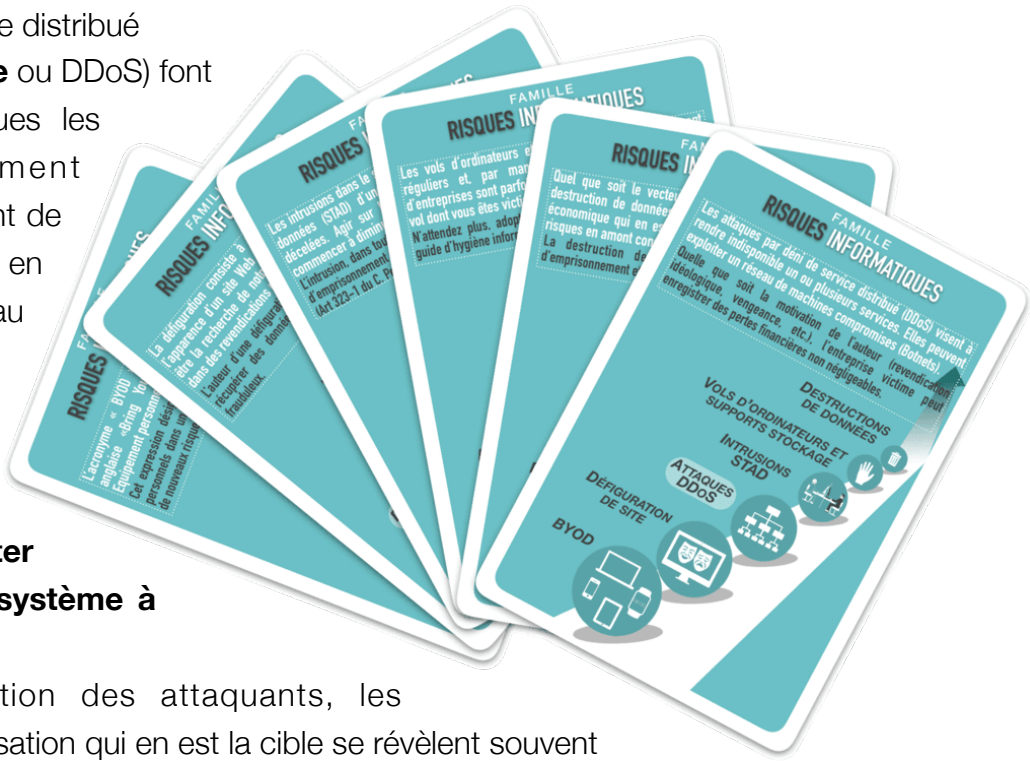
LES RISQUES INFORMATIQUES
Les attaques DDoS

VOUS EMPÊCHER DE RENDRE UN SERVICE !



Les attaques par déni de service distribué (**Distributed Denial of Service** ou DDoS) font partie des risques informatiques les plus fréquents, actuellement constatés, en raison notamment de leur relative simplicité de mise en oeuvre et leur faible coût au regard de leur efficacité.

L'ANSSI définit l'attaque DDoS, dans son glossaire, comme l'**action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu**.

Quelle que soit la motivation des attaquants, les conséquences pour une organisation qui en est la cible se révèlent souvent très préjudiciables. Prendre conscience des risques, c'est par exemple pour un dirigeant, protéger ses infrastructures et recourir à des technologies adaptées.

EN MODE ZOMBIE

Pour qu'une attaque DDoS soit couronnée de succès, elle doit reposer sur la puissance et les bandes passantes de centaines ou de milliers d'ordinateurs, afin d'envoyer d'énormes quantités de trafic vers un site Web, en vue de le rendre inopérant.

Les attaques DDoS peuvent être lancées à partir de réseaux de machines compromises appelés ***botnets ou machines zombie***, contrôlées à distance par un pirate informatique.

La méthode la plus simple et la plus rapide pour infecter un ordinateur reste l'infection par courrier électronique. La vigilance humaine vis-à-vis de certains liens hypertextes suspects et la mise à jour régulière de ses logiciels antivirus constituent la base d'un début de protection.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DES MENACES POUR LA E-ADMINISTRATION

Estonie 2007: quand l'administration de tout un pays se trouve perturbée

Figurant au rang des pays précurseurs en matière « d'administration en ligne », l'Estonie a subi, le 27 avril 2007 et pendant plus d'un mois, une vague d'attaques massives en déni de service distribué, lesquelles ont perturbé le fonctionnement de la vie courante du pays.

Le rapport d'information du Sénat sur la cyberdéfense de 2012, rapporté par JM. Bockel en dresse un récit.

France: Action publique 2022

Le 13 octobre 2017, le gouvernement français marquait ses ambitions en dévoilant le programme de transformation Action publique 2022. Ce programme vise notamment à ***moderniser l'environnement de travail*** des agents publics, renforcer la relation de ***confiance*** avec les usagers, et faire ***baisser la dépense*** publique.

La transformation numérique constitue l'un des chantiers majeurs et doit tendre vers ***100% de démarches administratives numérisées*** à l'horizon 2022. Dans un tel contexte, la protection des services en ligne contre les attaques en déni de service distribué (DDoS) constitue un enjeu majeur de souveraineté nationale.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour appréhender au mieux des attaques en déni de service:

- L'ANSSI fournit un guide destiné aux responsables de sécurité des systèmes d'information pour comprendre et anticiper les attaques DDoS,
- Vous pouvez suivre les conseils d'assistance et de prévention de cybermalveillance.gouv.fr et consulter notamment la fiche guide relative aux attaques DDoS de site web,
- Vous devez déposer plainte, si vous êtes victime, au commissariat de police ou à la brigade de gendarmerie le plus proche. Les articles 323-1 à 323-7 du Code pénal prévoient une sanction en cas d'entrave à un système de traitement automatisé des données (STAD).
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT