SOMMAIRE

3. ***REPARATION EN CAS D'INFECTION et QUELQUES ASTUCES***

<u>CONCLUSION</u>

INTRODUCTION

Le “marché” des VIRUS s’est énormément développé dans le monde des PC qui font tourner les Systèmes d’exploitation DOS, OS/2… ou UNIX. En général, la faculté d’être envahis par des virus est beaucoup plus facile pour le système monotâche et monoutilisateur tel le DOS (Windows 3.x, Windows 95), contrairement aux autres systèmes comme OS/2 ou UNIX qui sont bien mieux protégés au niveau de la sécurité. De plus la conception de ces derniers est beaucoup plus complexe, ce qui diminue le risque d’être facilement compréhensible par les auteurs de virus.

Cet exposé fera en premier partie, le tour des principaux types de virus, de vers et d’autre programme malveillant, de la manière dont ils s’introduisent dans l’ordinateur, des dégâts et nuisances qu’ils peuvent causer sur les fichiers ainsi que sur le système d’exploitation. Ces connaissances sont indispensables pour apprendre à se protéger, ce qui fera l’objet de la deuxième partie.

Partie I : LES VIRUS INFORMATIQUES

I.1. GENERALITES ET HISTORIQUE

I.1.1. Généralités:

La destruction, l'altération, la modification accidentelles ou délibérées, ou encore le détournement frauduleux de l'information, ont existé depuis longtemps, mais le traitement automatisé des informations et la puissance conférée aux spécialistes par la connaissance des méthodes de programmation, ont donné naissance à un nouveau type de délinquance. Certains de ces délits se proposent d'altérer ou détruire l'information, ou de perturber le fonctionnement du système informatique.

Ces fonctionnalités font partie des caractéristiques essentielles d'un nouveau type d'agression en informatique : ***les virus informatiques***

I.1.1. Un peu d'histoire :

L'histoire prenait son commencement par « John Von Neumann » (Mathématicien Hongrois et auteur du principe sur lequel reposent les ordinateurs actuels) au moment où il a pu démontrer théoriquement la possibilité de programmes autocopiables en 1949. Dix (10) ans plus tard, cette théorie était matérialisée par des informaticiens des laboratoires BELL quand ils avaient inventé le jeu « core war ». L'idée était basée sur l'implantation des programmes capable de créer des copies de lui-même tout en cherchant à éliminer les programmes adverses dans la mémoire d'un ordinateur. Ces programmes n'ont pas encore rien de malveillant, et puisqu'ils ne s'agissaient et ne se développaient que dans le mémoire vive d'un ordinateur il était plus facile de les neutraliser. Il suffit d'éteindre cette mémoire pour que tout rentre à l'ordre. Mais ceci n'empêche pas quelqu'un de redouter une mauvaise utilisation ou disfonctionnement, ceci étant prouvé par F. Cohen en 1983, il démontra théoriquement la possibilité de créer de véritables virus (capables de se reproduire sur mémoire de masse et de se propager en causant des dommages irréversibles). A partir de cette époque, les choses sérieuses commencent. Les

virus deviennent un sujet très important dans le domaine de l'informatique. Les premiers virus tel : le virus « Brain » par Basit et amjad Farooq, le virus «Virdem » par Ralf Burger ont été des virus fonctionnant sous DOS.
Dès mars 93 deux virus conçus pour fonctionner dans l'environnement Windows 3 étaient signalés et il existe maintenant un nombre considérable de virus fonctionnant avec les diverses versions de Windows. Il faut signaler que les Windows de la série NT (NT 4, 2000, XP) sont beaucoup plus résistants aux virus classiques que les versions 95, 98 et Millenium qui sont basées sur le DOS.
Malheureusement il existe de plus en plus de virus et vers conçus pour les versions NT.
L'étape ultérieure a été la création de virus utilisant le langage de script de Microsoft : ce sont les virus spécifiques à Word ou Excel. Enfin, les premiers virus de mail sont apparus plus récemment. Certains détournent également ce langage de script.

En 2002 plusieurs antivirus proclamaient qu'il était capables de détecter plus de
61000 virus (en comptant leurs variantes) et beaucoup proposent des mises à jour hebdomadaires ou même quotidiennes. Actuellement ce nombre doit être nettement plus élevé, mais il est difficile de trouver des informations. Un antivirus connu annonce actuellement qu'il a une base de l'ordre de 60000 critères de détection différents. Sachant qu'un critère peut assez souvent servir à détecter plusieurs virus (ou autres programmes malveillants) proches, une estimation de l'ordre de 100000 virus, vers et chevaux de Troie (ou plus) est vraisemblable.
Les causes de cette inflation incroyable du nombre de virus et programmes apparentés sont multiples. Tout d'abord, il faut savoir qu'il est bien plus facile de modifier un virus existant que d'en créer un de toutes pièces. C'est pourquoi de nombreux virus ont donné naissance à des variantes multiples qui constituent des familles de virus. Les changements peuvent être mineurs et viser à empêcher (au moins temporairement) la reconnaissance du virus par un programme

comparant son code à une liste de référence des virus connus ; ils peuvent aussi modifier la fonction d'agression ou en introduire de nouvelles.

I.2. DEFINITION

Les Virus informatiques (appelés véritablement « CPA ou Code Parasite Autopropageable ») sont des codes qui ont la particularité: de s'auto reproduire, d'infecter (contaminer), d'activer et d'altérer ou même détruire le fonctionnement du système ou de l'information stockée.

- ***Autoreproduction:***

L'autoreproduction est le terme correcte pour designer tout programme doté de la faculté de se recopier lui-même sans l'intervention humaine, et soit de façon systématique, soit si certaines circonstances ou conditions sont remplies.

- ***Infection***

L'infection signifie que le programme dupliqué va se loger de manière illégitime dans certaines parties du système informatique. Les cibles privilégiées sont la mémoire centrale (ce ne peut être la seule cible car le virus ne se propagerait pas d'un ordinateur à l'autre, sauf à travers des réseaux, et disparaîtrait à l'extinction de l'ordinateur) et les zones d'informations exécutables contenues sur les disques ou les disquettes (on pense immédiatement aux programmes enregistrés sur ces supports, mais ce n'est pas le seul cas possible). Lorsque l'ordinateur tentera d'exécuter ces instructions, le programme viral qu'elles contiennent s'exécutera également.

- ***Activation***

L'activation du virus, ou plus exactement celle de sa (ou de ses) fonction(s) pathogène(s) se produira uniquement si certaines conditions sont réunies : par exemple lors du nième lancement du virus, lors d'un double clic, ou toute autre conjonction arbitraire de conditions.

- ***Alteration***

Lorsque les conditions d'activation sont remplies le virus déclenche en effet une fonction d'agression (payload en anglais) restée en sommeil : il prend

au moins partiellement le contrôle du fonctionnement de l'ordinateur pour lui faire accomplir des actions diverses. Par exemple certains virus anciens pouvaient afficher un message inattendu, faire tomber les lettres en cascade de leur position normale sur l'écran vers les lignes du bas, ralentir fortement le fonctionnement de l'ordinateur... Mais les virus se limitent rarement à ces gags agaçants ou fortement gênants. Très vite les virus sont devenus beaucoup plus pervers : en particulier la plupart d'entre eux altèrent de façon plus ou moins étendue (voire complète) les fichiers enregistrés sur les mémoires de masse contaminées.

*Tous autres programmes malveillants qui n'ont pas ces critères tels les programmes simples comme les bombes logiques, les chevaux de Troie, les portes dérobées, les outils de captures d'information, les outils d'attaque réseau, les outils d'appropriation des ressources ne sont donc pas des virus. On les appelle plutôt « **infections informatiques** ». Nous en parlerons un peu plus tard.*

I.3. TYPOLOGIE ET CLASSIFICATION

I.3.1. Types

On classe les virus par leurs modes de reproduction, leurs modes d'infection, leurs mode d'activation et par leurs effets pour chaque cible. Ainsi, on distingue :

- *les virus programmes dont le vecteur de contamination est constitué par les exécutables,*
- *les virus systèmes dont le vecteur de contamination est constitué par le secteur de partition ou le secteur de démarrage,*
- *les virus interprétés regroupant les virus macro sur les documents et les virus de script utilisant un langage de programmation particulier qui se rapproche de la programmation par lot (batch),*
- *Les virus multipartites ou multifonctions qui regroupent plusieurs cibles et renforcent leurs capacités de contamination,*

I.3.2. ***Contenu par type***

a) ***Les virus Programmes***

Ces virus ont pour cible les exécutable binaire compilé. En générale leurs infections se font par étape. Tout d'abords ils se logent dans un fichier exécutable. Lorsque ce fichier est lancé, c'est les virus programmes qui exécutent leurs codes en premier, ils passent alors dans la mémoire de l'ordinateur et recherche sur le disque un (des) nouveau(x) programme(s) à contaminer. La contamination se fait donc de proche en proche. Tant que la fonction d'agression de ce type de virus n'est pas activée, aucune manifestation de la présence du virus n'est perceptible pour un utilisateur non averti.

- ***Principe de fonctionnement***

Les virus programmes agissent par deux manières soit: ***par ajout de leurs codes au programme cible*** *soit* ***par remplacement d'une partie du code de ce programme****.*

- ***par ajout de leurs codes au programme cible***

Dans ce mode d'infection, les virus insèrent leur code dans celui du programme donc la longueur de celui-ci va augmenter de la longueur de celle du virus. Mais comme la longueur d'un virus peut être trop petite (peut descendre jusqu'à l'ordre de 135 octets), il est parfois difficile de savoir si le programme contaminé a une taille plus longue que celle d'origine. De plus, certains virus de ce type sont « furtif s» qui détournent leurs instructions pour afficher non pas la longueur exacte du programme contaminé, mais leurs longueurs diminuées, alors le programme semblera avoir gardé sa longueur initiale. Cet effet peut faire tromper l'utilisateur.

- ***par remplacement d'une partie du code de ce programme***

Pour ce mode d'infection, la taille du fichier contaminé ne change pas mais on observera probablement assez vite des dysfonctionnements ou des blocages correspondant aux parties du programme remplacées (toutefois s'il

s'agit d'une partie du programme qui est rarement utilisée le problème tardera à se manifester).

- ***Exemples***

b) ***Les virus systèmes***

Il n'y a pas que les fichiers de programmes qui peuvent contenir du code exécutable. Mais en raison de la manière dont le système d'exploitation démarre et prend le contrôle des disques et disquettes, le premier secteur de la disquette (secteur d'amorçage ou secteur de boot/ Boot et DBR) ou les premiers secteurs du disque dur (secteur de la table de partition et secteur d'amorçage/ Boot et MBR) peuvent contenir un bout de code exécutable. C'est donc un endroit rêvé pour installer un virus. S'il s'agit du disque à partir duquel le système d'exploitation est chargé, ce procédé est d'autant plus redoutable que le code du virus s'exécutera et se chargera en mémoire au démarrage, avant le chargement du système d'exploitation et à plus forte raison avant celui d'un éventuel logiciel antivirus.

- ***Principe de fonctionnement***

Les virus du système (appelé aussi virus de boot) s'installent dans un ordinateur généralement par ***démarrage de celui-ci avec une disquette contaminée*** *ou par* ***les virus de programme.***

- *Par démarrage de l'ordinateur avec une disquette contaminée*

Par défaut, le BIOS tente normalement de lire le contenu du secteur d'amorçage de ***A:*** *avant celui de la partition* ***C:*** *cet effet facilite l'introduction du virus dans le secteur de d'amorçage (DBR) de la disquette via une disquette contaminée (qui peut ne pas contenir de programme) présente dans le lecteur* ***A:*** *(que cette disquette contienne ou non le DOS). Une fois présent dans le secteur d'amorçage, le virus contamine l'ordinateur lorsque le BIOS exécute le code. Le virus déplace ou écrase le code original du BOOT ou MBR du disque dur tout en remplaçant ce code par lui-même et il sauvegarde éventuellement le code excèdent dans un autre secteur libre ou occupé alors dès et à chaque*

démarrage, le virus sera résidant en mémoire et capable d'infecter une autre disquette ou autre partition.

- *Par les virus programmes*

Toutefois, les virus du type programme peuvent être également conçus pour aller infecter secondairement le secteur de boot. Le virus se loge d'abord dans un fichier exécutable et il ne fait qu'attendre le prochain démarrage. Dès que l'ordinateur redémarre c'est à dire lorsque le BIOS exécute le code, le virus prend le contrôle du BOOT ou MBR du disque dur et exécute les instructions que son auteur a programmées.

- ***Exemples:***

Infection du MBR : ***Jumper.B, Antiexe.***
Infection du Boot : ***Form.***

c) ***Les virus interprétés***

Les virus interprétés regroupent les virus macro et les virus de script.

1°) Les virus macro

Les applications sophistiquées de l'informatique bureautique, telles que le traitement de texte Word ou le tableur Excel, contiennent un langage de programmation qui permet d'automatiser des opérations complexes grâce à l'écriture de macroinstructions (connues sous le nom de macros) exécutées par l'application. Ces macros sont enregistrées dans les documents. Autrement dit, tout document renfermant des macros contient du code exécutable. Cette particularité a ouvert la porte à l'apparition de virus écrits en langage de macros et incorporés par des mécanismes d'infection spécifiques dans ces documents.

Les variations autour du concept du virus macro sont très nombreuses. Les modifications peuvent porter sur l'environnement : Barre d'outil, Menu, Raccourcis clavier, etc. Leurs effets peuvent être similaires à ceux des virus programme tels la modification de l'environnement, la modification du contenu du fichier, l'effacement du fichier, etc.

- ***Exemples***

Quelques exemples des virus macro : WM/Concept, W97M/Class, X97M/Laroux, O97M/Tristate, W97M/Melissa@MM, etc…

i. Les virus de script

Le langage script est un langage de programmation destiné à contrôler l'environnement d'un logiciel. Lorsqu'il est interprété, on peut l'exécuter sur tout ordinateur disposant de l'interprétateur approprié. Deux les plus utilisés sont les VBScript et les Javascript.

Le fait que ce langage de programmation se repose sur des codes source en clair mais non sur des codes compilés comme les applets, il est plus facile pour les auteurs (tant que professionnelles qu'aux amateurs) de modifier les codes sources (d'un virus ou peut être non) qu'ils rencontrent et peuvent aboutir par la création ou développement d'un virus.

- ***Exemples***

- *Sous VBScript : VBS/Freelink@MM, VBS/Monopoly@MM, VBS/Treplesix@MM,etc..*
- *Sous Java : JV/Strange Brew*
- *Sous JavaScript : JS/Kak@M*

d) Les virus multipartites

Ces sont des virus qui cumulent les cibles et renforcent ainsi leur capacité de contamination. Ils cherchent souvent à infecter les zones mémoire du disque dur ou des autres secteurs de masse et les fichiers exécutables. Leur but étant une plus grande propagation et tente de faire planter l'ordinateur. Certains virus de ce type infectent par exemple le secteur de partition du système puis, une fois résident en mémoire vive, infectes les fichiers exécutables sur d'autre unité logique.

- ***Exemples***

- *Tequila, One-Half, etc.*

e) Les virus polymorphes

Ces sont des virus qui peuvent prendre plusieurs formes. Les formes à prendre sont relatives en fonction de l'antivirus que l'utilisateur utilise. Cette relativité est réalisée en dotant les virus de fonction de chiffrement et de déchiffrement de leur signature (la succession de bits qui les identifie), de façon à ce que seuls ces virus soient capables de reconnaître leur propre signature. En effet, il est plus difficile pour les antivirus de détecter notamment les virus grâce à leur signature.

f) ***Les rétrovirus***

*On appelle « **rétrovirus** » ou « virus flibustier » (en anglais bounty hunter) un virus doté la faculté de déchiffrer et de modifier les signatures des antivirus afin de les rendre inopérants.*

3. ***Les autres infections informatiques :***

Une infection informatique est un programme malveillant qui peut produire des nuisances sur les systèmes informatiques alors qu'elle n'est pas autopropageable, ni autoduplicable : ce n'est donc pas des VIRUS. Il existe plusieurs types d'infection informatique dont nous allons voir ci-après.

a) ***Le ver***

Un ver est un programme malveillant qui a une existence autonome (ce n'est pas un parasite). Ainsi, contrairement aux virus les vers ne doivent pas se loger dans des programmes (ou autres informations exécutables) pour agir.

En général les concepteurs de virus s'efforcent de faire des programmes de petite taille pour rendre l'infection discrète. Au contraire, bien qu'on connaisse des vers très courts, beaucoup sont d'une taille nettement plus importante car ils ne cherchent pas à se cacher, mais à se faire passer pour un fichier normal." Certains résident uniquement en mémoire et disparaissent donc lorsqu'on éteint la machine; plus fréquemment ils sont enregistrés sur le disque dur et utilisent divers moyens pour se lancer à l'insu de l'utilisateur. Par exemple dans la plateforme Windows, la solution la plus utilisée consiste à introduire de façon clandestine le nom du ver dans la clé RUN de la base de registre.

b) *La bombe logique*

Une bombe logique est une fonction illicite ajoutée par un informaticien à un programme normal hébergé par un ordinateur. Cette fonction est généralement conçue pour se déclencher si certaines conditions particulières sont réalisées, de façon à constituer un moyen de vengeance ou de pression sur une entreprise. Un exemple bien connu est celui d'une bombe logique qui devait entrer en action si le nom de l'informaticien disparaissait du fichier du personnel. Lorsque l'informaticien fut licencié, la bombe logique commença à effacer progressivement des noms de clients du fichier de l'entreprise. Lorsque celle-ci s'en aperçut, longtemps après, les dommages étaient considérables et l'entreprise était au bord de la faillite. Compte tenu de la complexité des programmes, il est très facile de dissimuler de telles bombes. C'est toujours une agression commise par un informaticien au service de l'entreprise ou un prestataire de services. Il est vraisemblable qu'on ne sait pas tout dans ce domaine et bien d'autres cas ont dû être affrontés, ou négociés, avec un maximum de discrétion. On imagine toute l'importance que cette arme pourrait avoir pour des logiciels « sensibles », par exemple en terme de défense nationale.

c) *Le Cheval de troie*

Le cheval de Troie, au contraire, est un programme entièrement conçu pour provoquer des dommages, mais en empruntant le nom et l'apparence d'un programme ayant une autre fonction. En réalité, son action véritable était de détruire la table d'allocation du disque dur, ce qui entraînait la perte de tout le contenu de celui-ci. Les chevaux de Troie existent toujours et sont souvent désignés par l'appellation anglaise « trojan horse », ou plus brièvement «trojan» (ce qui est stupide puisque le cheval de Troie d'Homère n'était pas troyen,mais grec).

d) *Les backdoors*

Le terme backdoor se traduit par « porte dérobée ». C'est un moyen pour contourner la manière normale d'entrer dans un programme. A l'origine il s'agit d'une pratique informatique tout à fait normale : au cours de la mise au point d'un programme le programmeur peut souhaiter entrer dans le programme ou dans certains modules de celui-ci par une voie plus directe que celle offerte par l'exécution normale. Ces points d'entrée peuvent court-circuiter les procédures d'accès et les sécurités du programme. Normalement ces backdoors doivent être supprimées lorsque le programme a fini d'être testé. L'idée peut être généralisée à des fins malveillantes. Divers virus, vers ou chevaux de Troie peuvent installer des backdoors sur un ordinateur, ce qui permet à un pirate de prendre le contrôle de la machine, en général avec des privilèges d'administrateur. A partir de ce moment-là il est possible de faire n'importe quoi : pirater le contenu de l'ordinateur, récupérer le mot de passe vers un compte bancaire, et surtout se servir de cet ordinateur pour lancer, de façon masquée, une attaque vers d'autres ordinateurs bien plus intéressants du point de vue du pirate.

Chevaux de Troie et backdoors sont souvent introduits subrepticement par des vers ou la visite de pages Web piégées.

e) Les robots

Les robots, qui cumulent souvent les fonctionnalités de type ver et une activité d'appropriation des ressources, d'attaque réseau et/ou d'espionnage.

f) Autres virus

On distingue aussi les virus actuellement en circulation (virus in the wild, dans le jargon des spécialistes) et les virus in the zoo, qui ne se rencontrent que dans les collections des spécialistes et des éditeurs d'antivirus. Ce dernier groupe comprend des virus qui n'ont jamais vraiment réussi à percer, des virus expérimentaux et des virus très anciens qui ne se rencontrent plus actuellement. Cette distinction est importante : en raison de l'inflation du nombre des virus les éditeurs ont tendance à retirer de la base de signatures les virus les plus

anciens, afin d'éviter d'avoir une base de taille excessive qui ralentirait fortement l'analyse.

I.4. ***Voie d'entrée des virus***

Les ordinateurs sont isolés ou regroupés en réseaux locaux ou reliés à l'Internet. Un
virus ne peut s'introduire que par intermédiaire d'un support (disquette, CDROM, disque amovible, etc…) utilisé ou gravé dans un ordinateur contaminé ou par le réseau. Il faut se souvenir que des virus peuvent être transmis même par des fichiers Word ou Excel et non pas forcement via des fichiers exécutables.

Avec le développement des réseaux, les disquettes constituent maintenant une source mineure de virus, comme le prouve l'envahissement actuel par les virus ou vers de mail, mais aussi le cas moins connu du public de virus véhiculés par des pages Web, par IRC, par les échanges P2P comme Kazaa, ou ceux qui attaquent directement à travers l'Internet en l'absence de toute action de l'utilisateur. Un ordinateur en réseau local peut aussi être contaminé sans qu'aucune manipulation imprudente n'ait été effectuée à son niveau, tout simplement parce qu'un virus résidant initialement sur un autre ordinateur s'est propagé à travers le réseau. Ceci se produit par exemple avec divers vers lorsqu'il existe des disques partagés dans un réseau Windows.

Partie 2 : LES PROTECTIONS CONTRE LES VIRUS

II.1.RECOMANDATIONS ET PRECAUTIONS NECESSAIRE

Face aux multiples fonctions ainsi qu'aux type de virus très nombreux, l'utilisation de logiciel antivirus ne suffit pas pour protéger contrer les virus. L'organisation de la lutte antivirale passe par la mise en place des mesures et précautions à prendre pour l'utilisateur, suivi de la mise en place des outils de détection et de préventions depuis le poste de travail jusqu'à la passerelle internet.

II.1.1. ***Dimension humaine***

Les préventions fondamentales contre les virus reposent sur les mains des utilisateurs. Voici quelques-unes qui pourront être efficace.

- *Même si l'utilisation des disquettes n'est plus en vogue à nos jours, ils y en a encore des simples utilisateurs qui travaillent avec ces support, pour eux il est préférable de rendre le disque C: prioritaire avant le lecteur A: en modifiant un réglage du BIOS. Cette approche diminue le risque d'être contaminé via une disquette.*

- *Faire des générations de sauvegarde régulière et successives (par exemple un jeu de sauvegardes renouvelé journellement, un autre jeu qui sera renouvelé toutes les semaines, un autre tous les mois... selon l'importance des fichiers et de la fréquence de leur modification.) des fichiers importants sur des supports extractibles* ***(disque externe, CDROM R/W, etc..). Cette approche permet de*** *revenir à une copie*

*intacte **e**n cas **d'attaque par un virus.** Il faut toutefois être sûr que la copie de sauvegarde est saine, ce qui n'est pas toujours évident ; c'est pourquoi il faut faire : si la dernière est défectueuse, il faut revenir à l'avant dernière, ou même plus en arrière encore. C'est pourquoi dans le cas d'un réseau ces opérations de sauvegarde sont automatisées et sont faite au niveau du ou des serveurs sur des bandes magnétiques.*

- *Pour les utilisateurs de mail il est indispensable de contrôler son courrier avant de l'ouvrir et en particulier les pièces jointes. Concernant les pièces jointes, lorsqu'ils ont une double extension ou une des extensions telles: COM, EXE, BAT, PIF, VBS, LNK, SCR ce sont pratiquement à coup sûr des fichiers de virus. Pour y faire face, une bonne règle est de préciser dans le texte du message le nom et la nature du fichier joint. Si le message provient d'une personne de confiance ET si le fichier attaché est clairement annoncé dans le texte par l'expéditeur du message, on peut considérer que sa consultation est probablement peu risquée. Dans tous les autres cas il faut considérer que le fichier est suspect (même si on connait l'expéditeur). Il est aussi préférable de donner de préférence une adresse webmail dans les forums ou lors des téléchargements.*

2. ***Mettre à jour régulièrement les correcteurs de sécurité des logiciels***

Comme on le sait bien, tous les logiciels comportent souvent des failles de sécurité. Pour pallier à ces failles, il est nécessaire de télécharger les patchs de sécurité régulièrement mis à jour par les fabricants. Pour cela on a qu'à :

- *Fermer toutes les applications et **aller dans Windows Update.** En cas de gros problème, on trouvera un message illustrant quoi faire. A titre d'exemple pour Sasser, installer la mise à jour KB835732 pour xp.*

- *Cliquer sur "Rechercher des mises à jours". Dans le cas où la mise à jour qu'on cherche n'apparaît pas dans la liste, tant mieux. Cela signifie que cette mise à jour est déjà installée dans l'ordinateur. (Configuration automatique) sinon, on la télécharge.*
- *Regarder si d'autres mises à jour sont nécessaires.*
- *Installer les patchs concernant Outlook express et MS Explorer.*

2. *UTILISATION DES LOGICIELS*

1. *Les antivirus, logiciels anti-espions et mise à jour*

1. *Les antivirus*

Pour commencer, il est intéressant de souligner que malgré les complexités et facultés multiples que les virus possèdent tels le changement de son signature par lui-même, les facultés de déchiffrer les codes de signature de l'antivirus, aucun programme antiviral ne peut garantir une efficacité absolue, même s'il le prétend. Cependant, il faudra envisager l'utilisation systématique d'un programme antivirus ceci réduit fortement les risques. Il existe divers programmes commerciaux tout à fait sérieux. Ils permettent de contrôler et, lorsque c'est possible, de décontaminer les fichiers, disques infectés. Des versions sont adaptées à la protection des réseaux et certaines prennent en charge les risques nouveaux liés à l'utilisation d'Internet.

Beaucoup d'antivirus détectent les virus en recherchant systématiquement ces signatures dans le secteur d'amorçage et les fichiers. Il est évident que chaque virus (ou famille de virus) possède sa propre signature. En conséquence, on doit fournir une liste de signatures aux antivirus utilisant cette méthode. Bien entendu on ne peut détecter que des virus déjà connus; c'est pourquoi la liste des signatures doit être complétée périodiquement.

Posséder un antivirus a peu d'intérêt si on ne dispose pas de mises à jour fréquentes. Les antivirus doivent en effet être mis à jour régulièrement (au moins toutes les semaines, tous les jours si possible) en téléchargeant sur Internet les nouveaux fichiers de définitions virales. Cette opération peut être

automatisée sur la plupart des antivirus actuels. Ceci montre l'aspect illusoire des antivirus piratés.

L'idéal serait de pouvoir identifier dans le code des structures logiques caractéristiques des mécanismes viraux en général. Ceci rendrait possible la détection de virus encore inconnus. Malheureusement, rien ne permet d'identifier avec certitude un virus par cette méthode. Certains détails de structure sont fortement suspects car ils sont souvent employés dans les virus, mais l'exploration systématique des programmes montre qu'on peut parfaitement les rencontrer dans des logiciels tout à fait normaux, et même dans des fichiers du système d'exploitation.

- ***Bien utilisé l'antivirus***

Pour exploiter au maximum un logiciel antivirus, il y a deux stratégies fondamentales qu'on doit suivre.

- *La première est d'utiliser ces outils pour scanner tout fichier nouveau avant installation, et les support**s (flash disk, CD-ROM, etc..)** avant utilisation. Par précaution il est également recommandé de scanner périodiquement **le** disque dur.*
- *La deuxième technique consiste à installer en mémoire au démarrage de l'ordinateur un module antivirus spécial, appelé généralement moniteur. Tous les antivirus actuels possèdent un moniteur. Celui-ci peut rechercher automatiquement la signature de virus connus dans tout fichier devant être exécuté ou recopié. Il peut aussi surveiller en permanence l'activité de l'ordinateur, détecter et empêcher tout comportement suspect: tentative d'écriture sur le secteur d'amorçage, modification de la table d'allocation en dehors des procédures normales, effacement inopiné de fichier, formatage du disque, écriture directe sur le disque (en particulier dans un fichier de programme), contournement des fonctions du système d'exploitation ou détournement de celles-ci de leur rôle normal. Cette stratégie permet, en théorie, d'intercepter à la source les*

tentatives de contamination ou d'agression des virus même inconnus. Cependant, il ne faut pas choisir les moniteurs fonctionnant en temps réel car ils peuvent être moins efficaces que les programmes d'analyse lancés à la demande (pour des questions d'encombrement en mémoire ou de charge du microprocesseur) : ils ne dispensent donc pas de faire une analyse systématique du disque de façon périodique.

- *Si l'antivirus est paralysé par un virus ou ver il faut un Internet Explorer et on peut avoir recours à un antivirus en ligne, tel ceux qui sont disponibles sur les sites suivants:*

  http://fr.trendmicroeurope.
  com/consumer/products/housecall_pre.php
  http://www.mcafee.com/myapps/mfs/default.asp
  http://www.pandasoftware.com/activescan/fr/activescan_principal.htm
  http://www.bitdefender.com/scan/licence.php
  http://www.secuser.com/antivirus/index.htm

2. ***Les logiciels anti-espion***

Ils protégeront des logiciels espions appelés aussi les spywares qui sont des logiciels qu'un "cyberpirate" installe sur un ordinateur cible sans en informer le propriétaire. Son but étant de récolter des informations intéressantes (mots de passe, no de carte de crédit…). Il faut faire attention, ces spywares sont rarement détectés par de simples antivirus.

2. ***Les pare-feux (firewalls)***

Lorsqu'un ordinateur est connecté à l'Internet il est susceptible de subir des agressions variées en provenance du réseau. Ces tentatives d'intrusion utilisent des portes d'entrées (ports) par lesquels les divers protocoles communiquent avec d'autres ordinateurs (par exemple les serveurs Web communiquent à travers le port 80).

Le rôle d'un programme pare-feu est de fermer tous les ports inutilisés et d'ouvrir les ports nécessaires sur la base de critères bien précis. On trouve des programmes pare-feux facilement utilisables pour un usage personnel. Ils sont gratuits ou peu coûteux. Windows XP possède un petit firewall incorporé, mais il bloque uniquement ce qui pourrait venir de l'extérieur et ne permet pas de limiter ce qui sort de l'ordinateur, de telle sorte qu'un cheval de Troie ou spyware qui serait installé sur l'ordinateur pourrait communiquer en toute impunité avec l'extérieur (par exemple si vous êtes contaminé avec un ver de mail, il peut envoyer à l'extérieur à votre insu des milliers de mails infectés). Il est question que ce défaut soit corrigé dans le Service Pack 2 pour Windows XP. L'utilisation des parefeux dépasse largement le problème des virus/vers qui peuvent attaquer les ordinateurs directement à travers le réseau, mais il faut retenir que ce type de protection est absolument indispensable (même si là non plus l'efficacité absolue n'est pas garantie) le risque étant proportionnel à la durée de la connexion (les utilisateurs de l'ADSL restent en général connectés en permanence).

II.3. *Réparation en cas d'infection et Astuces*

La réparation en cas d'infection dépend totalement du type de virus et de la plate-forme utilisée. Vu la complexité de déchiffrer les virus, la plupart des opérations de réparation portant sur les fichiers ou le disque dur ne sont pas à la portée de n'importe qui, même en ayant des connaissances de base en informatique. Certaines tentatives maladroites causent plus de dommages que le virus lui-même et contrairement à ce qu'on pense un formatage complet du disque (dans l'espoir d'effacer toute trace de contamination) est inutile et même ne détruit pas les virus de système contenus dans le premier secteur du disque (table de partition ou MBR). Il ne suffit pas de désinfecter le disque dur. Il faut aussi examiner toutes les supports utilisés ou gravés sur les ordinateurs contaminés.

- ***Types et procédures d'intervention***

On distingue deux types d'interventions. Dans certains cas, le virus ou vers sera détecté avant le déclenchement de sa fonction de dommage. S'il s'agit d'un virus du système, il suffit de remplacer le secteur d'amorçage par une copie saine de celui-ci (idem si le virus est dans la table de partition, mais c'est plus délicat). S'il s'agit d'un virus de programme, la solution la plus simple est de détruire les programmes infectés et de les remplacer par une copie de réserve saine.

Dans un certain nombre de cas il est possible de réparer le fichier en supprimant le code du virus. Bien entendu, il ne faut pas que le virus ait détruit une partie du code du programme. Divers antivirus proposent la réparation automatique des programmes (pour certains virus uniquement). Tous les antivirus n'ont pas la même efficacité quant au nombre de virus qu'ils peuvent traiter ou l'état (plus ou moins fonctionnel) dans lequel ils restaurent les programmes. Les contaminations simultanées par plusieurs virus peuvent être redoutables car les tentatives de réparation risquent d'entraîner des dommages irréparables. Si la contamination touche des ordinateurs professionnels dont l'usage est critique, il vaut mieux payer le prix et utiliser les services d'un vrai spécialiste en sécurité (ils sont malheureusement très peu nombreux).

Contrairement aux virus, les vers sont autonomes puisqu'ils ne se greffent pas sur des programmes. Leur élimination est donc plus facile. Comme la quasi-totalité des « virus » de mail sont en fait des vers, cela explique pourquoi les éditeurs d'antivirus peuvent fournir très rapidement en téléchargement gratuit de petits utilitaires spécialisés dans l'élimination de chacun des vers susceptibles de contaminer un ordinateur. Face à un fichier contenant un virus qui ne peut être désinfecté, l'antivirus propose généralement l'effacement complet ou la mise en quarantaine (en gros, mise à l'abri dans un répertoire spécial). On rencontre toutefois de plus en plus de cas où l'élimination d'un ver (ainsi que des chevaux de Troie ou des backdoors qu'il installe) semble impossible. Cela peut être dû à deux problèmes. Le premier est qu'on ne peut généralement pas effacer le fichier d'un programme actif. Le deuxième est que de plus en plus de vers désactivent les antivirus connus. Cette difficulté est

généralement réglée en démarrant l'ordinateur en mode sans échec avant de pratiquer la désinfection. Il faut savoir que divers antivirus ne détectent pas les virus/vers des messages stockés dans Outlook ou Outlook Express en raison du format d'enregistrement; d'autres possèdent une option pour scanner la messagerie, mais cette option est inutile voire nuisible. En effet ces virus ou vers ne peuvent pas s'activer lorsqu'ils sont archivés. En outre chaque dossier (par exemple Boîte de réception) correspond à un fichier unique qui peut être de taille importante si on a l'habitude d'archiver ses mails. Comme souvent la seule solution en cas d'infection serait de détruire le fichier (ce qui est fait parfois automatiquement), on perdrait alors tous les mails archivés. Le bon réflexe, si on veut consulter le document attaché à un mail, consiste à l'enregistrer sur le disque dur et à le scanner avant ouverture (beaucoup d'antivirus, mais pas tous, détecteront d'ailleurs un éventuel virus dès la phase d'enregistrement).

Le deuxième type d'intervention correspond aux cas où le virus a déjà causé des dommages. Dans ce cas, il faudra détruire toute trace du virus mais également essayer de réparer ce qui peut l'être, car toutes les situations peuvent se rencontrer, depuis l'altération d'un petit nombre de fichiers jusqu'au formatage du disque dur. La règle de base est que tous les fichiers présents sur un disque dur doivent être régulièrement sauvegardés sur un support extractible, comme cela a déjà été expliqué. Il faut cependant savoir que certains dégâts qui semblent importants sont parfois plus facilement réparables qu'on ne le pense. Un fichier entièrement effacé peut souvent être récupéré grâce à des programmes spécialisés. Il en est de même pour un disque reformaté si certaines précautions ont été prises au préalable. De même une atteinte de la table de partition du disque peut faire croire que celui-ci est hors d'usage alors qu'il peut être récupéré assez facilement.

- ***Astuces pour combattre les infections des virus***

Comme mentionné plus haut, les réparations des infections des virus dépendent généralement du type des virus ainsi que de la plate-forme utilisée.

*- Une autre méthode pour éradiquer un virus présent sur une machine, si on sait le nom de virus, la meilleure méthode consiste tout d'abord à déconnecter la machine infectée du réseau, puis à récupérer le kit de désinfection adhoc**.** Pour cela redémarrer l'ordinateur en mode sans échec et de lancer l'utilitaire de désinfection. Un kit de désinfection est un petit exécutable dont le but est de nettoyer une machine infectée par un virus particulier. Chaque kit de désinfection est donc uniquement capable d'éradiquer un type de virus particulier voire une version particulière d'un virus. Les utilitaires de désinfection present ci-dessous ne remplacent en rien l'action d'un logiciel antivirus. Comme expliqué auparavant l'antivirus a un rôle préventif, afin d'intercepter le virus avant l'infection de la machine. Toutefois en cas d'infection, les kits de désinfection nous permettront de prendre des mesures correctives pour éradiquer le virus. On pourra en trouver sur le site :*

http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

CONCLUSION

- ***Actuellement, on trouve des logiciels qui agissent à la fois comme pare-feu, antivirus, anti-spam et anti espion. Ils ne protègent pas totalement mais diminuent considérablement les risques. Certains sont gratuits d'autres payants.***

S'il convient d'éviter la paranoïa, il faut également éviter de croire que les virus ne touchent que les autres !

Un ordinateur non protégé = un appartement avec une porte grande ouverte.

Rester vigilant, s'informer, se protéger

- *avec un antivirus régulièrement mis à jour, un pare-feu et un anti-espion*
- *mettre à jour les patchs des systèmes d'exploitation,*
- *trier son courrier avant de l'ouvrir,*
- *sauvegarder ses données sur un support externe.*