

VIRUS et ANTIVIRUS

<u>1. Les virus</u>	2
1.1. Qu'est-ce qu'un virus ?	2
1.2. Les formes de virus	3
1.3. Ce que les virus ne peuvent pas faire	4
1.4. Comment se propagent-ils ?	5
1.5. Pourquoi des virus ?	5
<u>2. Les antivirus</u>	6
2.1. Q'est ce qu'un antivirus ?	6
2.2. Comment se protéger ?	7
2.3. Comment savoir si son PC a "attrapé" des virus ?	8
2.4. Aspects techniques des antivirus	8
2.5. Efficacité des antivirus	11
<u>3. Quelques virus</u>	12
<u>4. Quelques adresses</u>	12
<u>5. Bibliographie</u>	13

1. Les virus.

1.1. Ou'est-ce qu'un virus ?

1.1.1. Définition.

Il s'agit d'un programme auto-reproductible et généralement destructeur qui contamine le disque dur ainsi que toute autre disquette utilisée et qui peut faire exécuter à l'ordinateur des actions non désirées.

Un virus informatique peut donc se propager à l'intérieur même de l'ordinateur, en infectant petit à petit tous les fichiers. Il est donc destiné à modifier à notre insu le fonctionnement de l'ordinateur, soit sur le secteur d'amorçage, soit en infiltrant les exécutable, ainsi que les macro virus qui se propagent via les fichiers de données.. Cette modification peut être un changement du contenu des fichiers, voire la suppression de ceux ci.

Certains virus peuvent simplement faire «beeper» le PC, d'autres peuvent détruire les données (formater, effacer le secteur de démarrage, voir détruire le matériel). Les virus peuvent être classés par catégories d'importance : d'ennuyeux à destructifs. Leur principale caractéristique réside dans leur capacité de "réplication", consistant généralement à s'attacher à une certaine catégorie de fichiers, parfois des exécutable .EXE ou des .COM...

1.1.2. Fonctionnement.

Sur les systèmes DOS et Windows, ils infectent principalement les fichiers .EXE et .COM. Ils infectent également les fichiers "systèmes", c'est-à-dire .SYS, .BIN, .OVL, .DRV. Une fois le virus attaché au fichier, c'est celui-ci qui devient dangereux pour la sécurité. Transporté sur un autre système, il peut infecter d'autres fichiers sans contact avec le virus original. Il existe maintenant des virus «de fichiers de données» ou «virus de macros», dont la particularité est de s'attaquer aux documents (World, Excel).

1.1.3. Objectifs des virus.

L'objectif d'un virus est de pouvoir se dupliquer le plus souvent possible sur une ou plusieurs cibles. Il existe trois phases d'existence :

- **Infection** : le virus infecte le système cible,
- **contamination** : il se duplique et infecte d'autres cibles sans perturber le fonctionnement du système,
- **destruction** : il entre en activité et produit les effets pour lesquels il a été conçu.

1.2. Les formes de virus.

1.2.1. Différentes familles de virus.

Il existe 5 familles de virus, mais une famille peut avoir un virus commun avec une autre famille.

- Virus de boot (secteur d'amorçage) : il remplace ou s'implante lui-même dans le secteur de boot (une partie du disque utilisée lors du démarrage de la machine). Ce type de virus peut empêcher la machine de démarrer.
- Virus exécutable : ils infectent un programme pour être lancés en même temps que lui.
- Virus macro : ils infectent les documents créés par les logiciels de la suite Microsoft Office, sous la forme de macro commandes. Ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté. Les virus macros non supprimés se répandent très rapidement. L'ouverture d'un document infecté va contaminer le document par défaut de l'application, puis tous les documents qui seront ouverts au sein de l'application. Les documents Word, Excel et PowerPoint sont en général les documents les plus partagés, et envoyés par Internet, ceci explique la diffusion rapide de ces virus.
- Les virus Win32 : Il s'agit d'un virus exécutable au format 32 bits de Windows. Ce type de virus est le plus dangereux car ils peuvent prendre le contrôle de l'ordinateur.
- Les VBS : Les parasites écrits en Visual Basic Script parviennent à se reproduire en se recopiant dans les répertoires de démarrage automatique, en modifiant la base de registre ou en se propageant par e-mails.

1.2.1. Les principaux types de virus.

- Les virus. Le **virus** est un code reproducteur. Il s'agit d'un programme capable d'infecter des fichiers, des disques durs, disquettes, ... en y greffant une copie fonctionnelle de lui-même.
- Les Vers : Le **ver** un programme indépendant, qui se copie d'ordinateur en ordinateur. Un virus qui est capable de se propager à travers des réseaux informatiques est appelé "ver", en particulier lorsqu'il se compose de plusieurs segments dispersés à travers le réseau. La différence, entre un ver et un virus, est que, **le ver ne peut pas se greffer à un autre programme** et donc l'infecter, il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de répliation peut donc non seulement infecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, ce ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.
- Les Chevaux de Troie : Un **cheval de Troie** est un virus qui est présenté comme un programme utile. En cours d'exécution, ce type de virus met en œuvre des actions destructrices à l'encontre du système, alors qu'il semble accomplir une tâche simple. Il s'agit d'un programme exécutable indépendant non reproductif. Lorsque le programme est lancé, il peut, par exemple, formater le disque dur, voler les mots de passe ou encore envoyer des informations confidentielles à son créateur via Internet.

1.2.2. Exemples de virus.

- Les virus de fichiers : Ces virus infectent les applications. Ils s'exécutent puis se répandent en infectant les documents associés ainsi que les autres applications à chaque fois qu'ils sont sollicités.
- Les virus résidents : il s'agit d'un virus actif dans la mémoire de l'ordinateur, qui prend place dans la mémoire vive et gère l'exécution des programmes de manière à poursuivre la contamination de la machine.
- Les virus furtifs : Ce type de virus (du MBR Master Boot Record ou non), enregistre des informations qui sont «servies» à la demande et qui font que le virus passe inaperçu. La plupart de ces virus copie le véritable MBR à un autre endroit du disque, empêchant ainsi leur détection, lorsque des processus le demande.

- Les virus polymorphes : Le virus polymorphe est un virus dont le programme change à chaque reproduction, mais l'action pour lequel il a été créé est toujours la même. Par exemple, le virus peut intervertir l'ordre des instructions de son action en son sein, ou rajouter de fausses instructions, afin de tromper la vigilance de l'antivirus, qui lui, recherche une signature précise. Beaucoup de virus polymorphes sont aussi encryptés. Le virus encryptera son code et ne le décryptera que lorsqu'il doit infecter un nouveau fichier, le rendant encore plus difficile à détecter.
- Les virus compagnons : Il s'agit d'un virus qui a la particularité d'infecter un programme, puis de créer un nouveau fichier infecté en remplacement de l'original.
- Les virus multimodes : Le virus multimodes est un virus qui a la propriété d'infecter autant de zones système que les fichiers exécutables.
- Les virus systèmes : Le virus système est un virus contaminant les fichiers système du système d'exploitation. Une fois installé, il devient un virus résident.
- Les virus de zone d'amorce : Il infecte la zone d'amorce des disques durs et des disquettes, la zone d'amorce correspond à la première partie du disque qui est lue par l'ordinateur lors de son démarrage. Pour être infecté, il faut avoir démarré sur une disquette, ou un disque amovible contenant le virus. Le virus se transmettra sur toute disquette ou support amovible inséré dans l'ordinateur. La plupart des virus de zone d'amorce est inopérante sur les systèmes d'exploitation tels que Windows technologie NT.
- Les virus multicibles : Les virus multicibles utilisent à la fois les techniques d'infection des virus programme et ceux de zone d'amorce. En doublant l'infection, ce qui double leur taille, le virus double sa chance d'être transmis à un autre ordinateur et de se répandre. Ceci explique qu'ils sont responsables d'un grand nombre d'infections, sans être très nombreux.
- Les "hoax" ou faux virus : Ces fausses alertes sont aussi sérieuses que les vrais virus. En effet, elles font perdre du temps et peuvent générer une certaine anxiété quant à la vérité ou non du message. Une des raisons pour lesquelles ces Hoax (Faux Virus) sont si répandus, c'est qu'il suffit d'avoir une certaine créativité et un talent rédactionnel, pour envoyer un e-mail contenant de fausses informations.

1.3. Ce que les virus ne peuvent pas faire.

Les virus ne peuvent pas infecter les fichiers placés sur des disques protégés en écriture. Ils n'infectent pas les fichiers compressés. Les virus ne peuvent pas s'attaquer au matériel (moniteurs, claviers, composants électroniques, etc.), car ils s'attaquent uniquement aux logiciels. Les virus ne se laissent pas forcément déceler, même s'ils ont un effet destructif.

Télécharger un fichier n'entraîne pas d'infection virale.

Il faut exécuter un programme pour contracter un virus.

Lorsque l'on télécharge un document, on peut attraper un virus en ouvrant le traitement de texte pour le lire. Toutefois, lorsque l'on télécharge un logiciel infecté, on peut déclencher la contamination lors de son installation ou de son exécution.

1.4. Comment se propagent-ils ?

Un virus peut se transmettre de plusieurs façons :

- Les virus se répandent lorsque l'on lance une application infectée ou que l'on démarre l'ordinateur depuis une disquette comportant des fichiers système infectés.
- Lorsque le virus est en mémoire vive, il infecte généralement toutes les applications que l'on exécute, y compris les applications réseau, voire dans certains cas, tous les fichiers existants sur le disque dur.

Tous les virus ne se comportent pas de la même façon :

Certains virus restent activés dans la mémoire jusqu'à ce que l'on éteigne l'ordinateur, d'autres y restent tout le temps que les applications infectées sont actives. Le fait d'éteindre l'ordinateur ou de quitter l'application infectée supprime le virus de la mémoire, mais ne le supprime pas du fichier ou du disque infecté. Si le virus réside dans un fichier système, il se réactivera lorsque l'on rallumera l'ordinateur depuis le disque en question. Si le virus s'est greffé sur une application, il se réactivera au prochain lancement de cette application.

Il suffit de copier un fichier infecté sur l'ordinateur puis activer le code du virus (en exécutant une application infectée par exemple, mais également en ouvrant une pièce jointe à un mail).

Il peut aussi détruire immédiatement tout un disque dur, ou encore s'auto-dupliquer par le système de messagerie et envoyer un message à tous les éléments du carnet d'adresse avec une copie de celui-ci en pièce jointe !

Il suffit, dans certains cas, d'ouvrir un mail pour activer le virus, puis il effectuera le travail pour lequel il a été programmé. Les mails peuvent contenir tous les types d'exécutables. Les virus utilisant le langage de programmation Microsoft VBScript (qui est un langage interprété intégré à Windows) sont très répandus.

1.5. Pourquoi des virus ?

Avec l'apparition des premiers micro-ordinateurs, sont apparus les premiers virus, et ce pour plusieurs raisons :

- **la vengeance** (salarié licencié).
- **malveillance d'un utilisateur** ou son amusement. En effet, pour certaines personnes, créer des virus est comme un jeu où il faut faire toujours mieux que le voisin, et rivaliser d'ingéniosité pour créer « LE » virus complètement invisible aux antivirus.
- **la pénétration de systèmes informatiques sécurisés**, et ce, pour avoir accès aux informations secrètes contenues dans ces systèmes. Par exemple, un utilisateur voulant obtenir le mot de passe du compte UNIX d'un autre utilisateur pour avoir accès à ses données et pouvoir les modifier par la suite, pourra créer un virus qui mettra tous les mots tapés au clavier dans un fichier, y compris les mots de passe. Il n'aura, ensuite, plus qu'à piocher dans ce fichier pour repérer le mot de passe.

Evolution du nombre de virus recensé par Dr Salomon's et Norton (éditeurs d'antivirus) entre 1989 et 2004 :

Année	Nombre de virus
1989	18
1991	409
1992	1 161
1993	2 723
1994	3 973
1995	6 006
1996	8 281
1997	11 241
1998	17 745
...	...
2004	66 308

2. Les antivirus.

2.1. Q'est ce qu'un antivirus ?

2.1.1. Définition.

Il s'agit d'un logiciel capable de détecter et de détruire les virus contenus sur un disque. Le logiciel a pour charge de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine le ou les fichiers infectés. Ils surveillent tous les espaces dans lesquels un virus peut se loger, c'est à dire la mémoire et les unités de stockage qui peuvent être locales ou réseau.

2.1.2. Fonctionnement.

Le programme est composé de 3 parties ayant chacune un rôle essentiel :

- Un " moteur " qui a pour rôle la détection des virus.
- Une base de données contenant des informations sur les virus connus. C'est cette base de données qu'il faut maintenir à jour le plus régulièrement possible, afin de permettre à l'antivirus de connaître les virus les plus récents.
- Un module de nettoyage qui a pour but de traiter le fichier infecté.

A chaque fichier testé, si le programme pense voir un virus, il regarde dans sa base de données si le virus est connu (chaque virus ainsi que ses variantes a une signature particulière, et c'est cette signature qui est comparée avec la base). Si le virus est connu, il y a de fortes chances qu'un antidote soit connu.

- Si le virus est connu, il est supprimé et le fichier est donc nettoyé.
- Si le virus n'est pas connu, le logiciel emploie une méthode heuristique (*Technique consistant à apprendre petit à petit, en tenant compte de ce que l'on a fait précédemment pour tendre vers la solution d'un problème. L'heuristique ne garantit pas du tout que l'on arrive à une solution satisfaisante. Opposé à algorithmique, l'heuristique est essentiellement utilisée dans les antivirus, pour détecter des virus en les reconnaissant selon ce qu'ils sont capables de faire plutôt que selon leur signature*) qui recherche une activité anormale ressemblant à celle d'un virus. Si tel est le cas, il met le programme infecté en quarantaine et affiche un message. Si le virus n'apparaît plus (parce qu'il est boggué et qu'il se réplique mal ou qu'il se détériore), les éditeurs d'antivirus le cataloguent comme «dormant» .

Comment détecte-t-il la présence d'un virus ?

Il existe une catégorie de détecteurs de virus qui opère sur une collection de signatures. Les virus les plus simples comportent tous une suite d'instructions caractéristiques, propre à chacun, mais parfaitement identifiable et qu'on appelle leur signature.

Un catalogue peut être établi afin d'y répertorier les nouveaux virus. Les programmes qui exploitent cette méthode s'appellent des **scanners**. Ils ne donnent que très peu de fausses alarmes, mais ils sont naturellement inefficaces pour les virus polymorphes puisque ceux-ci ont la faculté de modifier leur apparence.

L'inconvénient de cette méthode réside dans la nécessité de remise à jour périodique du catalogue. Une autre méthode existe, qui a l'avantage de ne pas nécessiter de mise à jour. Elle se fonde sur des algorithmes *heuristiques* pour détecter dans certaines successions d'instructions la possibilité d'un virus. La probabilité de fausses alarmes est plus forte qu'avec les scanners mais l'efficacité est permanente. Tout au moins jusqu'à l'apparition d'une nouvelle forme générale d'attaque.

2.1.3. Pourquoi des antivirus ?

Pour **sécuriser** les ordinateurs et **préserver** l'intégrité des données d'un ordinateur, qui peuvent être d'une importance énorme (par exemple, la base de données d'une banque ne doit sous aucun prétexte être modifiée par un virus...).

2.2. Comment se protéger ?

2.2.1. Au niveau individuel.

Les règles de base sont évidentes mais peu ou jamais appliquées :

- Utiliser un antivirus dont les définitions sont maintenues à jour.
- Ne jamais ouvrir de pièce jointe si l'expéditeur du message n'est pas connu, et si le contenu du message ne semble pas cohérent (un ami français qui vous écrit en anglais...).
- Ne pas télécharger de fichiers provenant de sites douteux.
- Ne pas récupérer tous les programmes qui courent sur disquettes, CD-ROM ou toute source de données dont la provenance est inconnue.
- Ne pas surfer sur le *web* et surtout sur les sites douteux.
- Dans le BIOS des machines, supprimer les possibilités de boot sur les médias amovibles.
- Dans les applications Office, forcer la demande d'autorisation d'exécution des macros.

2.2.2. Au niveau d'une entreprise.

- Regrouper les points de liaison entre l'Intranet et l'Internet en un seul point équipé d'un *proxy* avec des règles de filtrage adaptées (interdire l'accès à certains sites Web en fonction de critères draconiens tels que mots-clés, *URL* connues, ..., afin de se prémunir de l'accès aux sites sensibles)
- Mettre un *Firewall* entre l'Intranet et Internet afin de fermer les ports d'entrées/sorties inutilisés (pour se prémunir contre l'action des troyens)
- Maintenir une stratégie rigoureuse concernant l'utilisation de l'antivirus ainsi que ses mises à jour.
- Utiliser un antivirus permettant de traiter les mails avant leur distribution aux destinataires.
- Sensibiliser et informer les utilisateurs sur les règles de sécurité de base.

Il existe 2 types de protection :

- Temps réel : à chaque mouvement de fichier (lecture/écriture sur disque ou tout média de stockage), il y a vérification de la présence de virus.
- Par scan (parcours) des médias à la recherche d'un virus dans tous les fichiers.

2.2.3. Quelques règles à suivre.

La plupart des virus, sont relativement inoffensifs ; ils peuvent soutirer une petite quantité de mémoire, mais ils ne détruiront probablement pas tous les fichiers du disque dur.

Pour se protéger des virus, il faut :

- **Se procurer un logiciel antivirus** : Le logiciel antivirus parfait n'existe pas. Pour autant, aucun ordinateur ne devrait être sans logiciel antivirus. S'il s'agit d'un scanner, il faut le mettre à jour fréquemment, car de nouveaux virus apparaissent tous les jours.
- **Inspecter tous les disques** : En général, on devrait être très prudent avant d'insérer une disquette provenant de sources inconnues, surtout si la disquette a été partagée entre plusieurs personnes. Il faut inspecter tous les fichiers avec le logiciel antivirus. Il en va de même, pour les logiciels achetés et emballés. Lorsque l'on remet une disquette à quelqu'un d'autre, il faut la protéger en écriture. De cette manière, le virus situé sur l'ordinateur de l'autre personne ne contaminera pas votre disquette. Les CD-ROM sont moins risqués, mais mieux vaut les inspecter la première fois qu'on les utilise.

- **Télécharger de façon prudente** : Plusieurs utilisateurs d'ordinateur croient que la plus importante source de contamination provient du téléchargement de fichiers. Rien n'est plus loin de la vérité : la vaste majorité des virus voyage par l'entremise des disquettes partagées ou les fichiers d'un réseau. Par prudence, mieux vaut télécharger tous les fichiers dans un répertoire spécial sur le disque dur,
- **Inspecter les documents annexés aux courriers électroniques avant de les lire** : Alors qu'il est impossible de contracter un virus simplement en lisant un message, c'est possible par l'entremise d'un fichier attaché au message. Certains logiciels de courrier électronique vont ouvrir automatiquement certains documents annexés en utilisant l'application appropriée. C'est bien et cela rend la lecture des documents annexés plus efficace, mais peut devenir une source potentielle de cauchemars si des virus s'y cachent. Désactivez cette fonction de votre logiciel de courrier électronique, et inspectez chaque document annexé que vous recevez avant de les consulter.
- **Sauvegarder les fichiers partagés en format RTF** : Si on désire partager des données sur un serveur réseau, et que l'on souhaite conserver notre environnement à l'abri des virus, il faut sauvegarder tous les fichiers aux formats RTF et ASCII. Aucun de ces formats ne conserve macro commandes ni informations de styles, ce qui permettra donc d'être protégé contre les macros virus.
- **Faire une copie de sécurité complète** : Faire des copies de sécurité des documents de travail et des fichiers de configuration du système régulièrement. Mieux vaut les conserver ailleurs que sur le disque dur.

2.3. Comment savoir si son PC a "attrapé" des virus ?

Plusieurs symptômes peuvent révéler qu'un fichier a été infecté :

- changement de taille,
- de date de création,
- de somme logique de contrôle (checksum).
- un simple ralentissement de la machine,
- un comportement anormal,

La taille mémoire disponible pourra se révéler réduite par rapport à ce que l'on a tendance à observer (639 Ko au lieu de 640).

Les symptômes peuvent être par exemple :

- *un message d'erreur* indiquant qu'un périphérique n'a pas été reconnu,
- la disparition de données jusque-là accessibles,
- des bruits inhabituels ou un dysfonctionnement du disque dur.

2.4. Aspects techniques des antivirus.

2.4.1. Principales techniques de recherche de virus.

Les quatre techniques, principalement utilisées par les antivirus pour localiser les virus :

- **du scanning** : le scanneur recherche dans tous les fichiers, ou, en RAM, un code spécifique qui est censé indiquer la présence d'un virus,
- **du moniteur de comportement** : surveille les actions habituellement menées par les virus,
- **du contrôleur d'intégrité** : signalent les changements intervenus dans les fichiers,
- **la recherche heuristique** : recherche des instructions généralement utilisées par les virus.

Recherche de la signature (scanning) :

Il s'agit de la méthode la plus ancienne et la plus utilisée.

Son avantage est de permettre la détection des virus avant leur exécution en mémoire.

Son principe consiste à rechercher sur le disque dur toute chaîne de caractères identifiée comme appartenant à un virus.

Cependant, comme chaque virus a sa propre signature, il faut, pour le détecter avec un scanneur, que le concepteur de l'antivirus ait déjà été confronté au virus en question et l'ait intégré à une base de données. Un scanneur n'est donc pas en mesure de détecter les nouveaux virus ou les virus dits polymorphes (car ils changent de signature à chaque répliation); toutefois, une mise à jour régulière de la base de donnée est recommandée.

Utilisation d'un contrôleur d'intégrité des fichiers :

Un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque dur auxquels sont associés quelques caractéristiques.

Ces dernières peuvent prendre en compte :

- la taille,
- la date,
- l'heure de la dernière modification ou encore un checksum (somme de contrôle).

Un CRC (Code de Redondance Cyclique), ou un algorithme de checksum avec un système de chiffrement propriétaire, pourra détecter toute modification ou altération des fichiers en recalculant le checksum à chaque démarrage de l'ordinateur (si l'antivirus n'est pas résident), ou dès qu'un fichier exécutable est ouvert par un programme (si l'antivirus est résident) ; en effet, si le checksum d'un programme avant et après son exécution est différent, c'est qu'un virus a modifié le fichier en question, l'utilisateur en est donc informé.

D'autre part, l'antivirus peut aussi stocker la date et la taille de chaque fichier exécutable dans une base de données, et ainsi, tester les modifications éventuelles au cours du temps. Il est en effet rare de modifier la taille ou la date d'un fichier exécutable. La parade pour les virus est de sauvegarder la date du fichier avant la modification et de la rétablir après.

Moniteur de comportement :

Les moniteurs de comportement ont pour rôle d'observer l'ordinateur à la recherche de toute activité de type viral, et dans ce cas, de prévenir l'utilisateur. Un moniteur de comportement est un programme résident que l'utilisateur charge à partir du fichier **AUTOEXEC.BAT** et qui reste actif en arrière plan, surveillant tout comportement inhabituel.

Les différentes manifestations d'un virus pouvant être détectées sont :

- Les tentatives d'ouverture en lecture/écriture des fichiers exécutables.
- Les tentatives d'écriture sur les secteurs de partition et de démarrage.
- Les tentatives pour devenir résident.

Pour repérer ces tentatives, les antivirus détournent les principales interruptions de l'ordinateur et les remplacent par l'adresse de leur code.

Dès qu'un virus tente d'écrire sur le secteur de Boot, c'est l'antivirus qui est d'abord appelé, qui peut ainsi prévenir l'utilisateur qu'un virus tente de modifier le secteur de Boot.

L'antivirus peut alors éliminer le virus de la mémoire, enregistrer une partie de son code dans la base de donnée et lancer un scanning pour repérer la/les souche(s) sur le disque dur et les détruire.

Démarche heuristique :

L'analyse heuristique concerne la recherche de code correspondant à des fonctions virales. Elle est différente, dans son principe, d'un moniteur de comportement qui surveille des programmes ayant une action de type viral.

L'analyse heuristique est comme le scanning, passive. Elle considère le code comme une simple donnée, et n'autorise jamais son exécution.

Un analyseur heuristique va donc rechercher le code dont l'action est suspecte, s'il vient à être exécuté. L'analyse heuristique permet par exemple, pour les virus Polymorphes, de chercher une routine de déchiffrement. En effet, une routine de déchiffrement consiste à parcourir le code pour ensuite le modifier. Ainsi, lors de l'analyse heuristique, l'antivirus essaie de rechercher non pas des séquences fixes d'instructions spécifiques au virus, mais un type d'instruction présent sous quelque forme que ce soit.

Cette méthode vise à analyser les fonctions et instructions les plus souvent présentes et que l'on retrouve dans la majorité des virus. Elle permet ainsi, contrairement au scanning, de détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

Analyse spectrale :

Tout code généré automatiquement est supposé contenir des signes révélateurs du compilateur utilisé. Il est impossible de retrouver dans un vrai programme exécutable compilé, certaines séquences de code. C'est grâce à ce principe qu'entre en jeu l'analyse spectrale. Cette analyse vise à repérer les virus polymorphes qui sont indétectables autrement (leur signature changeant à chaque répllication). En effet, lorsqu'un virus polymorphe crypte son code, la séquence qui en résulte contient certaines associations d'instructions que l'on ne trouve pas en temps normal; c'est ce que détecte l'analyse spectrale.

2.4.2. Principales techniques d'éradication de virus.

Une fois un virus détecté, que ce soit en mémoire ou sur le disque dur, il reste à le supprimer.

Une fonction primordiale des antivirus est donc la suppression des virus. Leur but est de débarrasser l'utilisateur de ce programme malveillant. Mais il n'est pas si simple que l'on croit de les éradiquer et de récupérer le programme original.

En effet, cela est impossible dans le cas de virus avec recouvrement : ils détruisent une partie du programme sain lors de sa duplication. La seule solution est la destruction des fichiers infectés ou carrément le formatage du disque dur.

Pour les autres, même si ce n'est pas irréalisable, la tâche est cependant très ardue : il faut savoir très précisément où est localisé, dans le fichier, le virus en question, sachant qu'il peut être composé de plusieurs parties, ensuite il faut le supprimer, et enfin aller chercher la partie du programme dont le virus avait pris la place et la restaurer.

Toutes ces manipulations nécessitent une connaissance parfaite du virus et de son mode d'action. Cette éradication se faisant par une recherche (du virus, de la partie déplacée), toutes les caractéristiques des différents virus doivent être répertoriées dans une base de donnée mise à jour pratiquement quotidiennement.

2.5. Efficacité des antivirus.

Contre les vieux virus, les antivirus sont généralement efficaces à 100%.

C'est dans la détection de virus nouveaux que l'on peut voir les capacités des différents antivirus.

Produit	Editeur	Detéction Virus standart	Det. Macro Virus	Det. Virus Poly-morphes	Det. Virus Inconnus	Fausse alertes	Prix
AntiViral ToolKit Pro	Eugene Kaspery/ASD	98.41%	95.74%	45.54%	58.33%	0.50%	1100 F
Dr Salomon's Antivirus Toolkit 7.71	Dr Salomon/AB Soft	94.78%	93.62%	36.61%	41.67%	0.10%	1030 F
F-Prot Professionnal pour Win 95	Frisk/ Informatique developpement	94.9%	91.49%	40.18%	33.33%	0.00%	1690 F
IBM Antivirus V2.5.2	IBM	88.99%	82.98%	39.29%	33.33%	0.00%	340 F
VirusScan pour win 95 3.0.2	McAfee	97.35%	91.49%	61.61%	41.67%	0.00%	300 F
Norton Antivirus pour Win95	Symantec	91.67%	78.72%	33.93%	0.00%	0.00%	600 F
Panda Antivirus Pro for Win95 v5.0	Panda Software	93.14%	61.70%	66.07%	8.33%	0.00%	700 F
ThunderByte Anti-Virus pour Win95 v8.02	Delta Logic	96.16%	91.49%	57.14%	91.67%	3.00%	700 F
EliaShim's ViruSafe	EliaShim/CTI	83.86%	89.36%	18.75%	25.00%	0.00%	520 F
Avast32 pour Win	Calyx Data Control	97.26%	91.49%	60.71%	25.00%	0.00%	880 F
Vcontrol 45	Amplitude	84.27%	91.49%	58.04%	25.00%	0.00%	1200 F

Comparatifs d'antivirus : INFO PC n°175

3. Quelques virus.

Virus Macro : Melissa (Word)
Attach (PowerPoint)
Detox (Access)

Ver : I love you
KAK (Kakou anti-Kro\$oft)
BubbleBoy

Virus 32 bits : Happy New Year
ExploreZip

Parasite hybride : Nimda, Code Red
Virus Goner
Virus Sircam
Virus GodMessage

Virus macro : Attach, Detox, Unstable

Cheval de Troie : Qaz
Back Orifice

Virus Tequila : ce virus infectera dans un premier temps la zone d'amorce de l'ordinateur. La prochaine fois que vous allumerez votre ordinateur, ce virus Tequila infectera donc tous les programmes que vous utilisez ou qui sont lancés au démarrage de votre machine et, ainsi de suite, tout programme exécuté sera donc infecté.

Virus Klez : frappe tous les 6 de chaque mois. Il modifie et efface les fichiers de type image, MP3 ou codes HTML.

4. Quelques adresses.

VirusScan (95/98) à l'adresse : <http://www.mcafee.com> : le seul à effectuer une décontamination en ligne.

Norton antivirus (95/98/NT) à l'adresse : <http://www.symantec.com/avcenter/index.html>.

VirusSafe à l'adresse : <http://www.eliashim.com>.

Thunderbyte Anti-Virus : <http://thunderbyte.com>.

AVP : <http://www.avp.com>.

5. Bibliographie.

Revues :

- **Info PC n° 175** *Novembre 2000*:
Protéger vos données.
Comparatif de 5 antivirus.
- **Décision Micro & Réseaux n° 478** *Septembre 2001*:
Nimda contamine Internet.
Des risques d'intrusion accrus.
- **Décision Micro & Réseaux n° 499** *Mars 2002*:
Le point sur ...Les virus.
- **Décision Micro & Réseaux n° 510** *Mai 2002*:
Antivirus génériques : peu répandus mais appréciés.
- **Décision Micro & Réseaux n° 511** *Juin 2002*:
Les PME sous-estiment le risque informatique.
- **Décision Micro & Réseaux n° 512** *Juin 2002*:
Antivirus.
- **PC Expert n° 109** *Juin 2001*:
Dans le domaine de la sécurité informatique, I love you se décline...
- **Windows News n°100** *Juin 2002*:
Comparatif logiciel : Antivirus 2002 : une protection imparfaite.
- **Windows News n°105** *Décembre 2002*:
9 étapes pour un PC sécurisé : se préserver des menaces de l'e-mail.
Au cœur des programmes antivirus.

Internet :

- www.coupepouce.com/dossiers/virus/virus.htm.
- www.autourdupc.com.

Livres :

- **Editions Atlas** fiche "**Attention aux virus**".
- **Savoir tout faire à l'ordinateur.**
Un PC bien ordonné : Les virus informatique.
Description : La sécurité sur Internet.
Solutions logicielles : Les logiciels antivirus.
- **Le Grand Dictionnaire Marabout de la Micro-Informatique et de l'Internet**
Définitions :
Virus (compagnon, furtif, multimode, polymorphe, résidant, système).
Ver.
Cheval de Troie.