Prévenir les attaques par déni de service distribué et s'y préparer

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2023 | ITSAP.80.110

Les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) sont des cyberattaques au cours desquelles les auteures et auteurs de menace cherchent à perturber l'accès à un système, à un service, à un site Web ou à une application en réseau et à empêcher les utilisatrices et utilisateurs légitimes d'y accéder. Dans le cadre d'une attaque par DDoS traditionnelle, par exemple, des auteures et auteurs pourraient inonder de faux trafic le site Web d'une institution financière ciblée pour nuire aux activités bancaires en ligne de sa clientèle. D'autres attaques par DDoS sont stratégiquement menées en réponse à des événements géopolitiques ou sont utilisées comme technique d'extorsion contre les victimes en submergeant et perturbant les services en ligne de l'organisation ciblée. Les organisations et institutions dans différentes industries et différents secteurs dépendent toutes de ressources réseau et sont de potentielles cibles d'une attaque par DDoS. Advenant une telle attaque, votre organisation pourrait faire l'objet d'une perte de revenus, d'une atteinte à sa réputation, d'un fléchissement dans la confiance accordée par sa clientèle ou par les consommatrices et consommateurs, et de possibles obligations juridiques (lors d'une atteinte à la vie privée). Comme l'ampleur et la complexité des attaques par DDoS ne cessent d'augmenter, il est important que votre organisation prenne les mesures nécessaires pour s'y préparer et les prévenir. La présente publication donne des conseils sur les mesures que vous pouvez prendre lorsque survient une attaque par DDoS et ce que vous pouvez faire pour en atténuer les repercussions.

Quels sont les types d'attaques par DDoS?

Les attaques par DDoS peuvent être lancées par une auteure ou un auteur de menace unique au moyen d'un réseau de zombies composé d'un groupe de dispositifs connectés à Internet possiblement compromis ou mis à profit volontairement. Les attaques par DDoS peuvent également être menées par un groupe coordonné d'auteures et auteurs de menace qui utilise plusieurs machines pour attaquer une même cible. Quelle que soit la méthode, une attaque par DDoS fait en sorte qu'il est plus difficile d'identifier la véritable source de l'attaque et donne lieu à des répercussions plus grandes pour la victime. Les attaques par DDoS appartiennent à trois grandes catégories, selon la partie de la couche réseau qui est ciblée.

Attaques basées sur le volume

Objectif des auteures et auteurs de menace: Utiliser toute la bande passante du réseau et les capacités de traitement en l'inondant de fausses demandes de données. Les attaques par DDoS basées sur le volume sont l'un des types d'attaques les plus courants et elles sont souvent réalisées au moyen de réseaux de zombies .

Exemple: L'amplification du serveur de noms de domaine (DNS pour *Domain Name Server*) est un scénario dans le cadre duquel les auteures et auteurs de menace:

- usurpent l'adresse Web de leur cible
- conçoivent une demande de correspondance de nom de domaine qui amplifie la taille de la réponse (comme demander l'information du domaine et non pas l'adresse IP seulement)
- envoient la demande de nom de domaine à un serveur DNS public avec l'adresse usurpée et le serveur DNS transmet la réponse à la cible

Attaques basées sur le protocole

Objectif des auteures et auteurs de menace: Miner la capacité de traitement des ressources de l'infrastructure réseau de votre organisation, comme les serveurs, les pare-feu et les équilibreurs de charge, en leur envoyant des demandes de connexion malveillantes.

Exemple: L'attaque par inondation de paquets SYN (Synchronize) est un scénario dans le cadre duquel les auteures et auteurs de menace envoient à la cible une quantité excessive et répétée de demandes de connexion par l'entremise du protocole de contrôle de transmission (TCP pour *Transmission Control Protocol*) sans mettre un terme à la connexion. Les ressources des serveurs ciblés sont consommées à attendre la fin des connexions, ce qui occupe le système et l'empêche d'accepter les demandes de connexion légitimes

Attaques basées sur les applications

Objectif des auteures et auteurs de menace: Surcharger certains éléments de l'infrastructure du serveur d'applications, comme les serveurs Web qui sont souvent ciblés par de telles attaques. Les attaques par DDoS basées sur les applications sont moins courantes, mais sont généralement plus complexes et difficiles à détecter, puisqu'elles passent pour du trafic légitime sur le site Web.

Exemple: L'attaque par saturation du protocole de transfert hypertexte (HTTP pour *Hypertext Transfer Protocol*) est un scénario dans le cadre duquel les auteures et auteurs de menace inondent un serveur Web ou une application de multiples requêtes HTTP qui déclenchent un traitement complexe et intensif du côté du serveur

HTTP/2 – Rapid Reset: exemple d'une attaque par DDoS à grande échelle

La vulnérabilité CVE-2023-44487 (en anglais seulement) fournit plus de détails sur la vulnérabilité connue sous le nom de Rapid Reset. Elle a été observée par les chercheuses et chercheurs en sécurité entre août et octobre 2023. Ce type d'attaques exploite une faiblesse du protocole HTTP/2 et pourrait permettre à une auteure ou un auteur de menace d'inonder votre serveur en envoyant, puis en annulant des demandes à maintes reprises. Les auteures et auteurs de menace peuvent manipuler cette vulnérabilité de manière à submerger les sites Web ciblés et à lancer une attaque par DDoS à grande echelle.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Prévenir les attaques par déni de service distribué et s'y préparer

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Décembre 2023 | ITSAP.80.110

Une attaque par DDoS menée contre votre organisation, quelle qu'en soit la taille, peut avoir des répercussions importantes et parfois dévastatrices. Les mesures ci-dessous peuvent aider votre organisation à prévenir les attaques par DDoS et à y remédier efficacement lorsqu'elles surviennent.

Se préparer et prévenir

- ☐ **Définissez un point de comparaison pour l'activité normale du réseau** afin de comprendre ce qui est considéré comme étant acceptable en ce qui concerne le trafic généralement reçu par les hôtes et les nœuds de votre réseau. Vous pourrez ainsi comparer cette information aux niveaux de trafic élevés détectés sur un hôte en particulier.
- ☐ **Déployez des pare-feu d'applications Web (WAF pour *Web Application Firewall*)** pour créer un écran de protection entre vos applications et Internet. Ceux-ci vous permettent de contrôler le trafic entrant en fonction d'un ensemble prédéterminé de règles de sécurité.
- ☐ **Surveillez continuellement le trafic sur votre réseau** en faisant appel à divers outils, comme une solution de gestion des informations et des événements de sécurité (GIES). Vous pourrez ainsi détecter rapidement les anomalies dans les tendances du trafic de données.
- ☐ **Minimisez votre surface d'attaque** en mettant à jour vos dispositifs et votre sécurité, en ayant recours à l'authentification multifacteur (AMF) pour protéger vos comptes et en sensibilisant les utilisatrices et utilisateurs à l'importance de se méfier des courriels d'hameçonnage et des courriels potentiellement malveillants.
- ☐ **Élaborez un plan d'intervention en cas d'incident** qui comprend les processus, les procédures et les renseignements liés aux mesures de détection, d'intervention et de reprise que doit prendre votre organisation.
- ☐ **Effectuez des évaluations et des vérifications régulières** de votre infrastructure pour confirmer que les mesures de sécurité fonctionnent comme prévu et cerner les vulnérabilités de manière à pouvoir les atténuer plus tôt.
- ☐ **Soyez au courant des capacités que votre fournisseur d'accès Internet (FAI) et votre fournisseur de services infonuagiques (FSI)** peuvent fournir pour vous protéger des attaques par DDoS. Passez en revue l'accord sur les niveaux de service (ANS) et assurez-vous que le soutien contractuel nécessaire pour remédier au DDoS est bien en place.

Détecter et analyser

- ☐ **Communiquez avec l'administratrice ou administrateur de votre réseau** pour confirmer si une interruption de service est prévue aux fins d'une maintenance planifiée ou s'il s'agit d'une panne de réseau interne.
- ☐ **Communiquez avec votre FAI et votre FSI** pour vérifier s'il s'agit d'une panne connue ou si leur réseau fait l'objet d'une attaque par DDoS.
- ☐ **Déployez votre équipe d'intervention en cas d'incident** pour collecter l'information nécessaire afin de procéder à une analyse et à une validation rapides de l'incident. Si les ressources organisationnelles le permettent, vous pourriez envisager de faire appel à un fournisseur de services tierce qui possède l'expertise et les outils nécessaires pour analyser et diagnostiquer le type d'attaques par DDoS.

Contenir et éradiquer

- ☐ **Isolez vos réseaux les plus essentiels** de toute connexion à Internet et, dans la mesure du possible, des systèmes interconnectés jusqu'à l'atténuation de toutes les vulnérabilités et la suppression de tous les maliciels.
- ☐ **Mettez en place des contre-mesures de mise en trou noir** pour rediriger le trafic réseau du serveur cible vers un itinéraire nul. Cette technique est efficace dans certaines situations, puisqu'elle permet de protéger vos réseaux plus grands des effets négatifs de l'attaque.
- ☐ **Appliquez immédiatement les correctifs aux systèmes** lorsque les mises à jour sont disponibles.
- ☐ **Limitez l'accès Internet de vos applications Web** en fonction des addresses IP malveillantes connues ou des emplacements géographiques, dans la mesure du possible.
- ☐ **Envisagez le recours aux services d'atténuation des DDoS d'un tiers** pour tirer avantage des outils et de l'expertise de ce dernier et vous aider à contenir et à éradiquer plus rapidement les attaques.

Pour en savoir plus

- ☐ Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)
- ☐ Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)
- ☐ Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085)
- ☐ Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)
- ☐ Étapes à suivre pour déployer efficacement l'authentification multifacteur (ITSAP.00.105)
- ☐ Trafiquage du service de noms de domaine (DNS) (ITSAP.40.021)
- ☐ Cybersecurity and Infrastructure Security Agency's (CISA) DDoS Quick Guide (en anglais seulement)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada