LE DÉNI DE SERVICE

Une attaque en déni de service ou en déni de service distribué (dite 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 service ou site n'est souvent 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. Par ailleurs, ce type d'attaque est 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 la notoriété, au sérieux, et donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

BUT RECHERCHÉ

Une attaque en déni de service a généralement pour but de rendre un service indisponible pour ses utilisateurs.

Ce type d'attaque peut être le fait de groupes ou d'individus agissant pour des motivations politiques, idéologiques, par goût du challenge, à des fins de chantage, pour des raisons économiques (concurrence par exemple) ou par vengeance.

Dans certains cas, l'attaque en déni de service peut être utilisée par les attaquants pour faire diversion d'une autre attaque visant à voler des données sensibles de sa cible.

MESURES PRÉVENTIVES

- Appliquez de manière régulière et systématique les correctifs de sécurité du système d'exploitation et des logiciels installés sur vos serveurs.
- Ayez un pare-feu correctement paramétré : fermez tous les ports inutilisés.
- Sollicitez votre hébergeur afin qu'il prévoit une réponse à ce type d'attaque au niveau de ses infrastructures.

SI VOUS ÊTES VICTIME

- En cas de menace d'attaque, ne payez pas la rançon réclamée car vous alimenteriez le système mafieux sans garantie que l'attaque n'aura pas lieu ou même qu'elle aurait pu avoir lieu.
- Filtrez ou faites filtrer les requêtes de l'attaquant au niveau du pare-feu ou de l'hébergeur.
- Essayez de récupérer ou de faire récupérer les fichiers de journalisation (log) de votre pare-feu et des serveurs touchés qui seront des éléments d'investigation.
- Réalisez ou faites réaliser une copie complète de la machine attaquée et de sa mémoire.
- Evaluez 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. En cas de doute, changer tous les mots de passe d'accès aux serveurs suspectés touchés et envisagez leur réinstallation complète à partir de sauvegardes réputées saines.
- Faites appel au besoin à un prestataire technique pour la remise en production et la sécurisation des systèmes d'information touchés. Vous pouvez faire appel à un prestataire référencé sur www.cybermalveillance.gouv.fr.
- Déposez plainte au commissariat de police ou à la brigade de gendarmerie le plus proche et tenez à disposition des enquêteurs tous les éléments de preuves techniques en votre possession.

LE DÉNI DE SERVICE

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 :

- 323-2 : « *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'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende* ».

- 323-1 : « *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'Etat, 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.