1. Définition

Logiciel malveillant est une traduction de l'anglais malware, mot-valise formé à partir de « malicious » et « software ». En France, l'usage du terme logiciel malveillant est préconisé mais on utilise aussi **logiciel nuisible** ou **maliciel** ou **pourriciel**. Beaucoup de francophones optent pour l'usage de malware, évitant la lourdeur relative de « logiciel malveillant ».

Parce que les virus ont été historiquement les premiers logiciels malveillants, le terme « virus » est souvent employé abusivement pour désigner toutes sortes de logiciels malveillants. Le logiciel antivirus renforce cette utilisation abusive puisque son objectif n'a jamais été limité aux virus.

2. Historique

On attribue le terme de « virus informatique » à l'informaticien et spécialiste en biologie moléculaire Leonard Adleman : co-inventeur du cryptosystème RSA (Rivest, Shamir, Adleman) en 1977, Adleman a également travaillé dans la bio-informatique.

Les tout premiers logiciels de ce type étaient de simples divertissements. Pour ce jeu, chaque joueur écrit un programme. L'objectif du jeu est de détruire les programmes adverses tout en assurant sa propre prolifération. Les logiciels sont capables de se recopier, de se réparer, de se déplacer eux-mêmes en différentes zones de la mémoire et « d'attaquer » les logiciels adverses. La partie se termine au bout d'un temps défini ou lorsque l'un des joueurs voit tous ses programmes inactifs ou détruits. Le vainqueur est celui qui possède le plus grand nombre de copies actives.

En 1986, l'ARPANET, considéré comme l'ancêtre d'Internet, fut infecté par Brain, virus renommant toutes les disquettes de démarrage de système en (C)Brain. Les créateurs de ce virus y donnaient leurs nom, adresse et numéro de téléphone : c'était une publicité pour eux.

Les ordinateurs à base de Windows sont de très loin les plus touchés par les logiciels malveillants, essentiellement à cause de la part de marché qu'ils représentent.

3. Classification

Les logiciels malveillants peuvent être classés en fonction des trois mécanismes suivants :

1. Le **mécanisme de propagation** (par exemple, un ver se propage sur un réseau informatique en exploitant une faille applicative ou humaine) ;
2. Le **mécanisme de déclenchement** (par exemple, la bombe logique — comme « vendredi 13 » — se déclenche lorsqu'un évènement survient) ;
3. La **charge utile**, en fait la partie nocive (par exemple, le virus « Tchernobyl » tente de supprimer des parties importantes du BIOS - logiciel de démarrage de l'ordinateur - ce qui bloque le démarrage de l'ordinateur infecté).

La classification n'est pas parfaite, et la différence entre les classes n'est pas toujours évidente. Cependant, c'est aujourd'hui la classification standard la plus couramment adoptée dans les milieux internationaux de la sécurité informatique.

4. Mécanismes de propagation

Les mécanismes de propagation les plus connus sont :

- Type **virus**, au sens strict du terme, est un programme auto-réplicatif capable de se propager et de se reproduire sur d'autres ordinateurs en s'insérant dans des programmes légitimes appelés hôtes.
- Type **ver** (worm) est un programme capable de se propager et de se dupliquer par ses propres moyens sans contaminer de programme hôte : il se propage principalement grâce à la messagerie en récupérant l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant à toutes des copies de lui-même. Ces vers sont la plupart du temps des fichiers exécutables envoyés en pièce jointe et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier attaché.

- Type **cheval de Troie** (Trojan horse) est un programme d'apparence légitime qui comporte une routine nuisible exécutée sans l'autorisation de l'utilisateur. Il ne peut pas se reproduire. Il se répand via des virus, des vers ou des logiciels téléchargés. Son rôle est de faire entrer la charge utile sur l'ordinateur et de l'y installer à l'insu de l'utilisateur. Le cheval de Troie n'est rien d'autre que le véhicule, celui qui fait "entrer le loup dans la bergerie". Il n'est pas nuisible en lui-même car il n'exécute aucune action, si ce n'est celle de permettre l'installation du vrai parasite. Le cheval de Troie peut être une version modifiée d'un programme existant et légitime : il prend l'apparence d'un logiciel existant, légitime et parfois même réputé, mais qui aura été modifié pour y dissimuler un parasite. L'utilisateur va télécharger et installer le programme, pensant avoir affaire à une version saine. Les logiciels piratés peuvent être des chevaux de Troie qui vont allécher l'internaute qui cherche à obtenir gratuitement un logiciel normalement payant (Adobe Acrobat pro, Photoshop, Microsoft Office...).

La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005.

5. Charges utiles

Les charges utiles les plus connues :

- La **porte dérobée** (**backdoor**) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle. Enfin, selon l'étendue des droits que le système d'exploitation donne au logiciel, le contrôle peut s'étendre à d’autres voire l'ensemble des opérations de l'ordinateur. La **porte dérobée** (*backdoor*) est un programme qui va s'exécuter discrètement sur l'ordinateur où il est installé pour y créer une faille de sécurité. Le backdoor ouvre un ou plusieurs ports sur la machine, ce qui lui permet d'accéder à internet librement et de télécharger, à l'insu de l'utilisateur, un parasite. Le backdoor n'est donc pas un cheval de Troie : il ne véhicule pas le parasite en lui, il va simplement ouvrir l'accès et récupérer, via internet, le programme malveillant qui se trouve sur un serveur distant.
- Le **logiciel espion** (**spyware**) peut modifier la configuration de votre ordinateur ou collecter des données publicitaires et des informations personnelles et les envoyer à un organisme tiers. Il peut suivre les habitudes de recherche des internautes et peut également rediriger votre navigateur web vers un autre site web que celui que vous avez l’intention de visiter.

- Le **keylogger** est un petit logiciel espion capable d'enregistrer tout ce qui est tapé au clavier et de le renvoyer ensuite à un réseau de pirates. Les jeux en ligne comme World of Warcraft sont la cible privilégiée de ce type de malware.
- Le **logiciel de sécurité non autorisé** (Scamwares/Rogues Anti-spyware) tente de vous faire croire que votre ordinateur est infecté par un virus et vous invite en général à télécharger ou à acheter un produit qui élimine les virus. Ils peuvent empêcher l'ouverture d'applications telles qu'Internet Explorer ou afficher des fichiers Windows légitimes et importants comme étant infectés.
- Le **rootkit** est un ensemble de programmes chargés de dissimuler l'activité nuisible d'un malware. Il est chargé d'écraser la plupart des outils du système et de les remplacer par des commandes équivalentes masquant la présence du pirate. Ce dernier est habituellement bien caché dans le système d'exploitation et ne sera pas détecté par les logiciels antivirus et autres outils de sécurité. Le rootkit peut permettre d'abriter de nombreux outils malicieux comme ceux vu précédemment.
- Un **publiciel** (**adware**) est un logiciel gratuit dont le créateur finance ses activités en affichant de la publicité lors de l'utilisation du logiciel.
- Les **canulars** (**hoax**), sont des courriers électroniques qui visent à tromper le destinataire en lui donnant des informations inexactes et, parfois, en lui faisant faire des actions qui lui sont dommageables
- L'**hameçonnage** (**phishing**), est une application d'ingénierie sociale effectuée par courrier électronique pour faire faire au destinataire une action qui lui est nuisible comme révéler un mot de passe ou transférer une somme d'argent à un fraudeur.
- Le **pharming** (ou **dévoiement** en français) permet de voler des informations sensibles (principalement des mots de passe) après avoir attiré la victime sur un site web maquillé afin de ressembler au site demandé par l'utilisateur, et ce même si le nom de domaine est correctement saisi. Ces redirections concernent généralement des sites sur lesquels on manipule de l'argent.

Un site vous permet de vérifier si une information est un canular :

http://www.hoaxbuster.com/

6. Antivirus

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur.

Il existe plusieurs méthodes d'éradication :

1. La suppression du code correspondant au virus dans le fichier infecté ;
2. La suppression du fichier infecté ;
3. La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

7. Détection des virus

Les virus se reproduisent en infectant des « applications hôtes », c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant. Or, afin de ne pas avoir un fonctionnement chaotique, les virus sont programmés pour ne pas infecter plusieurs fois un même fichier. Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté : il s'agit de la signature virale.

Les antivirus s'appuient ainsi sur cette signature propre à chaque virus pour les détecter. Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus.

Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus. Toutefois cette méthode ne permet pas la détection des virus n'ayant pas encore été répertoriés par les éditeurs d'antivirus. De plus, les programmeurs de virus les ont désormais dotés de capacités de camouflage, de manière à rendre leur signature difficile à détecter, voire indétectable : il s'agit de "virus polymorphes".

Certains antivirus utilisent un contrôleur d'intégrité pour vérifier si les fichiers ont été modifiés. Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille et éventuellement une somme de contrôle). Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.

La méthode heuristique consiste à analyser le comportement des applications afin de détecter une activité proche de celle d'un virus connu. Ce type d'antivirus peut ainsi détecter des virus même lorsque la base antivirale n'a pas été mise à jour. En contrepartie, ils sont susceptibles de déclencher de fausses alertes.

8. Camouflage des virus

Virus mutants : en réalité, la plupart des virus sont des clones, ou plus exactement des « virus mutants », c'est-à-dire des virus ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou leur signature.

Le fait qu'il existe plusieurs versions (on parle de variantes) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données.

Virus polymorphes : dans la mesure où les antivirus détectent notamment les virus grâce à leur signature (la succession de bits qui les identifie), certains créateurs de virus ont pensé à leur donner la possibilité de modifier automatiquement leur apparence, tel un caméléon, en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature, de façon à ce que seuls ces virus soient capables de reconnaître leur propre signature. Ce type de virus est appelé « virus polymorphe » (mot provenant du grec signifiant « qui peut prendre plusieurs formes »).

Rétrovirus : on appelle « rétrovirus » ou « virus flibustier » (en anglais bounty hunter) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

9. Choix d'un antivirus

Comme tous les logiciels recherchés, il devra être gratuit et en français.

Windows 10 possède un antivirus intégré : Windows Defender. Ce logiciel s'approche de plus en plus des performances apportées par les antivirus gratuits. Ce n'est qu'en passant à un antivirus payant que l'on obtient une protection nettement supérieure à celle de Windows Defender. Lorsqu'on installe un antivirus, Windows Defender se désactive pour lui laisser la place. Il est formellement déconseillé de faire tourner deux antivirus simultanément, les performances de la machine étant alors fortement dégradées. La plupart des antivirus gratuits proposent maintenant d'être installés sur la machine et de rester en mode passif. Ils peuvent alors être lancés à la demande pour faire une recherche occasionnelle en cas de doute de pollution de la machine.

Pour les utilisateurs de Windows 7, il reste plus que souhaitable de se protéger avec un antivirus gratuit ou non.

En conclusion :

1. La machine possède un antivirus : le conserver.
2. Sinon sous Windows 10, il est possible de se contenter de Windows Defender. Sous Windows 7 installer un antivirus.

Le cœur de l'antivirus gratuit est identique à celui de la version payante. Seuls manquent des services autour comme le contrôle parental, le filtre à spam, etc. Régulièrement évalués par des organismes de contrôle indépendants, ils donnent des résultats satisfaisants.

Quelques exemples, vous pouvez considérer qu'ils se valent tous (ordre alphabétique) :

- Avast
- AVG
- Avira
- Bitdefender.

Personnellement, j'utilise AVG depuis de nombreuses années. Son récent rachat par Avast est peut-être le signe d'une fusion des deux logiciels… L'inconvénient d'AVG est de collecter des données non personnelles pour ses besoins propres mais aussi pour les exploiter par ailleurs mais il ne s'en cache pas. Les avantages :

- Une analyse automatique des mails (pièces jointes et liens).
- Une interface bien conçue et simple d'utilisation.