Synthèse les menaces informatiques

I) Les virus

Le virus est un programme informatique programmé pour exécuter des actions malveillantes.
Il se reproduire et de se propage en infectant des fichiers exécutables ou des pages web possédant du code informatique exécutable (capable d'effectuer des actions). Les fichiers exécutables possèdent généralement des extensions **.exe**

Les fichiers infectés peuvent à leurs tours infecter d'autres fichiers selon un effet boule de neige, le moyen de propagation peut être l'ouverture de pièces jointes d'émail, la consultation de site web, la consultation de fichiers informatiques dans des clefs USB ou via un réseau informatique,

Les fichiers de données en lecture comme les images, les sons, les vidéos ne peuvent pas posséder de virus par contre les logiciels qui les lisent peuvent en posséder.

Précaution : avoir un antivirus mis régulièrement à jour

II) Les malwares publicitaires appellés aussi les adwares

Ce sont des malwares qui s'attrapent le plus souvent lors de téléchargements sur des sites non officiels.
Les sites de téléchargements illégaux comportent beaucoup d'adwares publicitaires, la simple consultation de la page peut suffire à infecter l'ordinateur. Le résultat de l'infection se traduit par une modification des navigateurs internet, ceux ci affichent des fenêtres publicitaires en cascade.

Précaution : se méfier des applications gratuites mais dont les auteurs se rémunèrent avec de la publicité, faire des recherche sur les avis d'utilisateurs de différents sites avant de télécharger.
Privilégier les sites officiels de ce qu'on télécharge.

III) Les vers

Les vers n'ont pas besoin de fichiers exécutables pour se propager, ils infectent les carnets d'adresse et peuvent envoyer à vos contacts qui seront éventuellement infectés à leur tour, des logiciels malveillants ou des messages de tentative d'escroquerie.

Précaution :
Attention aux e-mail venant d'inconnus, méfiez vous des pièces jointes, utiliser des mots de passe sécurisés, ne confiez vos identifiant à personne. Activez les méthodes de sécurité disponibles comme la double identification.

IV) Les chevaux de troie (Trojan)

Le cheval de Troie est un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès de l'extérieur à votre ordinateur.
Il est souvent caché dans une pièce jointe, la pièce jointe est attractive et le message vous incite à la télécharger.

Précaution : assurer vous qu'il y a un pare-feux permettant de contrôler les communications entre votre ordinateur et internet.

V) L'hameçonnage (phising)

Le phising est une technique qui consiste à se faire passer par quelqu'un d'autre pour obtenir de lui des informations.
La technique la plus utilisée est celle d'un lien dans un e-mail vous envoyant vers une copie d'un site officiel.
Vous pensez rentrer vos identifiants sur la page de votre banque, de votre messagerie e-mail, de votre réseau social ou de votre magasin préféré en ligne. Mais dans le cas du phising vous rentrez sur site contrôlé par un pirate qui vas enregistrer vos identifiants.

Précaution : S'il est facile de copier l'apparence d'une page web, il est impossible pour un pirate de réserver le même nom de domaine (début de l'adresse d'un site web) que le site officiel.
Surveillez les liens qui vous sont envotés par mail, ne cliquez pas sans regarder l'adresse web

VI) Le ransomware (rançongiciel)

Ce virus malveillant va bloquer l'utilisation de votre ordinateur ou vous empêcher d'accéder à vos fichiers en les cryptant. Un message vous demande de payer une rançon pour obtenir la clef de décryptage et accéder de nouveau à vos fichiers. Le ransomware peut s'attraper par exemple en téléchargeant une pièce jointe, un fichier sur internet, en cliquant sur un fichier dans une clef USB. Les ransonwares sont avant tout destinés aux entreprises mais comme la diffusion des virus est incontrôlable, beaucoup de particuliers peuvent être touchés.

Précaution : en plus des précautions vu précédemment, faire des doubles sauvegardes de vos documents.

VII) Les hoax (messages trompeurs)

Ces messages vont utiliser votre naïveté ou votre manque de connaissance dans les technologies numériques pour vous faire cliquer et vous envoyer ainsi des fichiers malveillants (virus, cheval de troie, vers …) ou des escroqueries
Exemples de messages trompeurs : *vous avez 250 problèmes sur votre ordinateur télécharger notre logiciel ...*
Cliquez pour obtenir un Iphone pour 1€ Faites suivre ce message à 100 de vos amis pour avoir …

VIII) Les rootkit

Le rookit ou « outil de dissimulation d'activité » est un ou plusieurs logiciels dont le but est de prendre le contrôle d'un ordinateur serveur ou client. Une fois installé à votre insu, il ne va pas effectuer directement les actions néfastes mais va faciliter l'action d'autre malware en donnant un accès total à votre ordinateur.

Ses caractéristiques sont : difficile à détecter et difficile à enlever, pour cela il s'installe directement dans le système d'exploitation de la machine et efface ses traces ou les traces d'autres malware

Remarque :
Quelquefois le rootkit ne va pas effectuer d'action néfastes directement sur votre ordinateur, mais va faire en sorte que ce soit votre ordinateur ou serveur qui effectue pour le pirate l'action néfaste comme l'envoie de Spam par exemple. Votre ordinateur ou serveur sera transformé en machine zombi, qui effectua des actions cachés vers le réseau internet.