Typologie des menaces sur le Net

	Cybercriminalité	Atteinte à l'image	Espionnage	Sabotage
		Remplacer le contenu d'un site par des revendications politiques, religieuses, etc.	Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux.	Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique.
Cible	Les particuliers Les entreprises Administration	Les entreprises Les administrations	Les entreprises Les chercheurs	Tous
Type d'attaques	**Hameçonnage (phishing)** L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel. **Attaque par «Rançongiciel» (ransomware)** Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.	**Attaque par déni de service (DDOS)** L'objectif : rendre le site internet, et donc le service attendu, indisponible. Les motivations des attaquants sont diverses, allant des revendications idéologiques à la vengeance, en passant par les extorsions de fonds. **Attaque par défiguration (defacement)** Généralement revendiqué par des hacktivistes, ce type d'attaque peut être réalisé à des fins politiques ou idéologiques, ou à des fins de défi technique (challenge entre attaquants). L'objectif : modifier l'apparence ou le contenu d'un site internet, et donc violer l'intégrité des pages en les altérant.	**Attaque par point d'eau (watering hole)** Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données. **Attaque par hameçonnage ciblé (spearphishing)** Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée. Objectif : infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé.	Le sabotage s'apparente à une **« panne organisée »,** frappant tout ou partie des systèmes, selon le type d'atteinte recherchée – désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance.

Malwares

Les virus

Un virus est un programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB…

- ***Les vers*** : Logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.
- ***Polymorphe*** : Se dit d'un ver ou d'un virus dont le code est chiffré, changeant le code de déchiffrement d'une infection à l'autre, et donc l'apparence et/ou la signature.
- ***Cheval de Troie*** : Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

Remarques : La fonction cachée exploite parfois les autorisations légitimes d'une entité du système qui invoque ce programme. Elle peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données.

Espiogiciel (spyware)

Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

Moisson de courriels (Mail harvesting)

Action qui consiste à parcourir un grand nombre de ressources publiques (pages internet, groupes de discussion, etc.), afin d'y collecter les adresses électroniques avec des intentions malveillantes.

Remarques : Les adresses récupérées sont utilisées, par exemple, pour envoyer des courriels contenant des virus, des canulars ou des pourriels.

Autres malwares

- ***Mouchard internet (Web Bug)***

Support graphique implanté dans une page internet ou un courriel, qui a pour objectif de surveiller la consultation de cette page ou de ce courriel, à l'insu des lecteurs.

Remarques : Ces supports sont souvent invisibles, car beaucoup sont paramétrés avec une taille très petite. Ils sont aussi fréquemment représentés par des balises HTML IMG.

- ***Pourriel (Spam)***

Tout courrier électronique non sollicité par le destinataire.

Remarques : Le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, la spéculation boursière, des médicaments, le crédit financier, etc.

- ***Canular (Hoax)***

Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.

Remarques : Quelques canulars fréquents sont répertoriés sur des sites dédiés comme « Hoaxbuster » ou « Hoaxkiller ».

Sources : https://www.gouvernement.fr/risques/conseils-aux-usagers https://www.ssi.gouv.fr/