# NOTIONS D'INTERNET ET DE PROTOCOLE

# I - Présentation d'Internet

## 1.1 - Qu'est-ce que Internet ?

L'Internet se définie comme étant la fédération d'une multitude de réseaux interconnectés les uns aux autres à travers le monde par des artères de télécommunications de nature très diverses : liaisons spécialisées, réseaux câblés, satellites, wifi, etc.

## 1.2 - L'historique d'Internet

Internet est issu du réseau ARPAnet (Advanced Research Projects Agency), créé en 1968 par le département américain de la Défense, dans un but stratégique, pour relier ses centres de recherche.

Le réseau initial ne permettait que l'envoi de courrier électronique. Mis dans le domaine public (libre d'utilisation), il fut repris par les universitaires en 1979 (La Duke University à Durham Caroline du Nord), qui y virent le moyen d'échanger des informations.

Après les militaires et les universitaires (La National Science Foundation finance leurs mises en réseau), Internet devient aux Etats-Unis l'affaire des grandes entreprises privées, des P.M.E. et des particuliers.

En 1983, c'est au tour de l'Europe (par le biais en France du C.N.A.M. Conservatoire national des arts et métiers) et du reste du monde de se connecter à ce réseau de réseaux.

L'outil qui rendit populaire l'Internet à partir de 1993 est le WWW, le World Wide Web en un mot le Web. Le mot Web désigne la toile d'araignée et World Wide Web désigne donc la toile d'araignée couvrant le monde entier.

Le premier navigateur WEB graphique a été mis aux points au CERN (centre européen de recherche nucléaire) en 1993.

Un navigateur Web permet de se connecter à une multitude de sites diffusant des informations sans connaissances des règles de communication propre au réseau.

L'Internet reliait en 1995 plus de 2 millions d'ordinateurs et plus de 30 millions d'utilisateurs dans 146 pays.

## 1.3 - Les services offerts

Internet permet d'accéder à différents types de services dont :

- **Le courrier électronique**

Le courrier électronique ou messagerie électronique est la transmission de fichiers informatiques entre deux ordinateurs par les réseaux (liaisons spécialisées ou hertzienne). Il permet aussi d'envoyer et de recevoir des messages de pratiquement tous les correspondants qui disposent d'un ordinateur et d'une connexion à Internet. Si le correspondant n'est pas relié au réseau mais possède un abonnement auprès d'un Fournisseur d'Accès à Internet (FAI), par exemple : **AVISO,** c'est à lui que le message sera envoyé.

- **La consultation Web**

Depuis sa création en 1989, il a complètement échappé à ses concepteurs et à la communauté scientifique pour devenir le Système d'Information le plus utilisé sur Internet, avec plusieurs milliers de serveurs à travers le monde.

Les pages mises à la disposition des utilisateurs sont des documents qui peuvent contenir des textes, des sons, des images ou des séquences vidéo.

# II - Présentation de protocoles usuels

## 2.1 - La définition de protocole

Un protocole est un ensemble de règles et de conventions régissant la façon de transférer des informations. Le protocole fondamental qui nous permet de nous connecter à Internet porte le nom de TCP/IP (Transmission Control Protocol/Internet Protocol).

## 2.2 - Le protocole TCP/IP

Internet est constitué d'un ensemble de liaisons (liaisons spécialisées, fibres optiques ou liaisons satellite), de nœuds et de réseaux (réseaux téléphoniques, réseaux spécialises) qui constituent un maillage mondial par lequel, transitent les communications entre des points terminaux.

Les différents réseaux qui constituent Internet peuvent communiquer entre eux, parce qu'ils parlent le même langage. Le TCP/ IP représente la norme standard en matière de protocoles de communication.

### *2.2.1- Le protocole TCP*

Tous les réseaux sont des réseaux à commutation de paquets. Le protocole TCP est un service de livraison fiable, orienté connexion.

Il assure deux fonctions :

☞ la décomposition des informations en datagrammes.

Lorsqu'une session est établie entre deux points, le message numérisé à transférer est découpé en paquets, en datagrammes, avant d'être envoyé sur Internet ; chaque paquet y transite de façon autonome et porte l'adresse format IP du destinataire.

☞ la recomposition des datagrammes en informations.

Ainsi, deux paquets successifs peuvent emprunter deux chemins différents, selon la variation de l'état du trafic et des liaisons (rupture ou saturation d'une liaison).

Le message est reconstitué par le nœud desservant le destinataire à partir du réassemblage des datagrammes reçus, grâce au numéro d'ordre qui ont été insérés au moment décomposition.

### *2.2.2- Le protocole IP*

Le protocole IP a été mis au point pour offrir aux ordinateurs le service de routage et le transport des données à travers les différents réseaux qui constituent Internet.

Il se charge de véhiculer les datagrammes jusqu'au destinataire et assure que les paquets envoyés sont reçus à la bonne adresse. Autrement dit, la circulation des datagrammes à l'intérieur d'un réseau n'incombe pas au protocole IP, mais à celui du réseau en question, IP n'étant chargé que d'assurer le passage d'un réseau à un autre.

Pour passer d'un réseau à un autre, on utilise un matériel dédié : le routeur.
Celui-ci s'appuie sur une table de routage pour aiguiller un datagramme vers un réseau qui le rapproche de sa destination finale.

## 2.2 - Les protocoles HTTP et FTP

### *2.3.1- Le protocole HTTP (HyperText Transfert Protocol)*

Les pages HTML sont stockées sur des serveurs web. Le protocole http permet la communication de documents hypermédias entre un serveur Web et un poste client, par l'intermédiaire du logiciel de navigation du poste client.

Une fois le transfert effectué, le logiciel de navigation du poste client n'a plus qu'à interpréter le document. Si le document contient des images, du son et d'autres données que le logiciel de navigation ne peut pas interpréter directement, le poste client passe la main à un programme externe, situé sur la machine du serveur web, lui permettant de lire ce type de données ?

Ainsi, grâce au protocole http, les serveurs web et les postes clients peuvent être des machines totalement hétérogènes. Le web est donc une toile mondiale de serveurs http reliés les uns aux autres par des liens physiques, les réseaux matériels, et des liens logiques, les liens hypertextes. Ces liens hypertextes permettent de voyager d'un site à l'autre sur le réseau Internet par l'intermédiaire d'un navigateur.

### *2.3.2- Le Protocole FTP (File Transfert Protocol)*

Le service permettant le téléchargement de programmes et plus généralement de fichiers s'appelle **FTP**, sigle de **File Transfert Protocol.** C'est l'un des premiers outils à avoir été mis à la disposition des utilisateurs d'Internet. Ce service sert, en effet, à transférer des fichiers d'un ordinateur à l'autre, en appliquant des protocoles qui lui sont propres. Le **Protocol FTP** fonctionne sur le modèle client /serveur.

Des milliers de serveurs sont répartis sur Internet et fournissent des fichiers aux utilisateurs. L'utilisateur (le client) se connecte à un serveur **FTP** et peut y déplacer ou y prélever un fichier via **FTP**. On parle, alors, de sites **FTP.** Pour se connecter à un serveur **FTP**, il est nécessaire d'y posséder un compte avec un mot de passe. Nombre de ces sites sont connus sous le nom de sites **FTP** anonymes (anonymous FTP sites).

# VIRUS INFORMATIQUES DANS UN RESEAU

# I - Virus informatiques

## 1.1 – La définition

Un virus est un morceau de programme informatique malicieux conçu et écrit pour qu'il se reproduise. Cette capacité à se répliquer peut toucher un ordinateur, sans permission et sans que l'utilisateur ne sache.

En termes plus techniques, le virus classique s'attachera à un des programmes exécutables et se copiera systématiquement sur tout autre exécutable que l'utilisateur lancera. Il n'y a pas de génération spontanée de virus informatiques. Ils doivent avoir été écrits dans un but spécifique. A part se répliquer, le virus peut avoir ou non une action plus ou moins néfaste, allant de l'affichage d'un simple message à la destruction de toutes les données.

## 1.2 – L'historique

En janvier 1986, fut créé BRAIN, le premier virus informatique. Il s'attaquait au secteur de boot des ordinateurs et se propageait par disquette.

BRAIN était un virus relativement inoffensif de la famille des virus d'amorçage. Ces virus s'exécutent lorsqu'une disquette est présente dans le lecteur au démarrage de l'ordinateur. Une fois exécuté, BRAIN s'implante dans le secteur de boot de l'ordinateur – la première zone disque lue par l'ordinateur – et s'exécute à chaque démarrage de la machine.

La méthode de propagation utilisée par BRAIN ne lui a pas permis de se propager à grande échelle. Il fallait des mois, parfois même des années, pour infecter un nombre significatif de machines et semer véritablement le trouble. En 1986, aucun moyen de propagation rapide à grande échelle n'était offert aux concepteurs de virus.

Les virus s'attaquant aux secteurs de boot, des ordinateurs furent très actifs pendant presque dix ans pour totalement disparaître vers 1995. C'est à cette époque que les systèmes d'exploitation Windows et les logiciels de bureautique se sont multipliés, apportant avec eux de nouvelles fonctionnalités qui furent aussitôt détournées pour relancer la propagation des virus.

Dans un premier temps, des études ont été menées dans le cadre d'analyses et de conception de programmes informatiques dotés d'une possibilité d'autoréplication ont été réalisés. Ces études n'ont pas abouti à des cas concrets, à l'exception d'une expérimentation en 1981 d'un programme sur Apple-II qui parvenait à transmettre des copies de son code.

Puisque ces premiers tests sont restés dans le cadre d'un laboratoire et n'ont pas été diffusés dans la nature, on ne les considère par comme les premiers virus en tant que tel.

## 1.3 – Les différents types de virus

On peut classer les virus selon leur mode de déclenchement ou leur mode de propagation. On distingue alors plusieurs catégories de virus :

### 1.3.1- Le cheval de Troie

Un Cheval de Troie est un programme simulant de faire quelque chose, mais faisant tout autre chose à la place. Leur nom vient du fameux Cheval de Troie de la Grèce antique, offert en cadeau, mais qui en fait avait pour but de causer la ruine et la destruction de la ville ayant reçu ce cheval en bois. Un Cheval de Troie sur un ordinateur est un programme exécutable indépendant, qui est présenté comme ayant une action précise. Néanmoins, lorsque ce programme est lancé, il va, par exemple, formater le disque dur, voler les mots de passe ou envoyer des informations confidentielles au créateur via Internet.

### 1.3.2- Les virus Macro

Les virus Macro sont la plus grande menace à ce jour. Ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté. Un virus Macro est une série de commandes permettant d'effectuer un certain nombre de tâches automatiquement au sein des applications ci dessus. Le but non nuisible du langage de macro dans ces applications est à l'origine de pouvoir créer des raccourcis pour effectuer des tâches courantes, par exemple, en une touche, imprimer un document, le sauvegarder et fermer l'application.

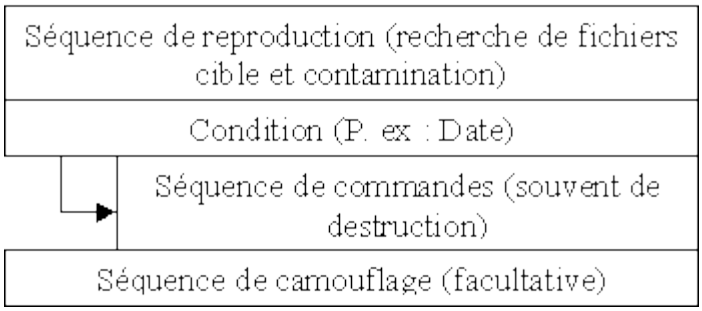
Les Virus Macro non supprimés se répandent très rapidement. L'ouverture d'un document infecté va contaminer le document par défaut de l'application, et ensuite, tous les documents qui seront ouverts au sein de l'application. Les documents Word, Excel et PowerPoint étant les documents les plus souvent partagés, envoyés par Internet, ceci explique la diffusion rapide de ces virus. De plus, le langage de programmation des Macros est beaucoup plus facile à apprendre et moins compliqué qu'un langage de programmation classique.

### 1.3.3- 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 véracité ou non du message. Une des raisons pour lesquels ces Hoax sont si répandus, c'est qu'il suffit d'avoir une certaine créativité et un talent rédactionnel, pour envoyer un email contenant de fausses informations. Le premier de ces Hoax connu a été envoyé par deux abonnés à AOL en 1992, il s'appelle **Good Times**.

Depuis les messages du type "si vous recevez un email avec comme sujet bonjour, effacez le, ne l'ouvrez pas, il détruira votre ordinateur", sont presque aussi répandus que les vrais virus. Nous pouvons facilement développer des armes pour lutter contre les vrais virus, il est plus difficile de concevoir quelque chose pour lutter contre la désinformation. Le seul moyen c'est l'éducation des utilisateurs de micro ordinateurs.

**Schéma type de virus :**




# II - Pourquoi crée t-on les virus ?

## 2.1 – Les avantages

Certains ont fait observer, il y a quelques années, que ceux à qui l'existence des virus profite le plus sont les concepteurs de logiciels antivirus. Cette remarque a été à la base de théories sur la création intentionnelle de virus à des fins commerciales. Rien ne permet d'accréditer cette hypothèse qui semble être du domaine de la rumeur non fondée, voire malveillante. D'autres interrogations (très probablement non motivées) sur l'intervention de services secrets avaient été suscitées jadis par l'abondance des virus d'origine bulgare.

### 2.2 – Les inconvénients

Les virus informatiques ralentissent l'ordinateur (PC), font perdre des informations, le plantent jusqu'à destruction de certains composants électroniques (hardware).

### 2.3 – La propagation des virus

Les virus ne peuvent entrer en action (pour se reproduire et pour provoquer des dommages) qu'à l'occasion de l'exécution d'un programme infecté. Son vecteur de propagation est donc toujours un programme (ou un document bureautique contenant un macro virus), et jamais un fichier de données passives.

Ainsi, un virus ne peut se propager au travers du texte d'un e-mail, mais bien dans un fichier exécutable annexé, et il s'activera uniquement si l'on commet l'imprudence d'ouvrir le fichier annexé.

Le caractère "programme exécutable" d'un fichier n'est malheureusement pas toujours évident à cerner : si, par exemple, les suffixes .exe, .com, .vbs, .pif dans les noms de fichier sur l'ordinateur correspondent toujours à du "code" exécutable, des programmes se dissimulent parfois derrière des noms de fichiers anodins (de type image par exemple), en mettant à profit certaines faiblesses de paramétrage du PC ou du logiciel de courrier.

S'il en est devenu le plus significatif, le mail n'est évidemment pas le seul mode de transport des virus : tout mode d'échange de fichier (disquette, cd, partage de fichiers en réseau, transfert de fichiers par le réseau, utilisation des "News" sur Internet, programmes de "chat" tels que irc ou icq, ...) peut offrir un cadre de propagation des virus.

## III - Actions des virus et les conséquences de ceux-ci

### 3.1 – Les actions des virus sur Internet

Bien qu'Internet existe depuis environ 20 ans, ce n'est que depuis la fin des années 1980 que l'on parle de diffusion des virus par le biais du réseau. Un incident a alors fait prendre conscience aux utilisateurs qu'ils étaient vulnérables à ce type d'invasion.

Les ordinateurs impliqués appartenaient à des agences fédérales, des universités, des laboratoires de recherche et des corporations qui envoyaient et recevaient des programmes, des données et du courrier électronique. Le 2 novembre 1988, un ver informatique a été introduit dans le réseau et s'est reproduit de façon incontrôlée pendant plusieurs jours.

Plus de 6 200 ordinateurs américains ont été infectés à un point tel que plusieurs systèmes se sont écroulés. En peu de temps, la nouvelle s'est répandue et plusieurs utilisateurs d'ordinateurs qui n'avaient pas encore été infectés se sont débranchés d'Internet afin d'éviter le fléau. Les coûts directs impliqués par l'intrusion de ce ver informatique dans le réseau sont évalués à près de cent millions (100 000 000) de dollars.

Cependant, les coûts réels ont été bien plus lourds et sont difficilement quantifiables. La perte de confiance dans Internet et la peur qu'ont ressentie les utilisateurs vis-à-vis de l'échange de données informatiques par le biais du réseau ont causé beaucoup de tort à celui-ci et ont retardé son expansion.

Cet événement plutôt spectaculaire qui a éveillé les consciences des utilisateurs du réseau a été suivi de plusieurs autres dont on n'a pas toujours entendu parler mais qui n'en ont pas été moins importants. La méfiance et la peur des internautes sont donc compréhensibles de même que leur besoin de s'informer des moyens possibles pour se préserver d'un danger qui peu prendre de multiples formes et agir sur plus d'un plan.

D’une manière générale, il est à constater que les virus, en fonction de leurs natures et caractéristiques, s’attaquent à l’un ou plusieurs aspects principaux de la sécurité à savoir :

- la confidentialité;
- l’intégrité ;
- la continuité de service.

Certains virus exercent une action nuisible directe : modification ou destruction de certains fichier, effacement du disque dur, reformatage du disque dur, modification ou destruction de certains fichiers vitaux du disque dur...

D’autres virus n’ont pas pour but de détruire spécifiquement des données mais sont néanmoins tout aussi menaçant. En effet, ces virus colonisent l’espace du disque dur et de la mémoire vive, allongent les temps de traitement et provoquent une forte régression des performances du système.

Les virus considérés comme bénins ont pour seul objectif de gêner les activités de l'utilisateur et entraînent des manifestations visuelles ou sonores plus ou moins problématiques : bruits parasites, lettres qui dégoulinent, disparition progressive du contenu de l'écran. A noter que ce type de virus n'entraîne aucun dommage.

L'action des virus peut être permanente, sporadique ou périodique. De même, une action peut n'avoir lieu qu'à une date précise (le virus Michel Angelo, par exemple, ne frappe que le 6 mars, date anniversaire du grand peintre Michel-Ange : ce virus provoque, entre autre, une perte du contenu du disque dur).

L'action du virus peut également être déclenchée par un événement extérieur (par exemple, si le nom de son initiateur est éliminé des listes de paie).

Encore plus dangereux et pernicieux, sont les virus qui ont pour mission de se disséminer afin de propager des « vulnérabilités » cachées et de « marquer » les systèmes atteints pour que ces systèmes soient détectables par un balayage sur internet.

Par conséquent, ces virus doivent demeurer le plus silencieux possible et éviter d'être détecté par l'utilisateur. Aussi, ces virus ne perturbent nullement le fonctionnement normal du système infecté et contaminé. Paradoxalement, les virus le plus dangereux pour la sécurité du système, sont ceux qui engendrent le moins de gêne possible.

Les virus de cette famille demeurent cachés jusqu'à jour où suite à un stimuli extérieur (par exemple une instruction envoyée par Internet), ils se déclarent et causent des dommages irréversibles (le virus Michel Angelo ressemble à ce type de virus sauf que le déclenchement est provoqué par la date de l'ordinateur). Cette famille de virus est, par excellence, une « arme stratégique » utilisée par les services de renseignements en vue d'être déclenchés lors d'un conflit, et de paralyser les systèmes d'information de l'adversaire.

## 3.2 – Les types de cibles

Le premier objectif est la contamination de une ou plusieurs cibles qui lui permettront d'être relancé le plus souvent possible. Une cible est appelée vecteur de contamination.

Les cibles des virus se présentent comme suit :

- les fichiers exécutables, surtout les .COM (avec le très célèbre COMMAND.COM qui est lancé à chaque démarrage du système);
- les fichiers systèmes, particulièrement les IO.SYS et MSDOS.SYS (qui sont lancés au démarrage du système aussi);

- les fichiers temporaires de recouvrement .OVL. ;
- les fichiers binaires .BIN. ;
- les fichiers pilotes .DRV. ;
- le secteur de la table de partition du disque dur (lu par le BIOS à chaque initialisation) ou d'une disquette BOOT.

En principe, il existe 3 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 programmé.

## 3.3 – Les conséquences de propagation des virus

### 3.3.1 - Conséquences informatiques

Les conséquences d'un virus ne sont pas toujours aussi graves qu'elles en ont l'air. En effet, bien qu'un virus est un programme qui se multiplie par définition, si un ordinateur est atteint par un virus qui ne fait que se reproduire, il n'y aura aucune autre conséquence qu'une perte de place sur le disque dur, et une faible perte de vitesse qui, si elle devient gênante, sera repérée et combattue.

Cependant, tous les virus ne sont pas aussi inoffensifs. A côté des virus bénins qui se contentent d'afficher des messages à l'écran, il existe des virus qui paralysent ou ralentissent fortement les machines, de façon à rendre la machine « cible » improductive. Ces virus sont toutefois anodins car dans la plupart des cas, il est possible de continuer son travail, plus tard, après une désinfection.

Malheureusement, il existe des virus destructeurs. Ces derniers détruisent de façon, souvent irrécupérable, des données et/ou des programmes. D'autres conséquences de ceux-ci peuvent être la destruction du matériel informatique, par exemple, le flashage du BIOS des cartes mères, c'est à dire la reprogrammation des instructions lues au démarrage de l'ordinateur avant toute utilisation de système d'exploitation modification ou de logiciel. Ce qui peut paralyser totalement l'ordinateur ou modifier un secteur du disque dur.

Il faut tout de même préciser que ces attaques contre le matériel sont assez rares et généralement les virus utilisant ces procédés bien détectés par les antivirus. De plus, pour un programmeur de virus il est beaucoup plus délicat de s'attaquer au matériel, la complexité d'un tel virus n'est vraiment pas à la portée de la grande majorité des programmeurs.

### 3.3.2 - Conséquences économiques

Les conséquences économiques sont un problème sérieux dans la société. Le budget passant dans la protection contre les virus dépasse l'imagination. En 1998, 260 millions de francs (40 millions d'euros) ont été dépensés (en France) pour l'achat d'antivirus. Mais, si le budget investi dans la protection contre les virus est si élevé c'est que la perte en cas de destruction de données serait encore plus élevée. Or, il est difficilement possible d'envisager tous les effets que pourrait engendrer une perte de données dans une société, vu la diversité des types d'entreprises.

# MISE EN ŒUVRE DE MESURES PREVENTIVES

# I – Comment se protéger contre les virus ?

## 1.1 - Les anti-virus

Un antivirus est, de par son nom, destiné à combattre les virus. Ces derniers étant toujours plus sophistiqués, les antivirus doivent s'adapter et devenir de plus en plus performant sous peine de devenir inutiles. Il est donc nécessaire de posséder un antivirus de qualité et surtout de le mettre à jour de façon très régulière.

Pour commencer, analysons le fonctionnement des antivirus. Le travail d'un antivirus se découpe en deux phases : la recherche du virus puis sa destruction.

Il existe plusieurs techniques de repérage d'un virus. La méthode la plus ancienne, et la plus utilisée, est la recherche de signature. Cette méthode est aussi nommé Scanning. Son avantage est qu'elle permet de détecter les virus avant leur exécution en mémoire. Son principe est de rechercher sur le disque dur toute chaîne de caractères identifiée comme appartenant à un virus, ce qui implique une mise à jour quasi permanente de l'antivirus afin de recenser un maximum de virus.

Une autre méthode de détection des virus par l'antivirus est de stocker dans une base de données la date de création et la taille de chaque fichier exécutable, de vérifier régulièrement les modifications éventuelles. Il est en effet rare de modifier la taille ou la date d'un fichier exécutable. Plus généralement, l'antivirus construit un fichier dans lequel il stocke de multiples données à propos des fichiers, ce qui va lui permettre de repérer d'éventuelles modifications anormales et de prévenir l'utilisateur.

Enfin, une autre manière de repérer les virus est de surveiller les instructions envoyées au processeur. En effet, tout code généré automatiquement est supposé contenir des signes révélateurs du compilateur utilisé. Cette analyse vise à repérer les virus polymorphes qui sont indétectables autrement (leurs signatures changeant à chaque réplication). Car, lorsqu'un virus polymorphe crypte son code, la séquence en résultant contient certaines associations d'instructions que l'on ne trouve pas en temps normal, c'est ce que peut détecter l'antivirus.

Une fois un virus détecté, il ne reste plus qu'à le supprimer. Mais ce n'est pas si simple qu'on le croit d'éradiquer l'intrus 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 leur duplication. La seule solution est alors la destruction des fichiers infectés.

Pour les autres types de virus, même si la récupération du fichier d'origine n'est pas impossible, la tâche est cependant très ardue. Il faut savoir très précisément où est localisé le virus dans le code du fichier en question, sachant qu'il peut être composé de plusieurs parties, ensuite, le supprimer puis, 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, d'ou la nécessité de répertorier dans une base de donnée mise à jour régulièrement toutes les caractéristiques des différents virus.

Une fois que l'on possède un antivirus de qualité, il faut l'utiliser de manière efficace. Pour cela, un antivirus possède deux fonctions essentielles :

- une fonction de balayage (communément appelé SCAN) qui permet, sur demande, à l'utilisateur de vérifier le disque dur ou certains fichiers à la recherche d'un virus qui pourrait déjà y être présent. Idéalement, ce procédé devrait être effectué une fois par semaine.

- une fonction résidente ou permanente : elle fonctionne dès le lancement de l'ordinateur jusqu'à son extinction. Celle-ci opère en arrière plan, de façon transparente, et elle surveille toute l'activité du PC : elle analyse de façon dynamique les fichiers entrants et sortants de l'ordinateur, que ce soit par disquette, CD-ROM, courrier ou téléchargement. Elle inspecte aussi tous les exécutables à leur lancement, afin d'être sûre qu'ils ne déclenchent pas un virus dont ils seraient porteurs.

## 1.2 - Les pare-feux

En plus de l'antivirus, la protection la plus répandue en entreprise est le pare-feu (firewall). Cette solution bloque l'émission et la réception de flux réseaux pour certaines applications ou ports jugés dangereux par l'administrateur.

Les pare-feux Internet sont conçus pour isoler votre réseau local privé des flammes de l'Internet, ou de protéger la pureté des membres de votre réseau local en leur interdisant l'accès aux tentations démoniaques de l'Internet. Il peut être physique ou logiciel.

# II – Réparation en cas d'infection

## 2.1 - Un virus, comment réagir ?

Un système d'exploitation en mauvais état ou surchargé peut aussi provoquer des symptômes, tel lenteur dans l'affichage des messages, etc.

Il se peut, par exemple, que vous manquiez d'espace sur votre disque dur ou que vos ressources mémoires soient insuffisantes pour faire tourner une application donnée.

Vous vous demandez alors comment faire la différence entre un système atteint d'un virus et un système qui n'aurait besoin que d'une bonne remise en ordre. Généralement, lorsque vous observez un comportement soudain et imprévu comme l'émission d'un son étrange ou l'apparition d'un nom de fichier que vous ne reconnaissez pas, vous êtes probablement en présence d'un virus.

Si vous croyez avoir contracté un virus, vous disposez de plusieurs options :

- **Lancez un logiciel antivirus**.

Un bon antivirus coûte environ 50 $, mais c'est très peu payé considérant l'importance de la santé de votre ordinateur. Vous pouvez configurer la plupart des utilitaires pour qu'ils partent à la recherche de virus dès le démarrage de votre machine et qu'ils vous avisent lorsqu'ils détectent des fichiers contaminés. Un utilitaire vous avisera également si vous tentez d'ouvrir un fichier contaminé. Le balayage antiviral n'est pas absolument sans faille; aussi, si votre ordinateur se met à fonctionner de façon suspecte, lancez l'antivirus et faites-lui vérifier le système entier afin qu'il détecte et répare les fichiers contaminés.

- **Remplacez les fichiers**.

Si l'antivirus s'avère incapable de réparer les dégâts, vous n'aurez alors d'autre choix que de supprimer le fichier fautif et de le remplacer par une copie sécuritaire que vous tirez de votre plus récente sauvegarde.

- **Redémarrez à partir d'un disque sain**

En effet, certains virus attaquent les enregistrements d'amorçage d'un disque (région d'un disque où sont lues les instructions de démarrage), ce qui pourrait même vous empêcher de démarrer votre ordinateur. Dans les cas où votre ordinateur refuse de démarrer ou tombe en panne avant même que vous ne puissiez ouvrir un programme, vous ne pourrez lancer le logiciel antiviral.

Vous devez alors éteindre votre ordinateur, puis le redémarrer à l'aide d'une disquette d'amorçage, protégée en écriture. Votre système d'exploitation vous permet de créer de telles disquettes de démarrage. Il vaudrait mieux les créer avant que ne surgissent les problèmes.

- **Lancez un utilitaire de diagnostic et de réparation de disque** (après avoir redémarré avec la disquette d'amorçage).

Les systèmes d'exploitation de Windows et de Mac fournissent tous deux des utilitaires que vous pouvez utiliser pour le dépannage. Une fois votre ordinateur remis sur pied, relancez votre antivirus afin qu'il vérifie tout votre système.

- **Formatez votre disque dur**.

Si le lancement d'un utilitaire s'avère infructueux, votre disque dur est sûrement endommagé. Utilisez, dans ce cas, une disquette de démarrage qui offre la possibilité de reformater le disque dur, puis réinstallez votre système d'exploitation, à partir du disque original.

## 2.2 - La réparation de fichiers infectés

En général, on sait qu'un virus est présent sur un poste parce qu'un antivirus vous le dit. Si le virus est d'un type réparable votre anti virus se charge de tout. Mais ce n'est pas certain. Beaucoup de virus modifient suffisamment d'éléments pour qu'un anti virus ne puisse le nettoyer. Il vous faut alors vous documenter sur le virus puis trouver un batch de nettoyage ou une procédure détaillée.

Prenons l'exemple du virus win32.blebla.b (son nom varie suivant les versions). Ce virus place sur la partition principale un fichier nommé sysrnj.exe, puis modifie l'association de tous les fichiers exécutables pour les dévier vers ce fichier (lequel vous donnera accès de façon invisible au programme demandé). A chaque exécution, il va ronger un peu plus chaque jour votre système d'exploitation (son fonctionnement en détail est flou).

Un anti virus va au mieux supprimer le fichier sysrnj.exe, mais ne va pas ré associer les fichiers exécutables aux bons programmes, d'où un apparent plantage du système d'exploitation. Il faut alors trouver sur le Web un batch qui va réparer les effets de ce virus en particulier. Dans ce cas précis on trouvera un fichier nommé « fixblebla.com » sur le Web.

En règle générale, ces utilitaires se nomment « fix_nomduvirus.bat ou .com » (utile à savoir pour une recherche en ligne).

La plupart des éditeurs d'anti virus proposent des batch de réparation.

Quel que soit le virus rencontré, le succès de son éradication repose sur sa connaissance. Il peut être utile d'appeler à l'aide sur des forums.

# Conclusion

Ainsi, les dangers que représentent les programmes de destruction sont bien réels.

Cependant, lorsque la majorité des variables sont connues, nul n'est besoin de paniquer. En adoptant une attitude préventive et responsable vis-à-vis de l'ordinateur et vis-à-vis du réseau Internet, les risques d'infection sont grandement minimisés.

Dans le contexte des bibliothèques sans murs qui semble être l'avenir des bibliothèques au XXIe siècle, la plus grande part des sources d'information ne seront plus disponible qu'à distance via les grands réseaux de télécommunication.

Il sera donc nécessaire de bien connaître les virus et leurs effets afin d'être en mesure d'en parer ou d'en minimiser les répercussions. Il sera également très important d'être capable de faire la part des choses, de distinguer le vrai du faux afin de ne pas être victime du moindre canular, de la moindre rumeur qui pourrait faire surface à propos du réseau Internet.

Et bien que l'information au sujet des virus soit régulièrement remise en question et qu'elle soit sujette à interprétation, la plus grande prudence est de rigueur lors du transfert ou de l'échange de données informatiques.

Dans l’ensemble, le thème de ce rapport de fin de stage nous aura permis d’appréhender l’un des aspects de la sécurité informatique et nous a été bénéfique.

# Glossaire

**Adresse IP :** on parle aussi d'adresse internet. Adresse exclusive d'un ordinateur sur internet. Une adresse IP se compose d'un jeu de quatre nombres séparés par des points (donc elle est rédigée sur 32bits).

**ARPAnet** : réseau développé dans les années 60 par l'Advanced Research Projects Agency, du département US de la défense.

**Binaire : é**criture de nombres sous forme d'une combinaison de 0 à 1dans le contexte du net, les données binaires représentent toutes organisation de ces bits en octets, par opposition à une organisation représentant des caractères de textes.

**Browser** : navigateur ou explorateur.

**Connexion :** lien entre deux entités, deux ordinateurs, par exemple, afin de procéder à des échanges d'informations.

**Datagramme :** il s'agit tout simplement d'un groupe de paquets d'information qui circule sur le Réseau, et qui ne concerne que son contenu c'est-à-dire TCP, à ne pas confondre avec la "trame".

**Fichier :** collection d'informations binaires ou ASCII enregistrées en mémoire centrale ou sur disque. Un fichier peut se composer de texte, d'un programme, d'une base de données, de graphiques, etc.

**Firewall:** est un ordinateur que l'on met entre un réseau local (celui d'une entreprise) et un autre réseau (qui peut être Internet), et qui fait office de filtre afin d'assurer la sécurité des informations à l'intérieur du réseau local.

**FTP: *File Transfer Protocol*;** protocole permettant de transféré des fichiers d'un ordinateur à un autre.

**Http:** Hypertext Transfer Protocol. Protocole utilisé par les clients et les serveurs du world wide web pour communiquer.

**Hub:** En général, un concentrateur (en anglais, hub - cette traduction est souvent utilisée en français, mais c'est un anglicisme) est le nœud central d'un réseau informatique. Il s'agit d'un dispositif électronique servant de commutateur réseau, et permettant de créer un réseau informatique local de type Ethernet.

**Internet:** réseau des réseaux. Il connecte des réseaux locaux (ou LAN : Local Area Networks) ou vastes (WAN : Wide Area Networks) en utilisant le protocole TCP/IP pour offrir ses services.

**Intranet** : réseau local d'entreprise utilisant les techniques d'Internet et du web, mais séparé du net totalement ou par Proxy et un mur pare-feu.

**IP :** Internet Protocol. Protocole Internet définissant les unités d'information transmises entre système en mode paquet.

**ISO :** norme ISO échange de documents électroniques définissant un modèle de structuration de leur contenu.

**LAN:** sigle américain désignant un réseau local (local area network).

**MAN:** Réseau métropolitain. Réseau de transmission de données conçu pour être utilisé dans une ville. Sur le plan géographique, les MAN sont plus grands que les réseaux locaux (LAN), mais plus petits que les réseaux étendus (WAN). Les MAN se caractérisent généralement par des connexions à très haute vitesse réalisées à l'aide de câbles à fibres optiques ou d'un autre support numérique.

**Routeur :** est un matériel de communication de réseau informatique. Son travail est de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination finale le plus rapidement possible. Ce processus nommé routage intervient à la couche 3 (couche réseau) du modèle OSI.* Le routage est souvent associé au protocole de communication IP, même si d'autres protocoles routables moins populaires existent.

**Topologie:** Disposition des ordinateurs, câbles et autres éléments sur un réseau. Un réseau peut être maillé, en bus, en anneau ou en étoile.

**WAN:** Wide Area Network. Ensemble d'ordinateurs ou de réseaux interconnectés via un système de communication longue distance, par exemple par lignes téléphoniques et satellites, au lieu d'une liaison câblée par fils.

**Web:** raccourci de World Wide Web.

# Bibliographie


- Ouvrages et documents utilisés :
  - **Internet cette fois je m'y mets de** Henri Lilen
  - **Dictionnaire Larousse classique.**
- Cours
  - **Cours de système informatique et de réseau TCP/IP** : de Mrs Yobouet Koffi et Attokotouakpouet Simplice (Professeurs).
- Projet de fin d'étude
  - **Interconnexion d'un réseau** : de Irié Gbaou Bi Olive, étudiant à ITES.
- www.yahoo.fr.
- www.google.fr.

# ANNEXES