Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

REAGIR A UN DENI DE SERVICE – REFLEXES

QU'EST-CE QU'UN DENI DE SERVICE ?

Une attaque par déni de service (DoS attack pour Denial of Service attack) est une attaque informatique ayant pour but de rendre indisponible un service et d'empêcher les utilisateurs légitimes de l'utiliser. Un déni de service peut être distribué (Distributed DOS) lorsqu'il est émis depuis plusieurs origines distinctes.

OBJECTIFS DE L'ATTAQUE

Empêcher les utilisateurs légitimes d'un service de l'utiliser (ex : site web, serveur de messagerie, équipement, etc.)

RISQUES

- ➔ **PERTE D'IMAGE**
- ➔ **PERTE FINANCIERE**
- ➔ **PERTE DE PRODUCTIVITE**

SYMPTOMES

UTILISATION DU SERVICE IMPOSSIBLE / RALENTIE
IMPOSSIBILITE DE CHARGER LES PAGES D'UN SITE INTERNET

VECTEURS D'ATTAQUES

- Botnet (ensemble de machines compromises)
- Attaque réseau basée sur des faiblesses protocolaires
- Exploitation d'une vulnérabilité ou d'une erreur de configuration

QUOI FAIRE

- **AVERTIR LE RESPONSABLE SECURITE**
- **AVERTIR LES TECHNICIENS**
- **PREVENIR LE SERVICE COMMUNICATION**
- **DEPOSER PLAINTE AUPRES DE LA POLICE OU LA GENDARMERIE**

REAGIR A UN DENI DE SERVICE – REFLEXES

GRAVE OU PAS ?

Une attaque par déni de service vise uniquement à rendre indisponible un service (pas d'impact pas sur la confidentialité et l'intégrité des données de l'équipement / application visé(e)). En général l'arrêt de l'attaque et un redémarrage permettent un retour normal du service.

LES BONNES PRATIQUES

- Installer les correctifs de sécurité du système et des logiciels
- Durcir l'équipement et l'application
- Réaliser des audits de sécurité et des scans de sécurité réguliers
- Installer un équipement de protection (pare-feu, répartiteurs de charge)
- Il est aussi possible de réfléchir à des solutions d'externalisation de l'hébergement ou des solutions de protection.

TECHNIQUES UTILISEES

Outre les vecteurs d'attaque décrits en première page, il existe des techniques telles que l'amplification, la réflexion, etc. qui sont utilisées pour lancer des attaques DDOS.
Voir chapitre ressources

REPARER / ENQUÊTER

LA PROTECTION CONTRE LES ATTAQUES PAR DENI DE SERVICE EST COMPLEXE.

AVANT TOUT, IL S'AGIT DE DETERMINER L'EQUIPEMENT VISE ET D'ETUDIER L'ATTAQUE QUI A ETE MISE EN ŒUVRE AFIN D'APPORTER DES CONTRE-MESURES ADAPTEES.

IDENTIFIER L'ORIGINE DE L'ATTAQUE EST IMPORTANT MAIS IL FAUT SURTOUT SAVOIR CE QU'ELLE VISE ET COMMENT ELLE FONCTIONNE. SELON LE CAS :

1. **SI L'ATTAQUE VISE LES COUCHES APPLICATIVES (BASEE SUR L'EXPLOITATION D'UNE VULNERABILITE / ERREUR DE CONFIGURATION)**

- Installer les derniers correctifs de l'équipement / application
- Durcir la configuration de l'équipement et/ou utiliser des applications spécifiques contre les attaques DOS
- Auditer l'application / équipement visé(e)
- Monitorer l'équipement / l'application (ex : surveillance de serveurs avec Nagios, etc.). Attention au déchiffrement du trafic SSL.

2. **SI L'ATTAQUE CONSISTE A SATURER LE RESEAU**

- Utiliser un équipement de type pare-feu ou répartiteur de charge. Attention même si ces équipements permettent d'améliorer la résistance à une attaque par déni de service, ils ne sont en général pas suffisants.
- Utiliser un équipement de protection spécifique aux attaques DOS. En plus de posséder des capacités de traitement adaptées, ces équipements possèdent des fonctionnalités de filtrage spécifique Anti-DOS.
- Solliciter l'opérateur de transit ou le fournisseur d'accès à Internet afin de filtrer le trafic en amont
- Etudier si l'équipement / application visée peut être hébergé(e) dans le « cloud »
- Recourir à des services de Content Delivery Service – Network (CDN-N)

RESSOURCES

- Comprendre et anticiper les attaques DDOS
- Dénis de service - Prévention et réaction