RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE DÉNI DE SERVICE

Une attaque en déni de service ou en déni de service distribué (**DDoS** pour ***Distributed Denial of Service*** en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité. L'attaque est souvent visible publiquement, voire médiatiquement, et laisse à penser que l'attaquant aurait pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données, y compris les plus sensibles (données personnelles, bancaires, commerciales...): ce qui porte directement atteinte à l'image et donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires...

BUT RECHERCHÉ

Rendre un service indisponible. Le cybercriminel agit pour des motivations politiques, idéologiques, par goût du challenge, chantage, vengeance, ou pour des raisons économiques (concurrence). Cette attaque peut être utilisée pour faire diversion d'une autre attaque visant à voler des données sensibles de sa cible.

SI VOUS ÊTES VICTIME

En cas de menace d'attaque, **NE PAYEZ PAS LA RANÇON** car vous alimenteriez le système mafieux, sans garantie que l'attaque n'aura pas lieu ou même qu'elle aurait pu avoir lieu.

FILTREZ LES REQUÊTES DE L'ATTAQUANT au niveau de votre pare-feu ou de votre hébergeur.

RÉCUPÉREZ LES FICHIERS DE JOURNALISATION (logs) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.

RÉALISEZ UNE COPIE COMPLÈTE DE LA MACHINE attaquée et de sa mémoire.

ÉVALUEZ LES DÉGÂTS CAUSÉS et les éventuelles informations perdues.

Assurez-vous que l'attaquant n'a pas profité du déni de service pour accéder à des informations sensibles, y compris sur d'autres systèmes. En cas de doute, **CHANGEZ TOUS LES MOTS DE PASSE** d'accès aux serveurs suspectés touchés et envisagez leur réinstallation complète à partir de sauvegardes réputées saines.

FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS pour la remise en production et la sécurisation des serveurs touchés. Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.

DÉPOSEZ PLAINTE au commissariat de police ou à la gendarmerie ou en écrivant au procureur de la République dont vous dépendez et tenez à disposition des enquêteurs tous les éléments.

NOTIFIEZ CETTE ATTAQUE À LA CNIL s'il y a eu une violation de données à caractère personnel.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.

Ayez un pare-feu correctement paramétré: fermez tous les ports inutilisés et ne laissez que les adresses des machines indispensables accéder à distance aux fonctionnalités d'administration du site.

Vérifiez que les mots de passe sont suffisamment complexes et changés régulièrement, mais également que ceux créés par défaut sont effacés s'ils ne sont pas tout de suite changés (tous nos conseils pour gérer vos mots de passe).

Sollicitez votre hébergeur afin qu'il prévoie une réponse à ce type d'attaque au niveau de ses infrastructures.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION