Que faire en cas d'attaque par déni de service (DDoS) ?

LECTURE : 3 MINUTES

Par **Bercy Infos** , le 20/11/2024 - **Sécurité numérique**

Les attaques par déni de service, aussi appelées DDoS (de l'anglais Distributed denial of service) ciblent les sites internet et les services numériques pour les rendre inaccessibles. Qu'est-ce qu'une attaque par déni de service ? Comment s'en protéger ? On fait le point.

Qu'est-ce qu'une attaque par déni de service (DDoS) ?

Le site **cybermalveillance.gouv.fr** définit l'attaque par déni de service comme une attaque « *visant à **rendre inaccessible un serveur** grâce à l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation de faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.* »

Les sites de e-commerce, les institutions financières, les gouvernements ou les structures d'hébergement sont des cibles fréquentes d'attaques par déni de service, mais **toutes les structures** peuvent être touchées si elles disposent d'une infrastructure réseau avec un accès à Internet.

L'attaque par déni de service est relativement **facile à mettre en œuvre par les personnes malveillantes** et les conséquences sont nombreuses :

- sur des sites de e-commerce, le site devient inaccessible ou rencontre des difficultés de fonctionnement, empêchant toute transaction
- les dysfonctionnements sur le site sont visibles par les internautes qui peuvent se poser des questions sur la sécurité du site, altérant la relation de confiance avec les usagers.

Les attaques par déni de service peuvent être commises pour différentes raisons : vengeance, revendications idéologiques, concurrence, extorsions de fond, etc. L'attaque peut aussi permettre de détourner l'attention pour mieux dérober des données sensibles par exemple.

Victime d'une attaque par déni de service (DDoS) : comment faire ?

Si le site internet de votre structure ne fonctionne plus, déterminez la cause de l'incident. L'inaccessibilité d'un site peut être provoquée par une panne de routage, un pic de fréquentation survenu pour un événement précis, un dysfonctionnement de DNS, etc.

S'il s'agit d'une attaque par déni de service, le site **cybermalveillance.gouv.fr** et **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** recommandent notamment :

- de prendre contact avec votre hébergeur pour qu'il identifie l'élément défaillant, le ou les protocoles utilisé(s) et les sources d'attaque et bloque les adresses IP source identifiées comme étant à l'origine de l'attaque,
- si cela est possible, de récupérer les fichiers de journalisation de votre pare-feu et des serveurs touchés,
- de réaliser une copie complète de la machine attaquée et de sa mémoire,
- de ne pas payer la rançon réclamée, le cas échéant,
- de faire appel à un professionnel référencé sur **cybermalveillance.gouv.fr** pour la remise en production et la sécurisation des systèmes d'information touchés,
- lorsque l'attaque est terminée, de procéder à un contrôle global du système d'information pour s'assurer que des données sensibles n'ont pas été dérobées,
- de modifier tous les mots de passe d'accès aux serveurs suspectés touchés. Il faut également envisager une réinstallation complète à partir des sauvegardes réputées saines,

- de notifier cette attaque à la CNIL s'il y a eu une violation de données à caractère personnel,
- de déposer plainte au commissariat de police ou à la gendarmerie.

À savoir

Les articles **323-1 à 323-7 du Code pénal** prévoient une sanction en cas d'entrave à un système de traitement automatisé des données (STAD). Il est donc important de déposer plainte au commissariat de police ou à la gendarmerie proche de chez vous. Pour cela, vous aurez besoin de tous les éléments techniques décrivant l'attaque.

Quelles sont les mesures préventives pour se protéger contre l'attaque par déni de service (DDoS) ?

Pour prévenir les attaques par déni de service, vous devez :

- effectuer régulièrement les mises à jour de sécurité de vos logiciels
- paramétrer correctement votre pare-feu
- vérifier la complexité de vos mots de passe et les changer régulièrement
- vérifier que votre hébergeur est préparé pour faire face à ce type d'attaque.

À savoir

Le site **cybermalveillance.gouv.fr** vous propose de nombreuses ressources et conseils. Vous pouvez retrouver **une fiche réflexe sur le déni de service pour adopter les bonnes pratiques et réagir en cas d'attaque**.

Ces contenus peuvent aussi vous intéresser

- Cinq conseils pour se prémunir contre les rançongiciels (ransomware)
- Sécurité de vos données : quelles sont les méthodes de piratage les plus courantes ?
- Entreprises : quelles règles de cybersécurité appliquer ?

En savoir plus sur les attaques par déni de service

- **Attaques DDoS, que faire ?** *sur le site cybermalveillance.gouv.fr*
- **Comprendre et anticiper les attaques DDoS** *sur le site de l'ANSSI*

Thématiques : **Sécurité numérique**