Types de menaces

Pour comprendre la notion de sécurité informatique, il faut déjà commencer par comprendre les différents types de menaces dont vous pouvez être victime.

Vous avez certainement déjà entendu parler des virus, mais le mot de « spyware » (ou logiciel espion en français), de « trojan » (cheval de Troie, comme dans la mythologie) ou encore « rootkit » vous semblera peut-être un peu chinois si vous ne lisez pas les quelques lignes en dessous. C'est pour ça que, pour qu'on se comprenne bien, nous allons parler de toutes ces joyeusetés qui circulent sur le net, et d'autres joyeusetés dont je n'ai pas encore mentionné le nom.

Commençons par une mise au point sur les virus :

Les virus

Un virus est un programme informatique écrit dans le but de se propager à d'autres ordinateurs en infectant un programme légitime. Certains de ces virus sont totalement inoffensifs (très rares), d'autres peuvent détruire irrémédiablement l'ordinateur (heureusement très rares aussi). Ce ne sont bien évidemment pas les seuls effets des virus. Voici une liste d'effets visibles ou même invisibles qui peuvent de produire si votre ordinateur attrape un virus :

- ralentissement global du PC
- l'ordinateur qui se met à écrire tout seul
- des millions de spams envoyés au monde entier à votre nom (ou pas) via votre ordinateur pour que des gens achètent du viagra ou se fassent élargir le pénis (les femmes reçoivent aussi ce genre de messages. Les virus ne sont pas particulièrement intelligents).
- Des fichiers que vous ne connaissez pas qui se retrouvent à des endroits auxquels ils n'ont rien à faire (des fichiers bizarres qui se retrouveraient dans vos photos par exemple / attention : certains programmes légitimes créent parfois des fichiers tout à fait légitimes dans vos documents, ne donc pas y voire tout de suite l'intervention d'un virus)
- Destruction complète de certains fichiers
- Infection de certains fichiers légitimes par des virus (afin de se répliquer pour quand vous ouvrirez ce fichier sur un autre PC)
- Impossibilité de démarrer l'ordinateur
- …

Impossible de faire une liste exhaustive des effets d'un virus informatique, car il y aurait sans doute plusieurs dizaines de pages. De plus, les virus et les chevaux de Troie sont très nombreux : F-Secure (une entreprise connue dans le domaine de la sécurité informatique) annonce que leur nombre pourrait dépasser le million à la fin de l'année 2008.

Les virus se répliquent en infectant des logiciels particuliers, mais il existe des variantes qui peuvent se multiplier par leurs propres moyens, sans infecter de logiciel hôte. Ce sont des vers.

Les chevaux de Troie

Un cheval de Troie est un type de logiciel malveillant. Le plus souvent, un tel programme exécute des actions nuisibles à l'utilisateur. Ce n'est pas un virus car il ne se réplique pas lui même. Cependant, il peut être apparu en même temps qu'un virus qui aurait installé lui même le cheval de Troie.

Le plus souvent, un cheval de Troie ouvre une porte dérobée dans votre ordinateur. De ce fait, un pirate informatique peut à tout moment prendre le contrôle de l'ordinateur à distance et en faire ce qu'il veut.

Les effets d'un cheval sont nombreux et similaires à ceux des virus.

Les logiciels espions

Appelé en anglais spyware, ou en français espiologiciel, ou plus rarement espiongiciel, un logiciel espion a pour but de collecter des informations contenue dans votre ordinateur (sites sur lesquels vous allez, et toutes autres informations que les concepteurs jugeraient intéressantes). Les logiciels espions accompagnent souvent les logiciels gratuits et sont souvent installés à l'insu des utilisateurs.

Les effets sont nombreux ici encore :

- ralentissement de l'ordinateur
- page d'accueil changée (avec impossibilité de revenir à l'ancienne page d'accueil)
- affichage de fenêtres non désirées (et souvent publicitaires)
- vol d'informations

Parfois, certains logiciels espions se font passer pour des logiciels anti-logiciels espions, tentent d'effrayer l'utilisateur et poussent à l'achat de la version complète du logiciel espion.

Il n'est pas rare aussi que certains logiciels espions soient livrés gratuitement avec des virus et autres chevaux de Troie.

Les rootkits

Les rootkit modifient le comportement de votre système d'exploitation (Windows, Linux, …) afin de cacher les opérations malveillantes effectuées par les chevaux de Troie et les autres cochonneries du Web qui seraient dans votre ordinateur. Ce qui les rend indétectables par des méthodes classiques et difficilement supprimables.

Il y a eu des affaires tristement célèbres sur les rootkits. De nombreux CD musicaux de Sony-BMG ont pendant un temps installé un rootkit qui rendait certains dossiers invisibles aux yeux des utilisateurs. Ce qui a permit à des virus de se mettre dans ces dossiers cachés et les antivirus ont eu du mal à les y enlever.

Les failles de sécurité

Ce ne sont pas à proprement parler des menaces directes. Une faille de sécurité est un défaut de fonction dans un logiciel qui permet à des virus ou des personnes physiques de corrompre le système, de voler des données et dans tout les cas, d'effectuer des actions non désirées.

Très nombreux (pour ne pas dire tous) sont les logiciels ayant des failles de sécurité. La plupart sont corrigées, d'autres ne sont pas encore découvertes.

C'est du fait des failles de sécurité qu'il faut mettre à jour ses logiciels, et donc éviter les logiciels piratés.

Le spam

Le SPAM en majuscule désigne une marque jambon épicé en boite de conserve utilisé souvent pour faire des sandwiches. Pourquoi je vous parle de ça ? Parce qu'il existe le même mot, mais en minuscules. Parfois traduit en pourriel, rarement en polluriel, ce mot désigne les emails indésirés qui ont été expédiés en masse à but publicitaire voire malhonnête.

Le spam peut être trouvé sous ces formes :

- Le spam contient généralement de la publicité. Les produits les plus vantés sont les services pornographiques, les médicaments (le plus fréquemment les produits de « dopage sexuel » ou, des hormones utilisées dans la lutte contre le vieillissement), le crédit financier, les casinos en ligne, les montres de contrefaçon, les diplômes falsifiés et les logiciels craqués.

- Des escrocs envoient également des propositions prétendant pouvoir vous enrichir rapidement : travail à domicile, conseil d'achat de petites actions (penny stock).
- Les chaines de messages ne sont pas réellement du spam, mais ce sont quand même des emails indésirables.
- Parfois aussi, mais de plus en plus rarement, il s'agit de messages d'entreprises ignorantes des règles du bon comportement sur Internet qui y voient un moyen peu couteux d'assurer leur promotion.
- Certains messages indiquant qu'un mail n'est pas arrivé à destination peuvent également être qualifiés de spam lorsque le message d'origine n'a pas été envoyé par vous même mais par exemple par un virus se faisant passer pour vous.
- Enfin la dernière forme de spam, le phishing

Le phishing

L'hameçonnage (phishing en anglais, terme dérivé de fishing, la pêche à la ligne), consiste à tromper le destinataire en faisant passer un email pour un message de sa banque ou d'un quelconque service protégé par mot de passe. Le but est de récupérer les données personnelles des destinataires (notamment des mots de passe, un numéro de carte bancaire) en les attirant sur un site factice enregistrant toutes leurs actions.

Les macros

Comme le nom ne l'indique pas, ce ne sont pas de petits poissons qui seraient cachés dans votre ordinateur. Ce sont de petits programmes qui sont inclus dans des documents. Il n'est pas rare d'avoir des macros dans des documents de traitement de texte, de tableur, ou d'autres types de documents.

Certaines macros sont agréables, elles permettent par exemple à ma mère d'envoyer des documents de son boulot facilement à ses employeurs. Mais il en existe de nombreuses qui ne le sont pas, et qui permettent la propagation de virus et autres cochonneries.

Les cookies

Tout comme les macros, les cookies ne sont pas de petits gâteaux secs avec des pépites de chocolat lorsqu'on est dans le domaine de la navigation sur Internet. Voici une définition tirée de Wikipédia légèrement retouchée par mes soins :

> Les cookies sont de petits fichiers textes stockés par le navigateur Internet (Internet Explorer, Mozilla Firefox, …) sur le disque dur du visiteur d'un site Web et qui servent (entre autres) à enregistrer des informations sur le visiteur ou encore sur son parcours dans le site.
>
> Le concepteur du site peut ainsi reconnaitre les habitudes d'un visiteur et personnaliser la présentation de son site pour chaque visiteur ; les cookies permettent alors de garder en mémoire combien d'articles il faut afficher en page d'accueil ou encore de retenir les identifiants de connexion à une éventuelle partie privée : lorsque le visiteur revient sur le site, il ne lui est plus nécessaire de taper son nom et son mot de passe pour se faire reconnaitre, puisqu'ils sont automatiquement envoyés par le cookie.
>
> Un cookie a une durée de vie limitée, fixée par le concepteur du site. Ils peuvent aussi expirer à la fin de la session sur le site, ce qui correspond à la fermeture du navigateur.
>
> Les cookies sont largement utilisés pour simplifier la vie des visiteurs et lui présenter des informations plus pertinentes. Mais une technique particulière permet aussi de suivre un visiteur sur plusieurs sites et ainsi de collecter et recouper des informations très étendues sur ses habitudes. Cette technique a donné à l'usage des cookies une réputation de technique de surveillance violant la sphère privée des visiteurs.

Comme vous avez donc pu le lire, les cookies ne sont pas tous à but malveillant. Le fait de vouloir à tout prix tous

les supprimer est inutile et même gênant. Nous verrons ça plus en détail à la fin de ces quelques pages.

Les Scripts Javascript

Pour pouvoir correctement expliquer ce que sont les scripts Javascript, il va falloir que j'explique ce que sont les pages Internet. Les pages Internet sont presque tout le temps conçues en HTML (ou ses dérivés).

Le HTML, c'est un langage qui est en quelque sorte un plan. C'est au navigateur d'afficher tout les éléments du plan correctement à l'écran. Comme vous vous en doutez surement, le HTML tout seul est quand même limité.

Les scripts Javascript sont de petits programmes inclus à l'intérieur des pages qui permettent d'améliorer la navigation sur Internet.

Ils permettent par exemple de changer la couleur d'une page, de faire apparaître du texte dans une page sans changer de page, …

Ils sont donc agréables, mais sont parfois malicieux.

Les faux logiciels de protection et les faux codecs

Il se peut que vous en rencontriez lors de vos navigations sur Internet.

Si vous avez une page vous disant quelque chose du genre « Votre ordinateur est infecté, téléchargez gratuitement WinAntivirus pour le désinfecter », ne le faites surtout pas. Bon nombre de ces soit-disant outils de désinfection sont en fait des outils d'infection, ou des outils totalement inefficaces.

De même si une page vous dit que vous n'avez pas le bon codec pour lire une vidéo ou une musique. Il existe de nombreux sites qui vous proposeront de vous installer des codecs ainsi qu'une quantité de cochonneries non désirées.

Dans le cas ou vous verriez ce genre d'alertes, utilisez votre antivirus et votre antispyware pour vous désinfecter.

Et si vous voulez vraiment installer un pack de codecs, il y a plusieurs choses à prendre en compte :

- La multiplication des packs risque de ralentir votre ordinateur ou de le faire bugger.
- Téléchargez le pack de codecs sur un site de confiance (pour éviter les risques d'infection par ce qui pourrait vous être proposé par un site peu sûr).

Malwares

En fait, un malware est un logiciel espion, ou un cheval de Troie, ou un rogue, ou un virus, …

Bref, le mot malware désigne toute cochonnerie pouvant s'incruster dans votre ordinateur. Ce terme sera donc de temps en temps utilisé dans ces quelques pages afin d'éviter d'écrire toute la liste des cochonneries pouvant infester votre ordinateur.