FICHE RÉFLEXE 2

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque 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 prestataires spécialisés susceptibles de pouvoir vous apporter leur expertise.

DÉPOSEZ PLAINTE au commissariat de police ou à la brigade de gendarmerie dont vous dépendez et tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.

MESURES **PRÉVENTIVES**

Appliquez de manière régulière et systématique les mises à jour de sécurité du système d'exploitation et des logiciels installés sur vos serveurs.

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 (www.ssi.gouv.fr/guide/mot-de-passe).

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

LES **INFRACTIONS**

L'incrimination principale qui peut être ici retenue est celle d'**entrave à un système de traitement automatisé de données** (STAD ou système d'information).

Les **articles 323-1 à 323-7 du code pénal** disposent que :

• **Article 323-2 du code pénal** : « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ». Cet article pourra être appliqué dans l'hypothèse d'une attaque par « déni de service ». Il est passible d'une peine de cinq ans d'emprisonnement et de 150 000 € d'amende. « *Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende* ».

• **Article 323-1 du code pénal** : « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* » est passible de deux ans d'emprisonnement et de 60 000 € d'amende. « *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système* », les auteurs sont passibles de trois ans d'emprisonnement et de 100 000 € d'amende. « *Lorsque les infractions […] ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende* ».

Les tentatives de ces infractions sont passibles des mêmes peines.

Si l'attaque fait suite à un « chantage » : les faits peuvent être qualifiés juridiquement de **tentative d'extorsion**, punie et réprimée par l'**article 312-1 du code pénal** : « *L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ». L'extorsion est passible de sept ans d'emprisonnement et de 100 000 € d'amende.

Version 2.0