et Internet pour accéder à des ordinateurs et à des serveurs sans autorisation.
Détection des intrusions	Service de sécurité qui surveille et analyse les événements réseau ou système afin d'émettre des alertes lorsqu'il détecte des tentatives d'accès non autorisé. Les résultats sont fournis en temps réel (ou quasi réel).
Maliciel	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les maliciels les plus courants sont les virus informatiques, les vers, les chevaux de Troie, les logiciels espions et les logiciels publicitaires.
Authentification multifacteur (*Multi-Factor Authentication*)	Mécanisme pouvant ajouter une couche supplémentaire de sécurité aux appareils et aux comptes. L'authentification multifacteur exige une vérification supplémentaire (comme un numéro d'identification personnel [NIP] ou une empreinte digitale) pour accéder aux appareils ou aux comptes. L'authentification à deux facteurs est un type d'authentification multifacteur.
Réseau privé virtuel	Réseau de communication privé généralement utilisé au sein d'une organisation ou entre plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisatrices et utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
Évaluation des vulnérabilités	Processus visant à déterminer les faiblesses ou les lacunes existantes dans le cadre des efforts de protection d'un système d'information.

8.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, *Évaluation des cybermenaces nationales 2023-2024*, 28 octobre 2022.
2	Centre canadien pour la cybersécurité, *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*, juillet 2022.
3	Cybersecurity and Infrastructure Security Agency. *CISA's DDoS Quick Guide*, octobre 2020.
4	Centre canadien pour la cybersécurité, *Application des mises à jour sur les dispositifs (ITSAP.10.096)*, mars 2021.
5	Centre canadien pour la cybersécurité, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*, juin 2022
6	Centre canadien pour la cybersécurité, *Reconnaître les courriels malveillants (ITSAP.00.100)*, avril 2022.

Numéro	Référence
7	Centre canadien pour la cybersécurité , *Protéger votre organisation contre les maliciels (ITSAP.00.057)*, juillet 2022.
8	Centre canadien pour la cybersécurité, *Les réseaux privés virtuels (ITSAP.80.101)*, octobre 2019.
9	Centre canadien pour la cybersécurité, *Sauvegarder et récupérer vos données (ITSAP.40.002)*, octobre 2020.