Préparation et réponse à des attaques de déni de service

Première publication : septembre 2011
Dernière mise à jour : mars 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

Introduction

Cette publication a été élaborée par la Direction australienne des signaux (ASD) en collaboration avec le Centre national de cybersécurité de Nouvelle-Zélande (NCSC-NZ), Akamai Technologies Ltd et Cloudflare Pty Ltd, en réponse à la recrudescence des attaques par déni de service (DoS) dans notre région. Elle offre aux organisations des conseils sur les meilleures pratiques d'atténuation, basées sur les techniques de gestion des menaces actuelles, pour se préparer et réagir aux attaques DoS.

Nous vous recommandons de lire ces conseils conjointement avec les publications d'ASD sur les *appareils IoT (Internet des objets)* et *la sécurisation de votre Wi-Fi et de vos routeurs*. Ces publications aident les individus à éviter de contribuer involontairement à des attaques DoS susceptibles d'impacter d'autres personnes.

Les attaques DoS sont des cyberattaques conçues pour perturber ou dégrader des services en ligne tels que les sites web, les messageries électroniques et les services DNS (Domain Name System), afin d'en refuser l'accès aux utilisateurs légitimes. Cela consiste généralement à inonder un service en ligne de données, de connexions ou de requêtes afin de le surcharger et de dégrader ses fonctionnalités.

Les attaques DoS nécessitent généralement un trafic réseau important pour réussir. Elles sont de plus en plus fréquentes, notamment en raison de l'augmentation du nombre d'appareils Internet des Objets (IoT) facilement compromis. Les fabricants d'objets connectés privilégiant souvent l'expérience utilisateur à la cybersécurité, les appareils vulnérables peuvent inclure des appareils domestiques connectés à Internet, tels que des téléviseurs connectés, des bouilloires, des aspirateurs et des systèmes de sécurité. Ces appareils peuvent souvent être compromis à distance par des acteurs malveillants afin de créer un 'réseau d'ordinateurs zombies' à partir duquel générer ce trafic réseau, ce qui peut amener les ménages et les organisations à contribuer involontairement à l'infrastructure permettant les attaques

Les activités récentes indiquent qu'une fois que des acteurs malveillants ont compromis un grand nombre d'appareils IoT, ils peuvent louer ou vendre cette infrastructure à des cybercriminels et des cyberactivistes, de plus en plus enclins à lancer des attaques DoS contre des cibles de leur choix. Dans la plupart des cas, les attaques DoS visent à réduire la productivité et les finances d'une organisation, ou à attirer l'attention du public sur une cause. Un exemple de cette activité est décrit dans l'avis d'ASD *concernant les acteurs liés à la République populaire de Chine qui compromettent des routeurs et des appareils IoT pour des opérations de réseau d'ordinateurs zombies.*

À mesure que notre économie se numérise davantage et que le nombre d'appareils IoT mal sécurisés connectés à Internet augmente, les attaques DoS vont probablement continuer à augmenter.

Pour perturber ou dégrader les services en ligne d'une organisation, les acteurs malveillants utilisent plusieurs approches, notamment :

- diriger un volume important de trafic réseau indésirable vers les services en ligne afin de consommer toute la bande passante disponible ;
- diriger un trafic réseau ciblé vers les services en ligne afin de consommer leurs ressources de traitement ;
- utiliser plusieurs ordinateurs, appareils IoT ou autres appareils connectés à Internet pour diriger le trafic réseau vers les services en ligne depuis plusieurs directions et à une échelle beaucoup plus grande, un type courant d'attaque DoS appelée attaque DoS distribuée (DDoS) ;
- détourner l'enregistrement de domaine ou les serveurs DNS d'une organisation afin de rediriger les utilisateurs légitimes vers les services en ligne de l'organisation.

Les organisations ne peuvent pas éviter d'être la cible d'attaques DoS, mais elles peuvent mettre en œuvre un certain nombre de mesures pour se préparer et potentiellement réduire leur impact. Se préparer aux attaques DoS avant qu'elles ne surviennent est la meilleure stratégie, car sans préparation, il est difficile et moins efficace de réagir lors d'une attaque DoS.

Quoique les organisations se concentrent principalement sur la protection contre les attaques DoS, elles doivent également prendre des mesures pour empêcher que leurs services en ligne et leurs appareils connectés à Internet ne soient utilisés à mauvais escient par des acteurs malveillants pour cibler d'autres acteurs.

Péparation aux attaques DoS

Dans le contexte face à l'augmentation du nombre d'attaques DoS dans notre région, avant de mettre en œuvre des mesures de préparation, votre organisation doit d'abord évaluer ses besoins opérationnels afin de déterminer si chacun de ses services en ligne doit rester opérationnel pendant les attaques DoS, ou si des interruptions de service temporaires sont acceptables.

Si votre organisation souhaite renforcer sa capacité à résister aux attaques DoS, vous devez mettre en œuvre proactivement les mesures suivantes, lorsque cela est approprié et réalisable, avant qu'elles ne surviennent.

- Si votre organisation utilise un réseau de diffusion de contenu (CDN), vous devez mettre en œuvre les mesures supplémentaires suivantes, lorsque cela est approprié et réalisable.
  - Envisagez d'utiliser un réseau CDN incluant des fonctionnalités pour protéger votre serveur web d'origine contre diverses attaques de la couche applicative et réseau ; certains réseaux de diffusion de contenu peuvent inclure ces fonctionnalités dans le cadre d'un pare-feu applicatif web en périphérie.
  - Évitez toute divulgation publique inutile de l'adresse IP (Internet Protocol) de votre serveur web d'origine et assurez-vous que toute exposition publique est protégée contre les attaques DoS.
  - Évitez d'utiliser pour votre serveur web d'origine une adresse IP que des acteurs malveillants pourraient prédire, par exemple une adresse IP appartenant au même sous-réseau que les adresses IP publiquement divulguées de vos services en ligne.
  - Utilisez des contrôles d'accès réseau (comme un pare-feu) pour garantir que seuls les réseaux de diffusion de contenu et de gestion autorisés de votre organisation puissent accéder à votre serveur web d'origine.
  - Envisagez d'utiliser une connectivité réseau diversifiée et résiliente, pouvant inclure une connectivité réseau privée, entre votre serveur web d'origine et votre fournisseur de CDN, si vous avez besoin d'un niveau de protection plus élevé pour votre serveur web d'origine.
  - Configurez les en-têtes HTTP du CDN, du serveur web d'origine et du client afin d'optimiser la mise en cache.
  - Envisagez de partitionner les serveurs web d'origine afin que les requêtes provenant d'adresses IP à faible risque soient traitées séparément des requêtes provenant d'adresses IP à risque plus élevé, si vous avez besoin d'un niveau de disponibilité plus élevé.

- Déterminez les fonctionnalités et la qualité de service acceptables pour les utilisateurs légitimes de vos services en ligne, comment les maintenir et celles qui ne sont pas requises en cas d'attaques DoS.
- Procurez-vous et utilisez un service cloud de mitigation des attaques DoS.
- Envisagez de réduire la surface d'attaque de votre organisation en :
  - externalisant les services en ligne fondamentaux (comme le DNS) auprès de fournisseurs de services réputés, capables de résister aux attaques DoS
  - séparant les services en ligne critiques (comme la messagerie électronique) des autres services en ligne plus susceptibles d'être ciblés (comme les sites web)
  - garantissant que le service de mitigation des attaques DoS autorise uniquement le trafic réseau associé au(x) port(s) réseau du service en ligne
- Discutez avec vos fournisseurs de services des détails de leurs stratégies de prévention et d'atténuation des attaques DoS, notamment :
  - capacité avérée à résister aux attaques DoS du monde entier
  - expérience avérée en matière de gestion des attaques DoS et de tests complets d'attaques DoS autorisées
  - capacité à atténuer automatiquement la plupart des types d'attaques DoS sans intervention humaine, comme l'analyse manuelle du trafic réseau
  - approche de tarification de leurs services, notamment si le coût est fixe ou varie en fonction du volume de trafic réseau et des ressources de traitement informatique utilisées, et si vous pouvez définir une limite de facturation
  - seuils de notification ou de désactivation de leurs services en ligne en cas d'attaque DoS
  - actions pré-approuvées pouvant être entreprises en cas d'attaque DoS
  - accords de prévention des attaques DoS avec les fournisseurs en amont.
- Mettre en œuvre des mesures pour détecter les attaques DoS, telles que la surveillance et l'alerte en temps réel de la disponibilité du système, du trafic réseau, des ressources de traitement informatique et des coûts associés.
- Préparez une version statique de votre site web nécessitant un minimum de traitement et de bande passante afin de garantir la continuité du service en cas d'attaque DoS.
- Procurez-vous et utilisez des services en ligne hautement résilients, dotés d'une bande passante importante, de ressources de traitement informatique adéquates, d'hébergements géographiquement dispersés et d'un système de nettoyage du trafic basé sur le cloud, afin d'éliminer le trafic réseau indésirable. Cela implique généralement l'utilisation d'un CDN réputé pour mettre en cache le contenu statique du site web et protéger votre serveur web d'origine du trafic réseau indésirable.
- Protégez les noms de domaine de votre organisation en utilisant le verrouillage du bureau d'enregistrement, en confirmant l'exactitude des coordonnées d'enregistrement du domaine et des autres informations, et en suivant les conseils complémentaires décrits dans la publication de l'ASD *sur la sécurité du système de noms de domaine pour les propriétaires de domaines*.
- Mettez à jour les coordonnées de vos fournisseurs de services et partagez-les avec eux, en vous assurant que tous les contacts sont disponibles selon les besoins de votre organisation, par exemple 24h/24,7j/7.
- Fournissez à vos fournisseurs de services les coordonnées hors bande de votre organisation pour un canal de communication fiable, en cas de défaillance des canaux de communication habituels.
- Développez, mettez en œuvre et maintenez un plan de réponse aux incidents de cybersécurité, couvrant différents types d'attaques DoS contre chacun de vos services en ligne devant résister à ces attaques, et testez ce plan au moins une fois par an.
- Concevoir des applications pour protéger les fonctionnalités fréquemment utilisées à mauvais escient consommant davantage de ressources informatiques ou générant des coûts supplémentaires (comme l'envoi de SMS).

  - Les protections incluent la limitation du débit et la vérification de l'origine des requêtes.
  - Réalisez des tests d'attaque DoS, notamment en ciblant les flux logiques inappropriés dans les fonctionnalités applicatives.
  - Réalisez des tests de charge plus étendus pour identifier et corriger les vecteurs DoS.

Répondre aux attaques DoS

Si votre organisation n'est pas préparée aux attaques DoS, vous pouvez tenter de mettre en œuvre certaines des mesures ci-dessus lors d'attaques DoS, même si elles peuvent être moins efficaces et prendre du temps, réduisant ainsi la capacité de réponse de votre organisation.

Votre organisation doit mettre en œuvre les mesures suivantes lors d'attaques DoS, lorsque cela est approprié et pratique.

- Mettez en œuvre votre plan de réponse aux incidents de cybersécurité.
- Renseignez-vous auprès de vos fournisseurs de services pour savoir s'ils sont en mesure de mettre en œuvre immédiatement des mesures réactives. Si vous n'avez pas discuté au préalable de leur capacité de réponse, vous pourriez découvrir qu'ils ne peuvent ou ne veulent pas intervenir, ou facturer des frais supplémentaires.
- Désactivez les fonctionnalités non essentielles ou supprimez le contenu non essentiel de vos services en ligne qui rendent l'attaque DoS actuelle efficace, par exemple, déployez une version de votre site web sans fonctionnalité de recherche, sans contenu dynamique ni fichiers volumineux.
- Maintenez la communication avec vos clients et vos fournisseurs de services, y compris votre prestataire de services de mitigation des attaques DoS, et continuez de surveiller la disponibilité de vos services en ligne.
- Envisagez de modifier l'adresse IP de votre serveur web d'origine s'il est directement ciblé et évitez de divulguer publiquement la nouvelle adresse IP sans protection.
- Signalez l'attaque DoS aux parties concernées, notamment à l'ASD et au NCSC-NZ, conformément à la section « Coordonnées » de cette publication.

Éviter de contribuer aux attaques DoS

Votre organisation doit mettre en œuvre les mesures suivantes pour éviter de contribuer involontairement à des attaques DoS susceptibles d'impacter d'autres personnes.

- Évitez d'exposer à Internet des services, des appareils IoT et autres appareils connectés inutiles, mal configurés ou mal entretenus.
- Configurez, maintenez et surveillez en toute sécurité les services, les appareils IoT et autres appareils connectés exposés à Internet.
  - Des conseils supplémentaires pour les petites entreprises sont disponibles dans les publications de l'ASD sur les *appareils IoT* et *la sécurisation de votre Wi-Fi et de vos routeurs*.

Si votre organisation exploite des services en ligne, vous devez mettre en œuvre les mesures supplémentaires suivantes.

- Priorisez la révision des protocoles décrits dans les recommandations de l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) *sur les attaques par amplification UDP*.

- Surveillez les nouveaux vecteurs d'amplification dès leur identification et sécurisez vos services en ligne contre eux.
- Configurez les contrôles d'accès réseau entrants et sortants pour limiter l'accès aux services et organisations en ligne autorisés.
- Bloquez l'accès public anonyme aux services en ligne sujets à l'amplification si cela n'est pas nécessaire.
- Envisagez de mettre en œuvre un mécanisme de limitation du débit pour réduire les conséquences des abus, si le blocage ou l'application de contrôles d'accès n'est pas possible ou approprié.

Éléments de lecture complémentaires

Le *manuel de sécurité des informations* de l'ASD est un cadre de cybersécurité que les organisations peuvent appliquer pour protéger leurs systèmes et leurs données contre les cybermenaces. Les conseils des *Stratégies d'atténuation des incidents de cybersécurité*, ainsi que les Huit Essentiels complètent ce cadre.

Le *Manuel de sécurité des informations de la Nouvelle-Zélande* est le manuel du gouvernement néo-zélandais sur l'assurance de l'information et la sécurité des systèmes d'information. Ce manuel destiné aux praticiens est conçu pour répondre aux besoins des responsables de la sécurité des informations des agences, ainsi que des fournisseurs, sous-traitants et consultants qui fournissent des services aux agences.

De plus amples informations sur les différents types d'attaques DoS sont disponibles dans le *Guide rapide DDoS* et les publications *Comprendre et répondre aux attaques par déni de service distribué » de la CISA* .

Coordonnées de contact

En Australie, si vous avez des questions concernant ces directives, *écrivez à l'ASD ou appelez le* 1300 CYBER1 (1300 292 371).

En Nouvelle-Zélande, pour signaler un incident de cybersécurité, envoyez un courriel à incidents@ncsc.govt.nz ou consultez la page web Signaler un incident du NCSC-NZ.

Avis de non-responsabilité

Les éléments figurant dans ce guide sont de caractère général et ne doivent pas être considérés comme des conseils juridiques ou une forme d'aide dans des circonstances particulières ou dans une situation d'urgence. Pour toute question importante, vous devriez obtenir les conseils d'un professionnel indépendant relativement à vos circonstances spécifiques.

Le Commonwealth n'endosse aucune responsabilité en cas de dommages, de perte ou de dépenses découlant de l'utilisation des informations contenues dans ce guide.

Pour de plus amples informations ou pour signaler un incident de cybersécurité, contactez-nous :

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Vous ne pouvez appeler ce numéro que depuis l'Australie.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre