QUELQUES VIRUS ET LEURS SPECIFICITES

Virus

Un **virus** est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a

Les **virus résidents** (appelés **TSR** en anglais pour *Terminate and stay resident*) se chargent dans la mémoire vive de l'ordinateur afin d'infecter les fichiers exécutables lancés par l'utilisateur. Les virus non résidants infectent les programmes présents sur le disque dur dès leur exécution.

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse.

Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection.

On distingue ainsi différents types de virus :

- Les **vers** sont des virus capables de se propager à travers un réseau ;
- Les **chevaux de Troie** (troyens) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle) ;
- Les **bombes logiques** sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...).

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 :

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

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.

Types de virus

Les 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.

Les 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*»).

Les 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.

Les virus de secteur d'amorçage

On appelle « **virus de secteur d'amorçage** » (ou *virus de boot*), un virus capable d'infecter le secteur de démarrage d'un disque dur (*MBR*, soit *master boot record*), c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.

Les virus trans-applicatifs (virus macros)

Avec la multiplication des programmes utilisant des macros, Microsoft a mis au point un langage de script commun pouvant être inséré dans la plupart des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic.

Ces virus arrivent actuellement à infecter les macros des documents Microsoft Office, c'est-à-dire qu'un tel virus peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (généralement Windows).

Or, de plus en plus d'applications supportent Visual Basic, ces virus peuvent donc être imaginables sur de nombreuses autres applications supportant le VBScript. Le début du troisième millénaire a été marqué par l'apparition à grande fréquence de scripts Visual Basic diffusés par mail en fichier attaché (repérables grâce à leur extension *.VBS*) avec un titre de mail poussant à ouvrir le cadeau empoisonné.

Celui-ci a la possibilité, lorsqu'il est ouvert sur un client de messagerie Microsoft, d'accéder à l'ensemble du carnet d'adresse et de s'auto diffuser par le réseau. Ce type de virus est appelé ver (ou worm en anglais).

Qu'est-ce qu'un hoax ?

On appelle **hoax** (en français *canular*) un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.

Ainsi, de plus en plus de personnes font suivre) des informations reçues par courriel sans vérifier la véracité des propos qui y sont contenus. Le but des hoax est simple :

- provoquer la satisfaction de son concepteur d'avoir berné un grand nombre de personnes.

Les conséquences de ces canulars sont multiples :

- L'**engorgement des réseaux** en provoquant une masse de données superflues circulant dans les infrastructures réseaux ;
- Une **désinformation**, c'est-à-dire faire admettre à de nombreuses personnes de faux concepts ou véhiculer de fausses rumeurs (on parle de *légendes urbaines*) ;
- L'**encombrement des boîtes aux lettres électroniques** déjà chargées ;
- La **perte de temps**, tant pour ceux qui lisent l'information, que pour ceux qui la relayent ;
- La **dégradation de l'image** d'une personne ou bien d'une entreprise ;
- L'**incrédulité** : à force de recevoir de fausses alertes les usagers du réseau risquent de ne plus croire aux vraies.

Ainsi, il est essentiel de suivre certains principes avant de faire circuler une information sur Internet.

Comment lutter contre la désinformation ?

Afin de lutter efficacement contre la propagation de fausses informations par courrier électronique, il suffit de retenir un seul concept :

Toute information reçue par courriel non accompagnée d'un lien hypertexte vers un site précisant sa véracité doit être considérée comme non valable !

Ainsi, tout courrier contenant une information non accompagnée d'un pointeur vers un site d'information ne doit pas être transmis à d'autres personnes. Lorsque vous transmettez une information à des destinataires, cherchez un site prouvant votre propos.

Comment vérifier s'il s'agit d'un canular ?

Lorsque vous recevez un courriel insistant sur le fait qu'il est essentiel de propager l'information (et ne contenant pas de lien prouvant son intégrité), vous pouvez vérifier sur le site **hoaxbuster** (site en français) s'il s'agit effectivement d'un hoax (canular).

Si l'information que vous avez reçue ne s'y trouve pas, recherchez l'information sur les principaux sites d'actualités ou bien par l'intermédiaire d'un moteur de recherche.

Les vers

Un **ver informatique** (en anglais *worm*) est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager; un ver est donc **un virus réseau**.

Les vers actuels

Les vers actuels se propagent principalement grâce à la messagerie (et notamment par le client de messagerie *Outlook*) grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes à tous ces destinataires.

Ces vers sont la plupart du temps des scripts (généralement VBScript) ou des fichiers exécutables envoyés en pièce jointe et se déclenchant lorsque l'utilisateur destinataire clique sur le fichier attaché.

Comment se protéger des vers ?

Il est simple de se protéger d'une infection par ver. La meilleure méthode consiste à ne pas ouvrir "à l'aveugle" les fichiers qui vous sont envoyés en fichier attachés.

Ainsi, tous les fichiers exécutables ou interprétables par le système d'exploitation peuvent potentiellement infecter votre ordinateur. Les fichiers comportant notamment les extensions suivantes sont potentiellement susceptibles d'être infectés : **exe, com, bat, pif, vbs, scr, doc, xls, msi, eml.**

Les chevaux de Troie

On appelle « **Cheval de Troie** » (en anglais *trojan horse*) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. Le nom « Cheval de Troie » provient d'une légende narrée dans l'*Iliade* (de l'écrivain *Homère*) à propos du siège de la ville de Troie par les Grecs.

Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à l'ordinateur sur lequel il est exécuté en ouvrant une **porte dérobée** (en anglais *backdoor*), par extension il est parfois nommé **troyen** par analogie avec les habitants de la ville de Troie.

A la façon du virus, le cheval de Troie est un code (programme) nuisible placé dans un programme sain (imaginez une fausse commande de listage des fichiers, qui détruit les fichiers au-lieu d'en afficher la liste).

Un cheval de Troie peut par exemple

- voler des mots de passe ;
- copier des données sensibles ;
- exécuter tout autre action nuisible ;
- etc.

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.

Les principaux chevaux de Troie sont des programmes ouvrant des ports de la machine, c'est-à-dire permettant à son concepteur de s'introduire sur votre machine par le réseau en ouvrant une **porte dérobée**.

Un cheval de Troie n'est pas nécessairement un virus, dans la mesure où son but n'est pas de se reproduire pour infecter d'autres machines. Par contre certains virus peuvent également être des chevaux de Troie, c'est-à-dire se propager comme un virus et ouvrir un port sur les machines infectées !

Détecter un tel programme est difficile car il faut arriver à détecter si l'action du programme (le cheval de Troie) est voulue ou non par l'utilisateur.

Les symptômes d'une infection

Une infection par un cheval de Troie fait généralement suite à l'ouverture d'un fichier contaminé contenant le cheval de Troie (voir l'article sur la protection contre les vers) et se traduit par les symptômes suivants :

- activité anormale du modem, de la carte réseau ou du disque: des données sont chargées en l'absence d'activité de la part de l'utilisateur ;
- des réactions curieuses de la souris ;
- des ouvertures impromptues de programmes ;
- des plantages à répétition.

Principe du cheval de Troie

Le principe des chevaux de Troie étant généralement (et de plus en plus) d'ouvrir un port de votre machine pour permettre à un pirate d'en prendre le contrôle (par exemple voler des données personnelles stockées sur le disque), le but du pirate est dans un premier temps d'infecter votre machine en vous faisant ouvrir un fichier infecté contenant le troyen et dans un second temps d'accéder à votre machine par le port qu'il a ouvert.

Toutefois pour pouvoir s'infiltrer sur votre machine, le pirate doit généralement en connaître l'**adresse IP**. Ainsi :

- soit vous avez une **adresse IP** fixe (cas d'une entreprise ou bien parfois de particuliers connecté par **câble,** etc.) auquel cas l'adresse IP peut être facilement récupérée
- soit votre adresse IP est dynamique (affectée à chaque connexion), c'est le cas pour les connexions par modem ; auquel cas le pirate doit scanner des adresses IP au hasard afin de déceler les adresses IP correspondant à des machines infectées.

Se protéger contre les troyens

Pour se protéger de ce genre d'intrusion, il suffit d'installer un **firewall**, c'est-à-dire un programme filtrant les communications entrant et sortant de votre machine. Un firewall (littéralement *pare-feu*) permet ainsi d'une part de voir les communications sortant de votre machines (donc normalement initiées par des programmes que vous utilisez) ou bien les communications entrant.

Toutefois, il n'est pas exclu que le firewall détecte des connexions provenant de l'extérieur sans pour autant que vous ne soyez la **victime choisie** d'un hacker. En effet, il peut s'agir de tests effectués par votre fournisseur d'accès ou bien un hacker scannant au hasard une plage d'adresses IP.

Pour les systèmes de type Windows, il existe des firewalls gratuits très performants :

- **ZoneAlarm**
- **Tiny personal firewall**

En cas d'infection

Si un programme dont l'origine vous est inconnue essaye d'ouvrir une connexion, le firewall vous demandera une confirmation pour initier la connexion. Il est essentiel de ne pas autoriser la connexion aux programmes que vous ne connaissez pas, car il peut très bien s'agir d'un cheval de Troie.

En cas de récidive, il peut être utile de vérifier que votre ordinateur n'est pas infecté par un troyen en utilisant un programme permettant de les détecter et de les éliminer (appelé *bouffe-troyen*).
C'est le cas de *The Cleaner*, téléchargeable sur http://www.moosoft.com.

Les bombes logiques

Sont appelés bombes logiques les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.

Ainsi, ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de *bombe à retardement* ou de *bombe temporelle*), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur : la bombe logique Tchernobyl s'est activée le 26 avril 1999, jour du 13ème anniversaire de la catastrophe nucléaire ...

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

Les espiogiciels

Un **espiogiciel** (en anglais **spyware**) est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé (on l'appelle donc parfois *mouchard*) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (on parle de *profilage*).

Les récoltes d'informations peuvent ainsi être :

- la traçabilité des URL des sites visités ;
- le traçage des mots-clés saisis dans les moteurs de recherche ;
- l'analyse des achats réalisés via internet ;
- voire les informations de paiement bancaire (numéro de carte bleue / VISA) ;
- ou bien des informations personnelles.

Les spywares s'installent généralement en même temps que d'autres logiciels (la plupart du temps des freewares ou sharewares). En effet, cela permet aux auteurs des dits logiciels de rentabiliser leur programme, par de la vente d'informations statistiques, et ainsi permettre de distribuer leur logiciel gratuitement. Il s'agit donc d'un modèle économique dans lequel la gratuité est obtenue contre la cession de données à caractère personnel.

Les spywares ne sont pas forcément illégaux car la licence d'utilisation du logiciel qu'ils accompagnent précise que ce programme tiers va être installé ! En revanche étant donné que la longue licence d'utilisation est rarement lue en entier par les utilisateurs, ceux-ci savent très rarement qu'un tel logiciel effectue ce profilage dans leur dos.

Par ailleurs, outre le préjudice causé par la divulgation d'informations à caractère personnel, les spywares peuvent également être une source de nuisances diverses :

- consommation de mémoire vive ;
- utilisation d'espace disque ;
- mobilisation des ressources du processeur ;
- plantages d'autres applications ;
- gêne ergonomique (par exemple l'ouverture d'écrans publicitaires ciblés en fonction des données collectées).

Les types de spywares

On distingue généralement deux types de spywares :

- Les **spywares internes** (ou *spywares internes* ou *spywares intégrés*) comportant directement des lignes de codes dédiées aux fonctions de collecte de données.
- Les **spywares externes**, programmes de collectes autonomes installés Voici une liste non exhaustive de spywares non intégrés : **Alexa, Aureate/Radiate,**

BargainBuddy, ClickTillUWin, Conducent Timesink, Cydoor, Comet Cursor, Doubleclick, DSSAgent, EverAd, eZula/KaZaa Toptext, Flashpoint/Flashtrack, Flyswat, Gator / Claria, GoHip, Hotbar, ISTbar, Lop, NewDotNet, Realplayer, SaveNow, Songspy, Xupiter, Web3000 et WebHancer.

Comment se protéger ?

La principale difficulté avec les spywares est de les détecter. La meilleure façon de se protéger est encore de ne pas installer de logiciels dont on n'est pas sûr à 100% de la provenance et de la fiabilité (notamment les freewares, les sharewares et plus particulièrement les logiciels d'échange de fichiers en peer-to-peer).

Voici quelques exemples (cette liste est non exhaustive) de logiciels connus pour embarquer un ou plusieurs spywares : **Babylon Translator, GetRight, Go!Zilla, Download Accelerator, Cute FTP, PKZip, KaZaA ou encore iMesh**.

Qui plus est, la désinstallation de ce type de logiciels ne supprime que rarement les spywares qui l'accompagnent. Pire, elle peut entraîner des dysfonctionnements sur d'autres applications.

Dans la pratique il est quasiment impossible de ne pas installer de logiciels. Ainsi la présence de processus d'arrière plans suspects, de fichiers étranges ou d'entrées inquiétantes dans la base de registre peuvent parfois trahir la présence de spywares dans le système.

Si vous ne parcourez pas la base de registre à la loupe tous les jours rassurez-vous, il existe des logiciels, nommés **anti-spywares** permettant de détecter et de supprimer les fichiers, processus et entrées de la base de registres créés par des spywares.

De plus l'installation d'un pare-feu personnel peut permettre d'une part de détecter la présence d'espiogiciels, d'autre part de les empêcher d'accéder à Internet (donc de transmettre les informations collectées).

Quelques anti-spywares

Parmi les anti-spywares les plus connus ou efficaces citons notamment :

- **Ad-Aware de Lavasoft.de ;**
- **Spybot Search&Destroy** .

Les keyloggers

Un **keylogger** (littéralement *enregistreur de touches*) est un dispositif chargé d'enregistrer les frappes de touches du clavier et de les enregistrer, à l'insu de l'utilisateur. Il s'agit donc d'un dispositif d'espionnage.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur.

Dans la mesure où les keyloggers enregistrent toutes les frappes de clavier, ils peuvent servir à des personnes malintentionnées pour récupérer les mots de passe des utilisateurs du poste de travail.

Cela signifie donc qu'il faut être particulièrement vigilant lorsque vous utilisez un ordinateur en lequel vous ne pouvez pas avoir confiance (poste en libre accès dans une entreprise, une école ou un lieu public tel qu'un cybercafé).

Keyloggers : logiciel ou matériel

Les keyloggers peuvent être soit logiciels soient matériels. Dans le premier cas il s'agit d'un processus furtif (ou bien portant un nom ressemblant fortement au nom d'un processus système), écrivant les informations captées dans un fichier caché.

Les keyloggers peuvent également être matériel : il s'agit alors d'un dispositif (câble ou dongle) intercalé entre la prise clavier de l'ordinateur et le clavier.

Se protéger des keyloggers

La meilleure façon de se protéger est la vigilance :

- N'installez pas de logiciels dont la provenance est douteuse ;
- Soyez prudent lorsque vous vous connectez sur un ordinateur qui ne vous appartient pas ! S'il s'agit d'un ordinateur en accès libre, examinez rapidement la configuration, avant de vous connecter à des sites demandant votre mot de passe, pour voir si des utilisateurs sont passés avant vous et s'il est possible ou non pour un utilisateur lambda d'installer un logiciel. En cas de doute ne vous connectez pas à des sites sécurisés pour lesquels un enjeu existe (banque en ligne, ...) .

Si vous en avez la possibilité, inspectez l'ordinateur à l'aide d'un anti-spyware.