

Diapo 18 (2005) Les virus : Différents types

Un ver 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 ...) pour se propager; un ver est donc **un virus réseau**.

On appelle "**Cheval de Troie**" (en anglais *trojan horse*) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur.

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 la machine sur laquelle 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.

Le virus macro s'attache au doc Word, Excel comme modèle. Un macro est un outil qui permet de faire des travaux manuels plates.

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 fréquences 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).

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 (anglicisé en *forwardent*) 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 relaye ;**
- **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 ([Google](#) étant un des plus fiables).

Un hoax est une information fausse, périmée ou invérifiable propagée spontanément par les internautes. Les hoax peuvent concerner tout sujet susceptible de déclencher une émotion positive ou négative chez le lecteur : alerte virus, disparition d'enfant, promesse de bonheur, pétition, etc. Ils existent avant tout sous forme écrite et incitent le plus souvent explicitement l'internaute à faire suivre la fausse nouvelle à tous ses correspondants.

http://www.cobweb.fr/s_page.php?Cible=31

Comment se protéger des vers ? <http://www.commentcamarche.net/virus/worms.php3>

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 susceptible d'être infectés :

exe, com, bat, pif, vbs, scr, doc, xls, msi, eml

Sous Windows il est conseillé de désactiver la fonction "*masquer les extensions*", car cette fonction peut tromper l'utilisateur sur la véritable extension d'un fichier. Ainsi un fichier dont l'extension est *.jpg.vbs* apparaîtra comme un fichier d'extension *.jpg* !

Ainsi, les fichiers comportant les extensions suivantes ne sont pas interprétés par le système et possèdent donc un risque d'infection minimale :

txt, jpg, gif, bmp, avi, mpg, asf, dat, mp3, wav, mid, ram, rm

Voici une liste plus complète (non exhaustive) des extensions des fichiers susceptibles d'être infectés par un virus :

Extensions
386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP

Quand on télécharge un fichier, même s'il contient un virus, rien ne se passera tant que le fichier n'est pas exécuté. Un fichier en texte pur, un .txt ne peut contenir de virus. Par contre dans un fichier Word, Excel si le texte ne peut contenir de virus, ce sont les macros associés au document qui peuvent être contaminés. Avec les dernières versions de ces produits, à l'ouverture de document contenant des macros, on est prévenu par le logiciel qui conseille de désactiver les macros, conseil qu'il faut suivre bien entendu.