C’est quoi un virus, Trojan, Worm, Spyware, Adware , Malware, Keylogger, Ransomware , Botnet ?

Adware

Adware vient de « **ad** » qui veut dire annonce ou publicité.

Un adware est un logiciel qui va afficher des fenêtres de publicité sur votre ordinateur.

Un adware s’installe sur votre ordinateur soit sous la forme d’un logiciel soit sous la forme de plugin dans votre navigateur. Du coup, il en profite dès que vous surfez pour vous afficher des fenêtres de publicité.

Pire, dans quelques cas, il change votre moteur de recherche qui va orienter les résultats de vos recherches vers les sites que les pirates auront choisi. C’est le cas des moteurs de recherche : Babylon Search, Delta Search etc…..

Spyware

Spyware vient du mot **« spy »** qui veut dire Espion.

Un Spyware est donc un logiciel qui va vous espionner. Ce logiciel va enregistrer et transmette à quelqu'un d'autre toute votre activité.

Les spywares vont fournir aux pirates, tous les sites que vous visitez et votre comportement sur Internet.

Ils sont capables également de lire votre carnet d'adresse pour récupérer la liste de tous vos contacts.

Malware

Le Malware *est un logiciel développé dans le but de nuire à un système informatique*
Le mot **Malware** est le mot qui désigne à lui seul tous les types de logiciels malveillants. Il permet donc de désigner des logiciels tels que des *Virus*, des *Vers*, des *Rogues*, des *Troyens*, des *Rootkits*...
Tous les mots cités ci-dessus désignent une famille de malwares, un certain type de malwares ayant des caractéristiques communes.
Le mot virus est la majorité du temps utilisé pour désigner l'ensemble des menaces mais un virus à proprement dit est destructeur et infecte de nombreux fichiers sur le PC, ce sont des fichiers hôtes. Ce mot est un abus de langage donc désormais, quand vous parlerez des menaces informatiques, vous utiliserez l'expression *Logiciel* ***Malicieux ou Malware***.
Bien qu'il existe aujourd'hui les mots "*troyens, virus, vers, rootkits...*" la majorité des infections qui polluent nos PC sont en fait apparentées à plusieurs familles de malwares. Prenons pour exemple, l'infection nommée "*Navipromo*", cette infection est un adware c'est-à-dire qu'elle affiche des publicités intempestives et pourtant Navipromo utilise un rootkit pour dissimuler l'infection et permettre toutes sortes d'activités à l'insu de l'utilisateur et aux solutions de sécurité.

Il faut faire attention aux termes employés et utiliser (s'il existe) le nom de l'infection elle-même , cela évite de se mélanger les pinceaux et de dire ou de faire n'importe quoi.
Le début de l'ère des malwares, s'annonce par l'apparition de virus et de vers au début de la création de l'informatique, et lors de l'apparition d'Internet et des premiers échanges par mail. Donc au début, les seules menaces se résumaient aux vers et aux virus, qui permettaient à leurs créateurs de démontrer leurs prouesses techniques et de prouver au ''commun des mortels'', qu'ils pouvaient détruire un PC, faire tomber des serveurs..

Les malwares ont évolué, ils ne servent plus à détruire des systèmes ou à tenter d'infecter le plus de gens possible dans le seul but que l'on parle d'eux. Aujourd'hui les malwares deviennent de plus en plus discrets, et leurs créateurs n'ont qu'une peur, que l'on parle d'eux, et que l'on s'intéresse à eux. Cela est en totale opposition avec les anciens pirates informatiques. Les pirates contemporains désirent rester dans l'ombre. Mais pourquoi tiennent-ils à rester cachés ?

Ils veulent rester cachés, car leurs motivations et leurs buts ont changé. Le seul but des pirates aujourd'hui et de générer du profit, de leur rapporter de l'argent en infectant le plus grand nombre de machines en un minimum de temps. Voilà quel est le but des pirates du XXIe siècle. Et c'est pour cela que des technologies comme les systèmes de **rootkits**, des malwares comme les **adwares** ou les **rogues** ont vu le jour, car certains permettent de générer de l'argent et les autres de rester discrets.

keylogger

Keylogger vient de la contraction de 2 mots :

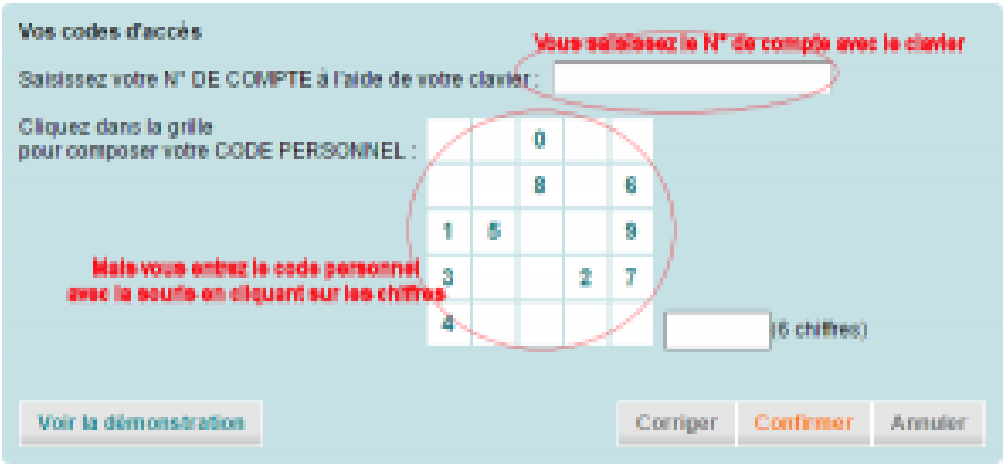
- Key : qui veut dire « touche »
- logger : qui veut dire « enregistreur »

Vous l'avez compris, un keylogger est un enregistreur de touche. Les suites de touches sont enregistrées et envoyées au pirate.

C'est très embêtant car la plupart du temps, nous utilisons notre clavier pour saisir nos identifiants et nos mots de passe sur différents sites tels que les banques.

C'est pourquoi depuis quelques temps, certaines banques (et quelques autres sites) utilisent un système de clavier virtuel qui permet de ne pas saisir le code d'accès à l'aide du clavier, mais avec la souris : ce qui rend le keylogger complètement inefficace.

Voici un exemple sur le site du crédit agricole :



Malheureusement, il reste beaucoup de site ou la connexion se fait encore via des identifiants et des mots de passe entièrement saisis au clavier.

Ransomware

Un ransomware (qui vient de ranson comme une raçon) est un logiciel qui va crypter vos fichiers et vous demander de l'argent (une rançon) pour que vous puissiez les décrypter.

Ce type de malware est particulièrement nocif car lorsqu'il s'attaque à un ordinateur, il crypte l'ensemble des documents qui lui sont accessibles.

Quelques entreprises sont victimes de ce genre d'attaques, car dès qu'un salarié attrape un ransomware, le logiciel s'attaque à l'ensemble des partages réseaux de l'entreprise auquel le salarié à accès.

Peu d'entreprises acceptent de payer la rançon préférant repartir d'une sauvegarde des documents.

On peut repérer un logiciel comme celui-ci par une lenteur extrême de l'ordinateur (en effet, elle est occupée à crypter l'ensemble des documents), il faut donc dès le premier symptôme le débrancher du réseau et l'éteindre l'ordinateur avec le bouton marche/arrêt (sans attendre la fin de l'arrêt de l'OS).

Phishing

Le mot phising est une contraction des mots phreaking (piratage des lignes téléphoniques) et de fishing (pêcher du poisson).

En français, on parle aussi de hameçonnage.

Le phishing, comme l'indique l'illustration à gauche, est la technique utilisée par les pirates pour récupérer des informations sur leurs cibles. On dit qu'ils vont à la pêche aux informations. Et croyez-moi, malgré toutes les mises en gardes que l'on peut voir un peu partout : ça marche encore.

Le principe est simple :

- le pirate envoie un mail se faisant généralement passer pour une grande entreprise (comme par exemple : fournisseur d'électricité, de gaz, d'eau, une banque, ou autre)
- dans ce mail, il est indiqué que votre compte sera coupé bientôt, ou alors que vous avez trop versé d'argent.
- on vous invite donc à vous connecter à votre compte pour régulariser.
- or, et c'est là qu'est le piège, le mail contient un lien vers un site qui n'est le site de la grande entreprise, mais le site du pirate.
- vous saisissez vos coordonnées bancaires sur le faux site, et le pirate les récupère pour les utiliser ensuite !

Les spams

Les spams sont des mails non souhaités. Bien souvent, ces mails sont à caractères publicitaires.

Si je reprends la définition de la CNIL : « Le « spamming » ou « spam » est l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière. »

Donc lorsque vous vous inscrivez à une lettre d'information et que vous recevez des informations du site sur lesquels vous vous êtes inscrit : ce n'est pas du spam !

Pour qu'un mail ne soit pas considéré comme spam, vous devez avoir la possibilité de vous désabonner.

Si on n'y prend pas garde, ce genre de mails fini par remplir les boites aux lettres et les rendre inutilisables lorsqu'elles sont devenues pleines.

Les hoaxes

Un hoax (canular) est un mail contenant une fausse information. Mais cette information est présentée de telle façon que la personne la recevant va en général la transmettre à l'ensemble de son carnet d'adresse croyant bien faire.
Et bien souvent cette information sera à nouveau renvoyée par tous ceux qui l'ont reçu, et cela peut continuer très longtemps.
Ce qui fait que des informations qui pouvaient parfois être vraies au début continuent de circuler en boucle, de boites aux lettres en boites aux lettres.

Voici un exemple de hoax : Vous recevez un mail vous informant qu'un terrible virus circule actuellement sur Internet. Sans vous posez de questions, vous transmettez ce mail à l'ensemble de votre carnet d'adresses sans avoir vérifié la véracité de cette information, et voila vous avez sans doute transmis un hoax.
C'était le cas aussi d'un mail circulant, appelant les personnes d'un certain groupe sanguin à appeler un centre de transfusion, et cela dans le but de sauver une petite fille. Le centre de transfusion était submergé par les appels généré par ce mail qui tournait depuis des années et qui n'était plus d'actualité.

Si vous avez un doute sur un mail reçu, n'hésitez pas à consulter le site hoaxbuster.com. Il vous dira si le mail est un canular.

BOTNET

Voilà une nouvelle apparition de ce que l'on nomme des **botnets** en français des **PC zombies**.

<u>Définition</u> :
En Sécurité informatique, une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique, ce dernier l'utilise alors le plus souvent à des fins malveillantes.

Un botnet est donc en **ensemble de PC reliés entre eux** par des chevaux de Troie, et tous ces ordinateurs sont contrôlés par un pirate informatique qui peut leur faire faire ce que bon lui semble. Comme **attaquer** les serveurs d'une entreprise et leur demander une somme d'argent en échange de l'arrêt de l'attaque ou encore envoyer 10 000 000 de spams à différentes adresses mail en échange d'une somme d'argent donnée par un autre pirate, qui paye pour utiliser le botnet. Ou encore infecter 5000 ordinateurs d'adware pour afficher des pubs d'un site de casino en échange d'une somme d'argent donnée par ce dernier...

Ce qu'il faut retenir de ceci, c'est que **les malwares évoluent, se diversifient**, et cette évolution n'est pas terminée et est de plus en plus inquiétante.