



Attaque DDoS - que faire?

- Consignez l'attaque (NetFlow, fichiers journaux des serveurs, échange de courriels avec les maîtres chanteurs, etc.). Ces informations sont précieuses pour une analyse ultérieure et pour éventuellement déposer plainte contre inconnu.
- Assurez-vous de pouvoir garder un minimum de canaux d'informations accessibles depuis l'extérieur, par exemple un site Web statique vous permettant d'informer vos clients et de leur offrir d'autres possibilités de contact (par ex. téléphone, télécopie, courriel).
- Analysez l'attaque et définissez une stratégie de défense:

Si l'attaque provient d'un nombre limité d'adresses IP, il suffit de filtrer ces adresses à l'aide d'un routeur ou d'un pare-feu. Si le flux de données dépasse la bande passante à votre disposition, votre fournisseur d'accès à Internet devra s'en charger.

Déplacez le cas échéant le système attaqué dans un autre sous-réseau (en cas d'agression uniquement basée sur l'IP). Il convient ici de rechercher une solution en étroite collaboration avec votre fournisseur d'accès à Internet ou un fournisseur spécialisé dans les solutions de mitigation DDoS.

S'il s'agit d'une attaque dont l'adresse IP d'origine a vraisemblablement été falsifiée:

C'est typiquement le cas des attaques volumétriques (*flooding*) qui exploitent les protocoles SYN, UDP, BGP et SNMP. Filtrer les adresses IP ne sert à rien dans ce cas-là et peut même bloquer des utilisateurs légitimes. Il convient ici de trouver une solution avec votre fournisseur d'accès à Internet. Il pourra détourner ce trafic ou le filtrer. Pour ce faire, vous devez toutefois savoir quels protocoles vous utilisez et lesquels peuvent être filtrés sans causer de dommages. Les sites Web publics sont généralement basés sur des protocoles TCP (HTTP, HTTPS, SMTP, etc.) ce qui permet de filtrer les protocoles dits sans état, tels que l'UDP (exception éventuelle: DNS).

Attaques contre une application:

Dans ce cas de figure, de nombreuses requêtes (complexes) paralysent votre application. Les attaques utilisent en règle générale des protocoles réseau TCP, d'où la difficulté pour l'expéditeur à falsifier son adresse qui pourra être filtrée selon divers critères.

Attaques contre le protocole SSL/TLS:

Il peut être utile de planifier une liaison SSL auprès d'un service en nuage (*cloud*), qui transmettra par la suite la liaison filtrée à vos systèmes.

Si la majeure partie de votre clientèle se trouve dans des pays bien précis, la géolocalisation sur Internet (*GeoIP*) permet de la filtrer ou de la classer par ordre de priorité. Le service restera ainsi plus longtemps accessible, même si l'un ou l'autre utilisateur légitime pourrait être ignoré, ou obtenir un faible niveau de priorité.

- Analysez l'attaque et définissez une stratégie de défense. Attendez-vous à ce que le cybercriminel cherche une parade à vos mesures de défense et recoure à de nouvelles tactiques. Le cas échéant, analysez sa nouvelle attaque DDoS et prenez les mesures qui s'imposent.
- Signalez l'incident à l'OFCS et portez plainte auprès des autorités de police compétentes pour (tentative de) détérioration de données (art. 144^{bis} du code pénal) et le cas échéant pour (tentative d') extorsion et chantage (art. 156 du code pénal). La détérioration de données concerne également les données rendues indisponibles et, par conséquent, inutilisables pendant un certain temps par une attaque.

Informations sur le paiement des rançons

- L'OFCS déconseille fortement de céder aux exigences des maîtres chanteurs.
- Si vous envisagez quand même de payer une rançon, l'OFCS vous recommande instamment de discuter de ces opérations avec la police cantonale.

Informations complémentaires

Mesures

Mesures contre les attaques DDoS

([/ncsc/fr/home/infos-fuer/infos-behoerden/aktuelle-themen/massnahmen-schutz-ddos.html](https://ncsc.ch/fr/home/infos-fuer/infos-behoerden/aktuelle-themen/massnahmen-schutz-ddos.html))

Dernière modification 01.01.2024

