Protéger son organisation contre les attaques par déni de service

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juillet 2022 | ITSAP.80.100

Les auteurs de menace mènent des attaques par déni de service (DoS pour Denial of Service) dans le but d'entraver la disponibilité des services et des données d'une organisation. Une attaque par DoS fructueuse empêche les utilisateurs d'accéder aux services offerts en ligne (p. ex. le courrier électronique, les sites Web, les comptes en ligne), à l'information et aux autres ressources d'un réseau. Les auteurs de menace lancent des attaques par DoS (ils sont parfois payés pour le faire) pour différentes raisons, que ce soit pour le simple plaisir de mener des attaques, pour tenter de perturber les activités d'une organisation concurrente ou pour entraver les systèmes démocratiques d'un autre pays en période électorale. Les attaques par DoS sont également utilisées par des groupes d'hacktivistes pour protester contre des enjeux politiques ou sociaux.

Les attaques par DoS peuvent cibler une infrastructure en particulier, des applications réseau ou d'autres systèmes, comme les systèmes de contrôle industriels (SCI). Lors d'une attaque par DoS, l'auteur de menace submerge la cible (p. ex. un serveur hébergeant un site Web ou le réseau d'une organisation) en lui envoyant un énorme volume de trafic. Étant ainsi surchargée, la cible n'est plus en mesure de traiter le volume excessif de trafic, ce qui mène souvent au plantage du système. Dans ce cas, un utilisateur peut recevoir un message d'erreur lorsqu'il tente d'accéder à un site Web. Les auteurs de menace utilisent différentes méthodes pour leurs attaques par DoS:

- **Attaque par inondation** – L'attaque par inondation est la méthode la plus couramment employée. L'auteur de menace bombarde le serveur ciblé de demandes de connexion sans jamais s'y connecter. Ces procédures de connexion incomplètes occupent et consomment toutes les ressources disponibles du serveur. Ainsi, le serveur ne parvient plus à traiter ni le trafic ni les demandes de connexion légitimes.
- **Attaque par arrêt de service** – Les attaques par arrêt de service sont moins courantes. Dans de tels cas, l'auteur de menace tente d'exploiter les failles du système ciblé pour provoquer une panne.

Attaque par déni de service distribué

Une attaque par déni de service distribué (DDoS pour Distributed Denial of Service) a le même objectif, soit celui de perturber ou d'empêcher l'accès aux services et aux informations, mais elle se distingue quelque peu du simple DoS. Dans le cadre d'un DDoS, un auteur de menace a recours à plusieurs machines pour attaquer une cible. Une attaque par DDoS peut résulter de l'effort coordonné d'un groupe d'auteurs de menace, mais elle peut également être menée par une seule personne faisant appel à un réseau de zombies. En plus d'accroître la puissance de l'attaque, le DDoS fait en sorte qu'il est plus difficile d'en identifier la véritable source.

Le document *Security Tip* (ST04-015) (en anglais seulement) publié par la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis mentionne que le nombre d'attaques par DDoS a augmenté avec l'utilisation grandissante de l'Internet des objets (IdO). Les contrôles de sécurité et les capacités de chiffrement des appareils IdO actuels sont faibles, ce qui les expose à d'éventuelles menaces et les rend vulnérables à l'exploitation.

Consultez le document *DDoS Quick Guide* (en anglais seulement) de la CISA pour de plus amples renseignements sur les méthodes d'attaque, les possibles répercussions et les stratégies d'atténuation applicables.

Par **réseau de zombies,** on entend un groupe d'appareils connectés à Internet que l'on a préalablement piratés. Pour créer un réseau de zombies, un auteur de menace doit être en mesure d'exploiter les failles de sécurité ou les lacunes des nombreux dispositifs qu'il cherche à contrôler. Pour éviter que vos systèmes et vos appareils soient exploités par un réseau de zombies, il convient d'y installer les mises à jour et les correctifs de sécurité dès qu'ils sont disponibles.

Répercussions d'une attaque par DoS

Les attaques par DoS sont conçues pour monopoliser toutes les ressources de votre réseau, notamment la bande passante, la puissance de traitement, la mémoire et les zones de stockage.

En plus de perturber l'accès à vos services et à vos ressources, l'attaque par DoS peut servir de diversion, pendant que l'auteur de menace mène d'autres attaques, notamment des tentatives de vol de données.

Votre organisme pourrait également subir les répercussions suivantes :

- Coûts associés aux interventions visant à contrer l'attaque par DoS
- Perte de fonctionnalité intégrale ou partielle sur les services touches
- Diminution de la productivité

Il n'est pas nécessaire que votre organisation soit la cible directe d'une attaque par DoS pour être touchée. En effet, lorsque vos fournisseurs de services (p. ex. votre fournisseur d'accès Internet ou de services infonuagiques) font l'objet d'une attaque, votre organisation peut devoir composer, à son tour, avec des pertes de services.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Protéger son organisation contre les attaques par déni de service

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juillet 2022 | ITSAP.80.100

Reconnaître une attaque par DoS

Soyez à l'affût des signes qui pourraient indiquer que vos systèmes ont été la cible d'une attaque par DoS :

- Ralentissement considérable des fonctions réseau, notamment lorsqu'il s'agit d'ouvrir un fichier ou d'accéder à un site Web
- Sites Web hors service ou inaccessibles
- Incapacité de récupérer les données des capteurs ou de contrôler des processus critiques sur votre SCI

Ces signes peuvent ressembler aux problèmes temporaires de performance que l'on rencontre parfois et qui ne sont pas forcément causés par des activités malveillantes (p. ex. une augmentation du nombre de visiteurs sur votre site Web à la suite d'un communiqué de presse). À long terme, votre organisation doit établir une base de référence définissant ce qui est considéré comme une activité réseau normale. Ainsi, vous pourriez utiliser cette base de référence pour comprendre les variations importantes de l'activité réseau et reconnaître, le cas échéant, les tentatives d'inondation de votre réseau. Pour être en mesure de distinguer une attaque par DoS des problèmes non malveillants, votre organisation doit surveiller et analyser en permanence le trafic et les informations de journalisation, ce qui lui permettra de repérer les pannes et les redémarrages de services .

Prévention des attaques par DoS

Vous pouvez réduire les risques d'attaque par DoS et les répercussions de ce type d'attaque en suivant les consignes énumérées ci-dessous:

- **Travaillez avec votre fournisseur d'accès Internet et de services infonuagiques pour conclure des accords sur les niveaux de service qui comprendront des dispositions relatives à la défense contre les DoS**. Vos fournisseurs de services peuvent utiliser divers outils et techniques pour aider votre organisation à se protéger contre les attaques par DoS.
- **Assurez-vous que vos administrateurs de systèmes connaissent bien les services de protection contre les attaques par DoS**. En effet, une bonne connaissance de ces services peut les aider à juger s'il convient, par exemple, d'imposer des limites ou de recourir à une liste d'applications autorisées.
- **Surveillez le réseau et les systèmes**. Configurez des outils de surveillance qui pourront vous alerter en cas d'augmentation importante du trafic (hors des limites fixées pour la base de référence) ou lorsque du trafic suspect cherche à submerger un site Web.
- **Installez et configurez des pare-feu et des systèmes de prévention des intrusions.** Vous pouvez utiliser ces outils pour surveiller le trafic, de même que bloquer le trafic illégitime et que l'on sait malveillant.
- **Installez et assurez la mise à jour des antivirus et des antimaliciels.** Configurez les antivirus et les antimaliciels de façon sécurisée sur tous les appareils connectés. Mettez en place des antimaliciels dotés de fonctions automatisées de mise à jour et d'analyse.
- **Mettez à jour et corrigez les systèmes d'exploitation et les applications.** Mettez à jour et corrigez les systèmes et les applications, y compris vos pare-feu, pour vous assurer que les problèmes de sécurité seront abordés sans tarder et empêcher les auteurs de menace d'exploiter les failles des systèmes.
- **Utiliser un service d'hébergement de sites Web qui met l'accent sur la sécurité.** Avant de choisir le service qui hébergera votre site Web, assurez-vous que le fournisseur a mis en place des mesures de sécurité adéquates pour ses clients.
- **Défendez le périmètre de votre réseau.** Pour protéger votre réseau, adoptez une approche axée sur la sécurité par couches en mettant en place de multiples techniques et mécanismes de contrôle.
- **Soyez prévoyant.** Prévoyez un plan de récupération qui donne la priorité aux systèmes et aux processus en fonction de leur période d'indisponibilité acceptable. Vous devez également identifier les points de contact et former une équipe d'intervention en cas d'incident.
- **Sauvegardez vos données.** Procédez à la sauvegarde de votre information et de vos applications essentielles. Testez régulièrement vos sauvegardes pour vous assurer de pouvoir récupérer vos données.

Intervention en cas d'attaque par DoS

Voici quelques exemples de mesures qu'il convient d'appliquer lorsque vos systèmes ont été ciblés par une attaque par DoS :

1. **Identifier.** Signalez les indicateurs d'attaque par DoS, comme une mauvaise performance du réseau, et comparez-les à votre trafic normal (volume et nature). Communiquez avec votre administrateur de réseau et votre fournisseur d'accès Internet pour confirmer la cause de la panne ou du problème.
2. **Contenir.** Repérez les limites de votre réseau et les actifs exposés. Utilisez les systèmes de sécurité du réseau, notamment les pare-feu, ou envisagez d'avoir recours aux services de protection contre les DoS qui pourraient être offerts par votre fournisseur de services. Communiquez avec votre fournisseur d'accès Internet et de services infonuagiques dès que possible.
3. **Amorcer la reprise.** Vérifiez si d'autres signes d'activités malveillantes auraient pu se manifester parallèlement à l'attaque par DoS. Rétablissez les connexions et annoncez que les services sont de nouveau en ligne. Assurez-vous d'avoir une stratégie permettant la reconnexion progressive des sessions des clients.
4. **Réviser les leçons retenues.** Après le processus de reprise, passez en revue les mesures appliquées et apportez les améliorations requises. Le cas échéant, documentez les changements dans votre plan d'intervention.

Si votre organisation a été victime d'une attaque par DoS, veuillez en aviser le Centre canadien pour la cybersécurité : **contact@cyber.gc.ca**.

Renseignements supplémentaires

Pour obtenir des conseils et des ressources, vous pouvez consulter les publications suivantes sur notre site Web :

- *Sauvegarder et récupérer vos données* (ITSAP.40.002)
- *Application des mises à jour sur les dispositifs* (ITSAP.10.096)
- *Protéger l'organisme contre les maliciels* (ITSAP.00.057)
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur* (ITSAP.30.030)
- *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* (ITSM.10.089)
- *Élaborer un plan d'intervention en cas d'incident* (ITSAP.40.003)
- *Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels* (ITSAP.00.050)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

 No de cat.D97-1/00-100-2021F-PDF ISBN 978-0-660-43194-9