République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Génie Logiciel (G.L)*

Thème

La mise au point d'un antivirus

Réalisé par :

- **ADDAD Nesrine**

Présenté le 14 Décembre 2015 devant le jury composé de MM.

- *Mme.ILES Nawel* *(Président)*
- *Mme.DIDI Fedoua* *(Encadreur)*
- *Mr.BELHOUCINE Amine* *(Examinateur)*

Année universitaire : 2015-2016

DEDICACES

Je dédie ce modeste travail et ma profonde gratitude à celle qui m'a transmis la vie, l'amour, le courage, à toi chère maman toutes mes joies, mon amour et ma reconnaissance, à mon très cher père à qui m'adresse au ciel les vœux les plus ardents pour la conservation de sa santé et de sa vie, pour l'éducation qu'ils m'ont prodigué ; avec tous les moyens et au prix de toutes les sacrifices qu'ils ont consentis à mon égard, pour le sens du devoir qu'ils mon enseigné depuis mon enfance.

J'adresse ma gratitude aussi à mes très chères sœurs Hind et Menel

Je n'oublie pas mon petit frère Mohammed Rayen et toute ma Famille

Je dédie aussi ce projet de fin d'études aux responsables du notre département, à tous mes enseignants surtout à mon encadreur, et sans oublier mes collègues de 2 ème année master informatique et mes chers amis.

ADDAD Nesrine

REMERCIEMENTS

Avant tout, le grand et le vrai merci à Allah qui nous a donné la volonté et le courage pour la réalisation de ce travail.

Nous tenons à remercier tout particulièrement Mme DIDI Fedoua enseignante à l'université Abou Bekr Belkaid notre encadreur de mémoire pour son aide, son soutien, ses conseils, sa patience et sa générosité. Son ouverture d'esprit, sa disponibilité et ses analyses pertinentes ont contribué à rendre cette étude agréable et enrichissante.

Nous souhaitons remercier nos examinateurs d'avoir accepter de participer au jury de ce mémoire : Mr. BELHOUCINE Amine, Mme.ILES Nawel

Nous nous n'oublierons pas de remercier tout le corps enseignement de notre université (faculté des sciences de l'ingénieur de Tlemcen) pour les conseils avises et les suggestions qui nous ont été proposées.

Enfin, nous tenons à remercier tous ceux qui ont contribué d'une façon ou d'une autre à la réalisation de ce mémoire.

TABLE DES MATIERES

TABLE DES MATIERES

TABLE DES MATIERES

Aujourd'hui la sécurité devient un enjeu majeur pour tout le monde parce que chacun de nous est devenu une victime potentielle pour ceux qui convoitent l'information personnelle ou industrielle ou autre, sécuriser ses informations, son réseau son matériel est un besoin plus que important.

La sécurité informatique c'est l'ensemble des moyens techniques utilisés pour garantir et assurer un ou plusieurs concepts comme la confidentialité, l'authentification, l'intégrité, la non répudiation, le contrôle d'accès et la disponibilité.

- ✓ La confidentialité : consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- ✓ Authentification : consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
- ✓ Intégrité : consiste à vérifier si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- ✓ Non répudiation : empêcher l'émetteur ou le récepteur de nier avoir transmis ou reçu un message.
- ✓ Contrôle d'accès : est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications.
- ✓ Disponibilité : son objectif est de garantir l'accès à un service ou à des ressources.

Notre application est une simple application antivirus qui est considéré comme un chainon parmi les mécanismes de la sécurité.

Le document est organisé comme suit :

Chapitre I : décrit quelques notions sur les virus et les techniques de détection d'un virus.

Chapitre II : présente les détails d'implémentation de notre application.
Et en fin une conclusion générale qui résume notre travail.

Chapitre I : Généralités sur les virus et les Techniques de détection d'un virus

I. Introduction

De nos jours, l'internet joue un rôle de plus en plus prépondérant dans notre vie quotidienne, cela implique que toute personne qui utilise internet risque d'être victime d'un virus informatique en téléchargeant des données, recevant ou bien envoyant des e-mails ou encore en chatant tout simplement …etc.

Pour cela, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services ou de l'information. Parmi ces mécanismes l'antivirus est un outil primordial pour au moins assurer la pérennité de son PC et au mieux préserver son PC d'intrusions malveillantes.

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur à travers des techniques, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible. [1]

Dans ce chapitre nous passons en revue quelques notions sur les virus les plus connus, ainsi que les techniques de détection des virus.

II. Généralités et historique

II.1. Historique

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 de programme 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 encore rien de malveillants, et puisqu'ils ne s'agissaient et ne se développaient que dans le mémoire vive d'un ordinateur. Il était donc facile de les neutraliser. Il suffit d'éteindre cette mémoire pour que tout rentre dans 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 la mémoire de masse et de se propager en causant des dommages irréversibles). A partir de cette époque, les choses sérieuses commencèrent. Les virus sont devenus un mal inévitable et 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. Puis les premiers virus via le 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. [7]

II.2. 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.***[7]

III. Définition d'un virus informatique

Les Virus informatiques sont appelés véritablement « CPA ou Code Parasite Autopropageable », ils 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. [7]

III.1. 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. [7]

III.2. 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. [7]

III.3. 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. [7]

III.4. Altération

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 les 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. [7]

IV. Cycle de vie d'un virus

Les virus informatiques passent par 7 grandes étapes :

IV.1. Création

C'est la phase ou le développeur implémente le virus. [9]

IV.2. Gestation

C'est la période pendant lequel le virus est copié en un endroit stratégique afin que sa diffusion soit la plus rapide possible. [9]

IV.3. Reproduction (infection)

C'est la phase pendant laquelle le virus doit se reproduire un nombre important de fois avant de s'activer pour garantir sa pérennité. [9]

IV.4. Activation

C'est le moment ou le virus s'active et commence son travail mais cela après la vérification des conditions bien précises. [9]

IV.5. Découverte

Cette phase de l'existence d'un virus n'est pas forcément consécutive à son activation, la découverte d'un virus est faite par l'utilisateur quand il s'aperçoit que son système a des comportements étranges, ou bien un antivirus performant qui détecte le virus avant qu'il ai eu le temps de faire des ravages. [9]

IV.6. Assimilation

Une fois la phase de découverte faite, le développeur doit modifier la base de signatures d'antivirus pour qu'il puisse détecter la présence du virus, il doit faire aussi le traitement adéquat de ce virus si c'est possible bien sur. Cette phase peut durer des jours ou bien des mois selon les compétences du développeur. [9]

IV.7. Elimination

C'est la mort du virus ou au moins la mort de l'exemplaire du virus sur une machine Dans les faits, aucun virus n'a réellement disparu, mais un grand nombre d'entre eux ont cessé de constituer une menace réelle. [9]

V. Structure des virus

Un virus est constitué de trois fonctionnalités principales et d'une quatrième optionnelle, on peut schématiser la structure d'un virus comme ci-dessous :

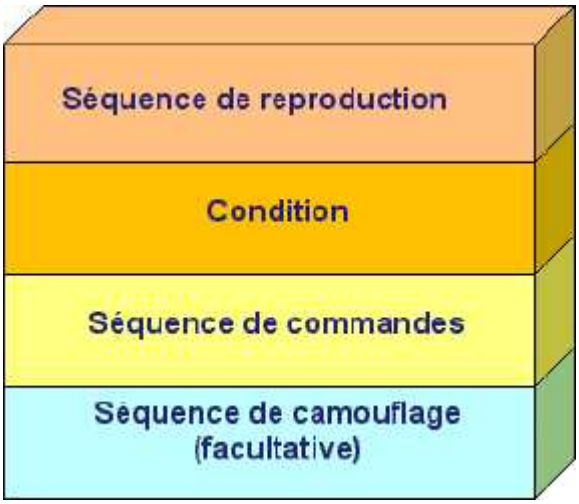

Figure I.1 : Structure d'un virus [2]

V.1. Séquence de reproduction

C'est le premier objectif du virus, elle contient une partie pour la recherche qui permet de localiser des fichiers à infecter mais elle doit assurer que le fichier n'est pas infecté déjà .Un virus ne doit pas se reproduire deux fois dans un fichier car son comportement serait faussé. [2]

V.2. Condition

C'est la partie qui va conditionner le lancement de travail d'un virus (détruire un fichier, casser le système d'exploitation ou autres choses). C'est la séquence de commande où de destruction qui est chargée de cette action. Elle est déclenchée lorsque la condition est satisfaite. Cette dernière peut être une date, une touche de clavier ou autre. [2]

V.3. Séquence de commandes

Elle effectue l'action d'un virus. Cette dernière peut être de détruire des fichiers, casser un système d'exploitation … [2]

V.4. Séquence de camouflage

Les développeurs essaient de cacher de façon toujours plus efficace leurs virus. Pour dissimuler au maximum leur création, les développeurs ont imaginés plusieurs techniques : il y a d'abord le cryptage qui consiste à rajouter au virus une routine de cryptage plus ou moins élaborée. Le problème est qu'une fois un virus crypté, il faut le décrypter afin qu'il puisse s'exécuter et appliquer ses précédentes fonctions. Il y a donc en plus de la routine de cryptage, une routine de décryptage qui apparaît en

clair dans le virus. Afin de parer cette lacune, d'ingénieux concepteurs de virus ont eu l'idée d'intégrer dans la séquence de décryptage des instructions aléatoire n'ayant aucun effet. Chaque variante du virus devient donc vraiment unique et indétectable par l'antivirus, on appelle ces virus **des virus polymorphes**.

Une autre technique de **furtivité des virus** est de faire croire au système d'exploitation que des secteurs du disque dur sont défectueux, il suffit alors au virus de s'y camoufler en attendant son activation. Cependant, si trop de secteurs deviennent défectueux, le système repère quelque chose d'anormal et il se peut que le virus soit détecté.

Enfin, une autre méthode permettant de ″ cacher ″ le virus est de le placer dans le secteur de Boot puisque quand un ordinateur se lance, il exécute toujours un certain secteur du disque (le boot) qui va lui permettre de lancer le système d'exploitation. Le virus se situant dans ce secteur sera alors exécuté à chaque démarrage. [8]

VI. Objectif d'un virus

L'objectif d'un virus est de pouvoir se dupliquer le plus souvent possible sur une ou plusieurs cibles. [3]

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. [3]

VII. Les familles de virus

Il existe quatre familles principales de virus. Elles ont chacune une cible bien précise :

- Les virus de boot : virus capable d'infecter le secteur de démarrage d'un support (disque dur, clé USB, etc.…). Il s'exécute lorsque votre ordinateur démarre (ou en lisant une clé USB infectée), un tel virus est ainsi chargé à chaque démarrage et prend le contrôle total de la machine avant que l'utilisateur ou un logiciel le prenne. Il est très répandu dans les années 1990 et au début des années 2000, il tend peu à peu à disparaitre. [9]

  Exemples: French boot ou Parity boot, Form.

- Virus de macros : ce type de virus infecte les macros des documents Microsoft Office c'est-à-dire qu'il peut être situé à l'intérieur d'un document banal (document Word ou bien Excel) et il exécute une portion de code à chaque création d'un document ou d'ouverture d'un document reposant sur lui. Dans ce cas il est possible de transmettre un virus d'un ordinateur à un autre par l'échange d'un document Word par exemple. [2]

- Les rétrovirus : on appelle aussi « flibustiers », ce type a la capacité de s'attaquer à l'antivirus pour le rendre inopérant. Parmi les méthodes utilisées par les rétrovirus, la modification des signatures de l'antivirus en est un bon exemple, ils peuvent aussi décharger la mémoire d'un antivirus c'est pour ça les rétrovirus font parti des virus les plus dangereux mais également les plus rares. [10]

- Virus d'application : Les virus d'applications infectent les fichiers exécutables, (notamment ceux portant les extensions *.exe*, *.com* ou *.sys ou .bat*). Il s'agit d'un morceau de programme, souvent écrit en Assembleur, qui s'intègre au début d'un programme normal.

Pour infecter, il cherche un programme cible, et remplace le premier segment de cet exécutable par son code viral. La section originale est ajoutée en fin de programme. Au moment de l'exécution du fichier, le code viral est donc lancé en premier. Il cherche encore d'autres programmes à infecter et les infecte, par le même mécanisme. Il restaure ensuite la première section du programme infecté (qu'il avait conservée, rappelons-le), et exécute le programme de manière normale. Sa propagation est donc complètement invisible, ce qui rend ces virus très contagieux. La détection de ce genre de virus est cependant assez aisée, ne serait-ce qu'en contrôlant

la taille des exécutable. Le fichier infecté est en effet plus grand que son homologue sain, puisqu'il contient le code du virus en plus du programme. [2]

VIII. Types de virus

Parmi les virus les plus connus :

- Vers : on appelle aussi «Worms » est 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 "vers", en particulier lorsqu'il se compose de plusieurs segments dispersés à travers le réseau. La différence, entre un vers et un virus, est que, **le vers 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 réplication peut donc non seulement infecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, le vers peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles. [3]
- Bombes logiques : se sont de petits programmes restant inactifs jusqu'à la détermination d'une condition. Cette dernière peut être un signal, une date, une heure ou encore une action attendue d'un utilisateur…etc.

  Une fois cette condition remplie, une suite de commandes va se déclencher.

  Le but des bombes logiques sont fréquemment utilisées pour créer un déni de service en saturant les connexions réseau d'un site d'un service en ligne ou d'une entreprise. Un exemple d'une bombe logique : Michelangelo qui devait se déclencher à la date anniversaire de la naissance de l'artiste (Michel-Ange).[1]
- Le Cheval de Troie : est un programme caché sous le nom ou au sein d'un programme légitime, il peut aussi s'intégrer dans une pièce jointe d'un courriel, via un lien piégé par le téléchargement de logiciels ou bien l'échange de clés USB, ils sont souvent désignés par l'appellation anglaise Trojan Horse. Son objectif est de pouvoir exécuter des actions à l'insu de l'utilisateur

(récupération, détournement, diffusion ou destruction des données), et /ou pour prendre à distance le contrôle de l'ordinateur. [2]

Exemple : Back orifice : permet l'administration à distance.

- Spyware : est un logiciel qui collecte les informations personnelles sur un ordinateur et les envoie sans l'autorisation de l'utilisateur. [5]

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

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

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

  □ consommation de mémoire vive,

  □ Utilisation d'espace disque,

  □ Mobilisation des ressources du processeur,

  □ Plantages d'autres applications,

  □ Gêne ergonomique (par exemple l'ouverture d'écrans publicitaires ciblés en fonction des données collectées). [5]

- Porte dérobée : C'est un moyen de contourner les mécanismes de contrôle d'accès. Elle s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle. [1]
- Cookies : Un cookie est un petit fichier très simple, en fait un texte, enregistré sur le disque dur de l'ordinateur d'un internaute à la demande du serveur gérant le site Web visité. Il contient des informations sur la

navigation effectuée sur les pages de ce site. L'idée originelle est de faciliter l'utilisation ultérieure du site par la même personne.

Un cookie n'étant pas exécutable, il ne peut contenir de virus. [1]

Il ya quelques attaques qui visent le courrier électronique parce que c'est un moyen de diffusion efficace et il est énormément utilisé par les gens, alors on peut citer :

- Spam: Envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact au préalable, et dont il a capté l'adresse électronique de façon irrégulière. (pourriel en français) [5]

  Pour éviter un spam il ne faut pas :

  - ✓ acheter par l'intermédiaire de publicité faite par un spam (des études indiquent que 29% des utilisateurs le font).
  - ✓ Répondre à un spam.
  - ✓ mettre d'adresses électroniques sur les sites web mais les encoder par un script ou dans une image (exemple: http://www.caspam.org);

Remarque : au lieu d'utiliser l'adresse électronique on peut créer des adresses jetables et les utiliser par la suite. Exemple: http://www.jetable.org (adresse valable d'une heure à un mois, certains sites peuvent ne pas accepter ce genre d'adresses). [5]

- Phishing : c'est une technique d'ingénierie sociale utilisée par des arnaqueurs (scammers). Elle est utilisée depuis 2003, L'objectif est d'obtenir des adresses de cartes de crédit, des mots de passe, etc. Dans ce cas l'utilisateur peut recevoir un courrier d'un site qui lui est familiale (banque, ..). [5]
- Hoax : c'est un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes (message alarmiste, fausses alertes de virus, vente pyramidale, promesse de gains, légendes urbaines, faux complots, prises par les bons sentiments, etc).

  Ils encombrent le réseau, et font perdre du temps à leurs destinataires. [6]

Il ya aussi d'autres attaques sur le réseau :

- Sniffing : interception des messages ou mot de passe par des renifleurs, identification des services du réseau, des machines qui communiquent, etc.
  C'est un outil permet de visualiser les trames sur un segment de réseau, il utilise les sockets. [6]
- IP Spoofing : Méthode d'attaque qui parodie l'adresse IP d'un autre ordinateur (usurpation). Elle permet de brouiller les pistes ou d'obtenir un accès à des systèmes sur lesquels l'authentification est fondée sur l'adresse IP (rlogin, rsh sur les machines à numéro de séquence TCP prévisible). [5]

- Déni de service (DOS) : c'est une attaque destinée à empêcher l'utilisation d'une machine ou d'un service. C'est un type d'attaque utilisée par frustration, par rancune, par nécessité, …
  Ce type d'attaque peut engendrer des pertes très importantes pour une entreprise. [5]
  On peut citer plusieurs types d'attaques DOS :
  - ✓ DOS local (épuisement de ressources) :
    – Saturation de l'espace disque
    – répertoires récursifs
    – boucle infinie de fork ()
    – …
  - ✓ DOS par le réseau (consommation de bande passante) :
    – SYN flood (Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible).
    – Réassemblage de fragments (Ex: teardrop, ping of the death)
    – Flags TCP illégaux
    – DOS distribué (DDOS) : Type d'attaque très en vogue.
    L'objectif est d'écrouler une machine et/ou saturer la bande passante de la victime. Nécessite un grand nombre de machines corrompues. [5]

- Scam : c'est une pratique frauduleuse d'origine africaine ("ruse") pour extorquer des fonds à des internautes. Par exemple la réception d'un courrier

électronique du descendant d'un riche africain décédé dont il faut transférer les fonds.

Elle est connue aussi sous le nom de 419 en référence à l'article du code pénal nigérian réprimant ce type d'arnaque. [5]

IX. Les conséquences des virus

Parmi les conséquences des virus, vers, spywares et spam :

- Perte de données
- Perte de temps de travail
- Perte d'image de marque
- Perte de fonctionnalités (système ou email bloqués)
- Perte de confidentialité. [5]

X. Les mécanismes de la sécurité

À cause des menaces provenant des logiciels malveillants, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

X.1. Cryptage

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre.

La Figure I.2 montre le fonctionnement de chiffrement. [1]

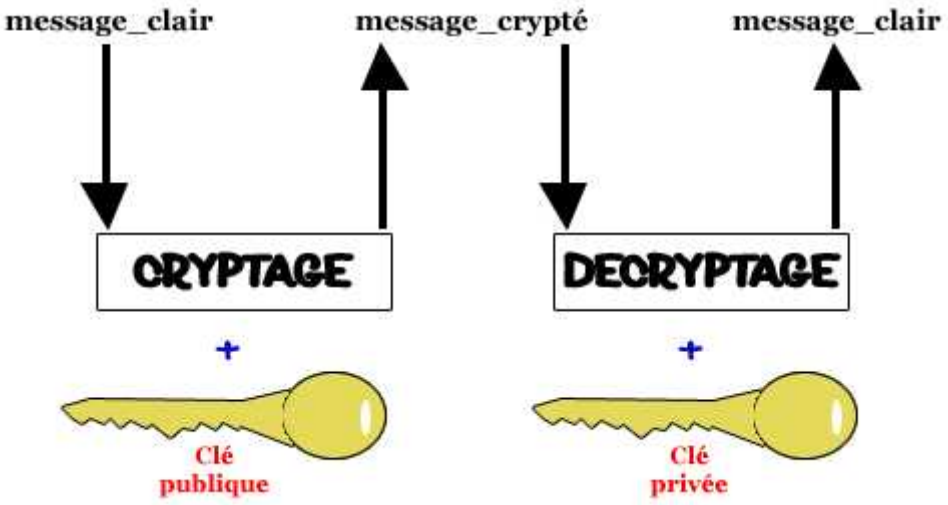

Figure I.2 : Cryptage [11]

X.2. Pare-feu (firewall)

C'est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité.

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante.

Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne.

D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau. [1]

La Figure I.3 schématise le fonctionnement d'un pare-feu.

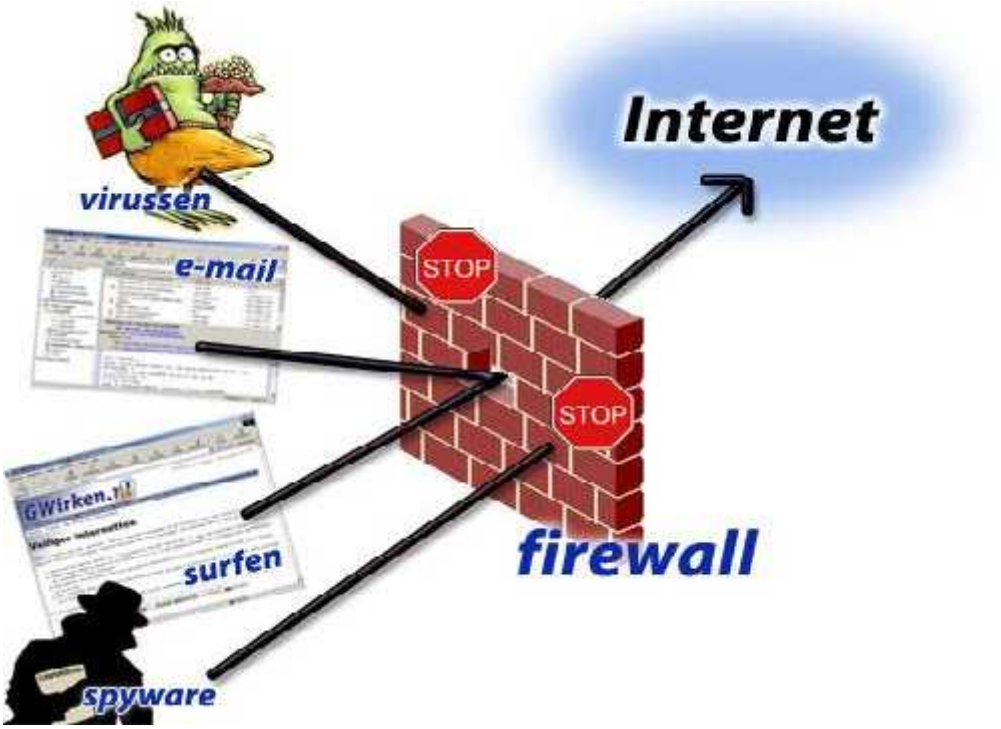

Figure I.3 : Pare-feu[12]

X.3. Antivirus

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]

X.4. IDS

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.[1]

X.5. IPS

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les

risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement.[1]

X.6. VPN

Dans les réseaux informatiques, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet).

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.[1]

La Figure I.4 montre le principe de protocole de tunnelisation.

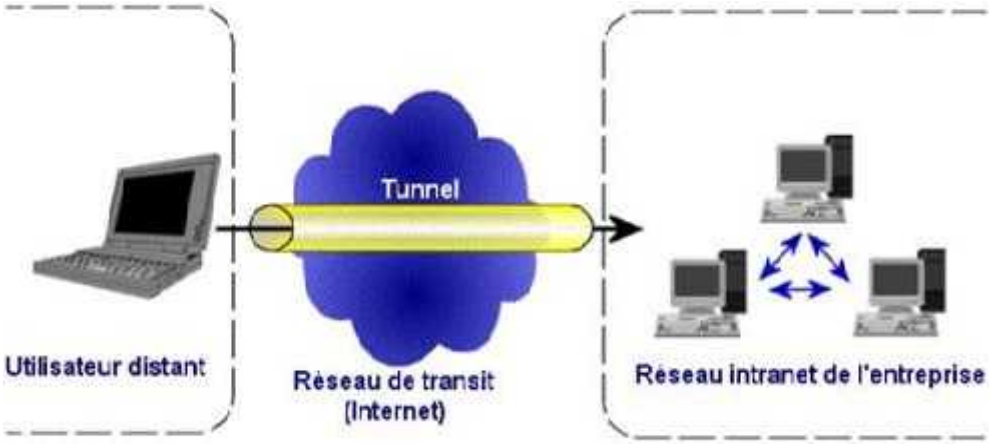

Figure I.4 : Principe de VPN [13]

XI. Fonctionnement d'un antivirus

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 l'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 ». [3]

✓ 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. [3]

XII. Les techniques de détection utilisées par un antivirus

Les antivirus utilisent principalement cinq méthodes pour détecter les virus :

- Recherche par signature
- Recherche heuristique
- Analyse spectrale
- Contrôleur d'intégrité
- Moniteur de comportement

XII.1. Recherche par signature

Il s'agit de la méthode la plus ancienne et la plus utilisée dans la plupart des antivirus.

Comme nous l'avons vu, les virus infectant des applications, copient leur code dans ces programmes. Et les virus sont programmés pour ne pas infecter plusieurs fois le même fichier. Dès lors, ils intègrent dans l'application infectée une signature virale, c'est-à-dire une suite d'octets significative, qui leur permet de vérifier si tel ou tel programme est déjà infecté.

La méthode de base utilisée par les antivirus est donc de détecter cette signature propre à chaque virus. Evidemment, cette méthode n'est fiable que si l'antivirus possède une base virale à jour, contenant les signatures de tous les virus connus.

Néanmoins, ce mécanisme ne permet pas la détection des virus « inconnus », c'est-à-dire n'ayant pas encore été répertoriés par les éditeurs. En outre, n'oublions pas que les virus polymorphes, dont nous avons déjà parlé, sont capables de se camoufler, c'est-à-dire de rendre leur signature indétectable (en la cryptant et en la modifiant à chaque copie). [2]

XII.2. Recherche heuristique

L'analyse heuristique est relative à la recherche de code informatique correspondant à des fonctions de virus. C'est-à-dire qu'elle est vouée à découvrir des virus encore inconnus. L'analyse heuristique est passive. Elle considère le code comme une simple donnée, et n'autorise jamais son exécution. Un analyseur heuristique recherche du code dont l'action pourrait s'avérer suspecte. En l'occurrence, il ne cherche pas des séquences fixes d'instructions spécifiques à un virus, mais un type d'instruction. Par exemple, des instructions visant la modification d'un fichier.

Cette méthode se dirige vers une démarche « intelligente » de recherche de virus.

Cela dit, elle est loin d'être totalement efficace. Elle fonctionne bien pour les macrovirus, moins bien pour les autres. Les plus sensibles des anti-virus heuristiques produisent un nombre de fausses alertes, et les moins agressifs rateront à coup sûr de véritables virus. [2]

Tous les anti-virus modernes utilisent fortement cette méthode en complément de la détection par signature. [4]

XII.3. Analyse spectrale

L'analyse spectrale repose sur le postulat que tout code généré automatiquement contiendra des signes révélateurs du compilateur utilisé. De même, on part du principe qu'il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code. L'analyse spectrale vise donc elle aussi à repérer les virus polymorphes ou inconnus. Lorsqu'un virus polymorphe crypte son code, la séquence en résultant contient certaines associations d'instructions que l'on ne trouverait pas dans un vrai programme. C'est ce que l'analyse spectrale tente de détecter. Par exemple, si dans un programme exécutable, l'antivirus trouve une instruction de lecture d'un octet au delà de la taille limite de la mémoire, on sera probablement en présence de code crypté, donc d'un virus polymorphe. [2]

XII.4. Contrôle d'intégrité

Un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque dur auxquels sont associées 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. [3]

XII.5. 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. U 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. [3]

XIII. Eradication de virus

XIII.1. Méthode d'éradication

Une fois un virus détecté, il faut le supprimer. Mais il n'est pas toujours simple de supprimer un virus sans endommager le programme original. En effet, certains virus détruisent une partie du programme sain lors de leur duplication. Il ne reste plus alors

qu'à détruire purement et simplement le fichier infecté. Dans les autres cas, la suppression du virus n'est pas forcément évidente non plus. Il s'agit d'abord de découvrir très précisément où est localisé le virus dans le fichier, sachant qu'il peut être composé de plusieurs parties. Il faut ensuite supprimer ces octets infectés, et récupérer la partie du programme dont le virus avait pris la place, afin de la restaurer. Toutes ces manipulations nécessitent bien sûr une parfaite connaissance du virus et de son mode opératoire. C'est à cela que servent les fichiers de signatures de l'antivirus, régulièrement remis à jour. Il faut non seulement pouvoir détecter le virus, mais aussi savoir où il cache la portion de code dont il a pris la place.

Certains virus plus complexes nécessitent un outil de suppression pour éliminer toutes les manifestations de la bête. Ils sont également utilisés pour les virus à grande échelle, lorsque les utilisateurs n'ont pas d'antivirus. Par exemple, pour le ver Blaster, un programme de *fix* a été proposé par l'éditeur Symantec, qui n'avait pas besoin d'antivirus pour s'exécuter. [2]

XIII.2. Les antivirus sont-ils efficaces

Il est entendu qu'aucun antivirus ne détecte tous les virus. Lorsqu'un nouveau virus est détecté, et qu'une mise à jour est disponible, même en quelques heures, il faut la télécharger, sans quoi l'antivirus ne fonctionne pas. A part les quelques techniques de découverte des virus inconnus, qui, nous l'avons vu, ne sont pas totalement au point.

Mais, et c'est plus grave, une étude menée dans les laboratoires Hewlett-Packard en Grande-Bretagne a conclu que les antivirus seraient en train de perdre la guerre contre les virus. En effet, selon eux, le principe même de fonctionnement de l'antivirus n'est pas efficace puisque les vers informatiques se propagent trop rapidement par rapport au temps requis pour l'application des mises à jour. Cela a été prouvé par les différents vers très connus, comme *I Love You* récemment. La multiplication des machines connectées à l'Internet associée à un ver qui se transmet par le réseau occasionne une contamination massive et exponentielle en très peu de temps. Ainsi, le ver Slammer avait infecté 90% des machines vulnérables en quelques minutes. Moins de temps qu'il n'en faut pour qu'un éditeur crée la réponse.

Dans une simulation par ordinateur, les chercheurs de HP ont démontrés que si les vers informatiques se propagent suffisamment rapidement, comme Blaster ou ILoveYou, les mises à jour nécessaires pour protéger les utilisateurs ne pourront pas être appliquées à temps.

Les chercheurs n'ont pas de solution concrète au problème. Ils proposent de créer un système de détection de modules malicieux qui repérerait les virus possibles en étudiant leur comportement. Un peu dans l'idée des analyseurs heuristiques ou spectraux, en plus efficaces. [2]

XIII.3. Mise à jour des antivirus

Cela pose donc la problématique de la mise à jour rapide des anti-virus, et donc de la mise à disposition rapide des antidotes. Symantec Security Response (anciennement le SARC - Centre de Recherche AntiVirus de Symantec) est composé d'une équipe dédiée de chercheurs, dont l'unique mission est de rechercher les nouvelles menaces et de développer des antidotes pour ces menaces. Cette équipe assure une permanence 24h/24 et 7 jours sur 7 afin d'être toujours là en cas de problèmes. Les chercheurs sont capables de développer des définitions de virus en moins de 24 heures pour Norton AntiVirus, et ils sont continuellement à la recherche de nouvelles technologies pour améliorer la lutte contre les virus. Symantec Security Response emploie 40 personnes dans le monde, avec un budget de 4 millions de dollars.

Malgré toutes ces bonnes intentions, rien ne garantit que l'utilisateur final effectue des mises à jour assez régulières. Ni qu'un virus à propagation rapide n'aura pas déjà infecté les machines avant la mise à disposition de l'antidote. [2]

XIV. Conclusion

Dans ce chapitre, nous avons donné des notions sur les virus les plus connus et quelques attaques. Nous avons présenté par la suite quelques mécanismes de la sécurité, parmi ces mécanismes : l'antivirus.

Le prochain chapitre décrit la mise en œuvre de notre application certes simple qui consiste à lancer un simple antivirus qui détecte les virus dans un fichier choisi par l'utilisateur.

Chapitre II: La conception et l'implémentation

I. Introduction

Ce chapitre présent la description de notre application développée, cette description est divisée en deux parties : La conception et l'implémentation, la première présente quelques aspects relatifs à la conception et la modélisation de l'application, tandis que la deuxième traite la phase d'implémentation ainsi que les outils de développement.

II. La conception et l'implémentation

II.1. La conception

Notre objectif est de mettre en œuvre un simple antivirus qui fait l'analyse d'un fichier et détecte les virus dans ce fichier à travers des signatures spécifiques à chaque type de virus.

Pour mieux décrire notre application on va utiliser quelques diagrammes UML : le diagramme de cas d'utilisations, le diagramme de classes et les diagrammes de séquences.

II.1.1 Le diagramme de cas d'utilisation

Le diagramme suivant (figure II.1) représente la vue utilisateur de notre application, il décrit les cas d'utilisation du système implémenté.

Ce diagramme contient un seul utilisateur, son rôle est de :

- ✓ scanner un fichier avec deux manières différentes, la première consiste à choisir le fichier puis le scanner. Et la deuxième consiste à choisir le fichier et ajouter le virus à ce fichier, ensuite scanner ce dernier. S'il contient un virus il donne la possibilité de le supprimer.
- ✓ Contacter le développeur pour poser des questions ou bien pour obtenir une nouvelle version d'antivirus.
- ✓ changer le thème de l'application selon son gout.

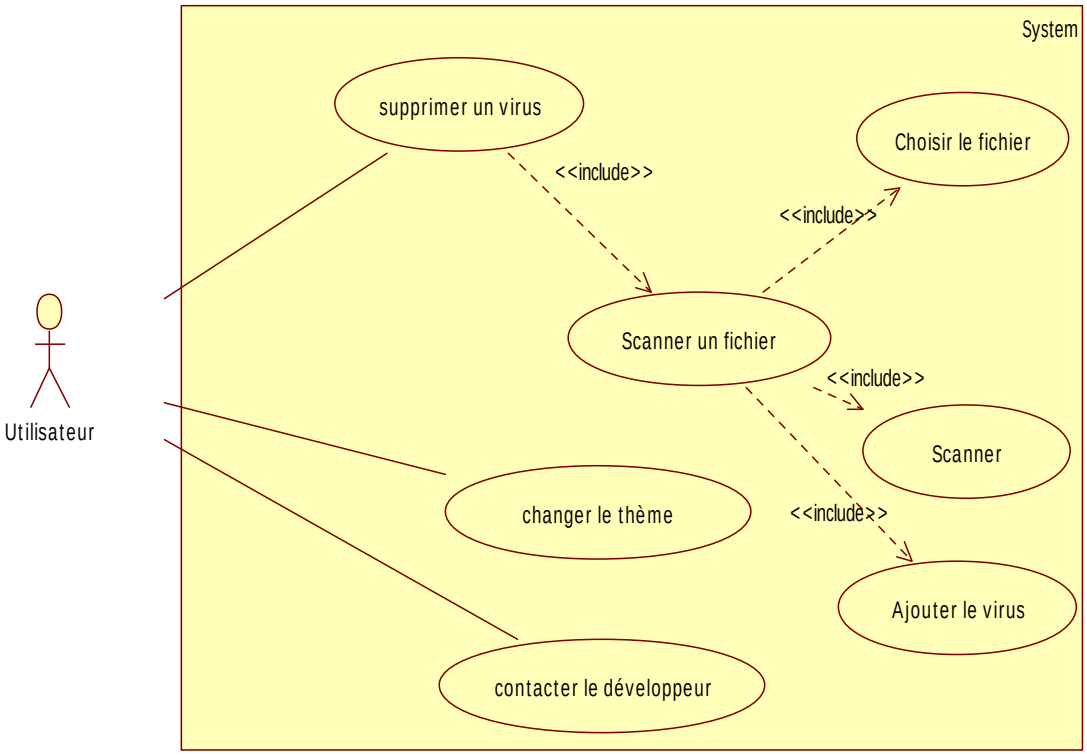

Figure II.1 : diagramme de cas d'utilisation

II.1.2. Le diagramme de classes

Le diagramme suivant (figure II.2) décrit l'ensemble des classes de notre application. Nous avons utilisé des simples classes antivirus, lecture de fichier, lecture de base, une classe pour scanner le fichier et une autre donner l'arborescence d'un répertoire, classe pour ajouter le virus et une autre pour le supprimer.

La classe antivirus est une classe qui fait la relation entre les autres classes

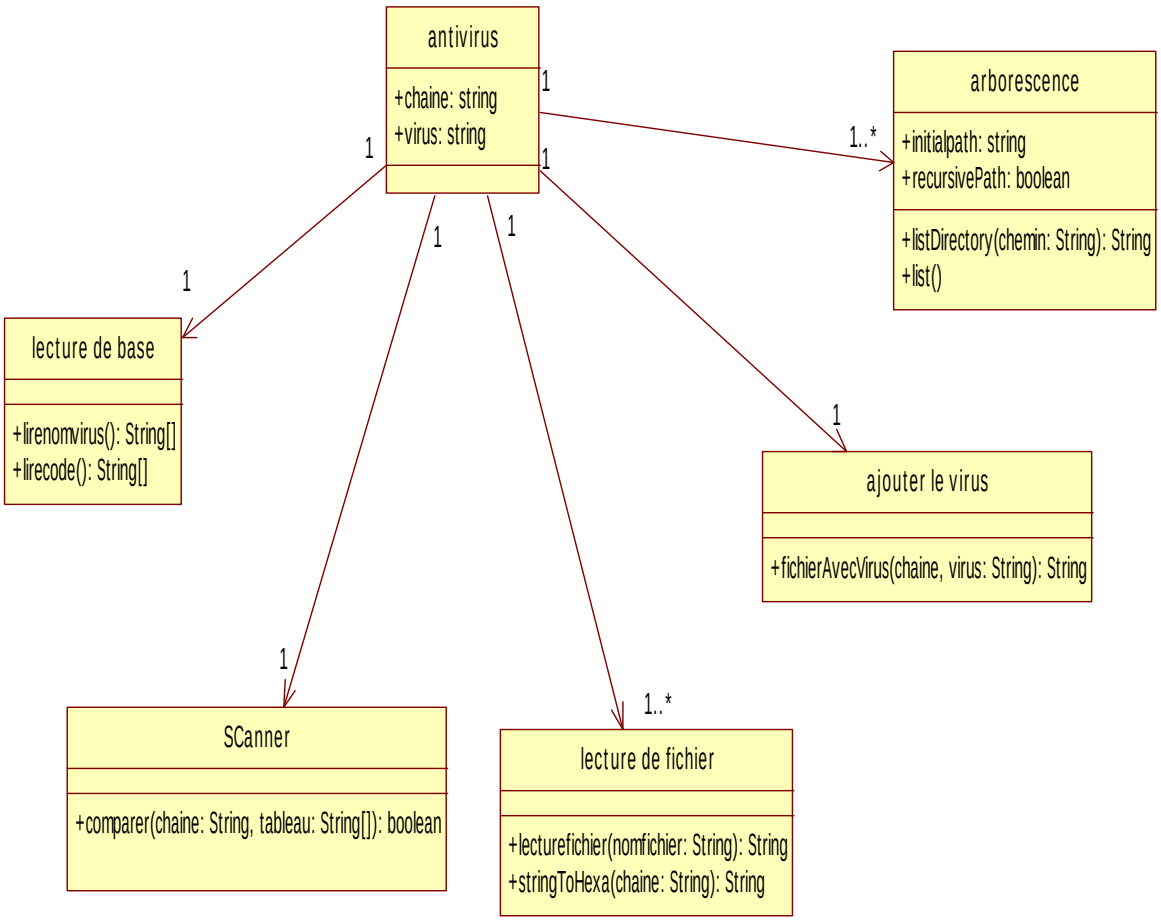

Figure II.2 : diagramme de classes

II.1.2. Le diagramme de séquence

- Scanner un fichier sans virus :

Ce diagramme (figure II.3) décrit le premier cas d'utilisation : scanner un fichier sans virus

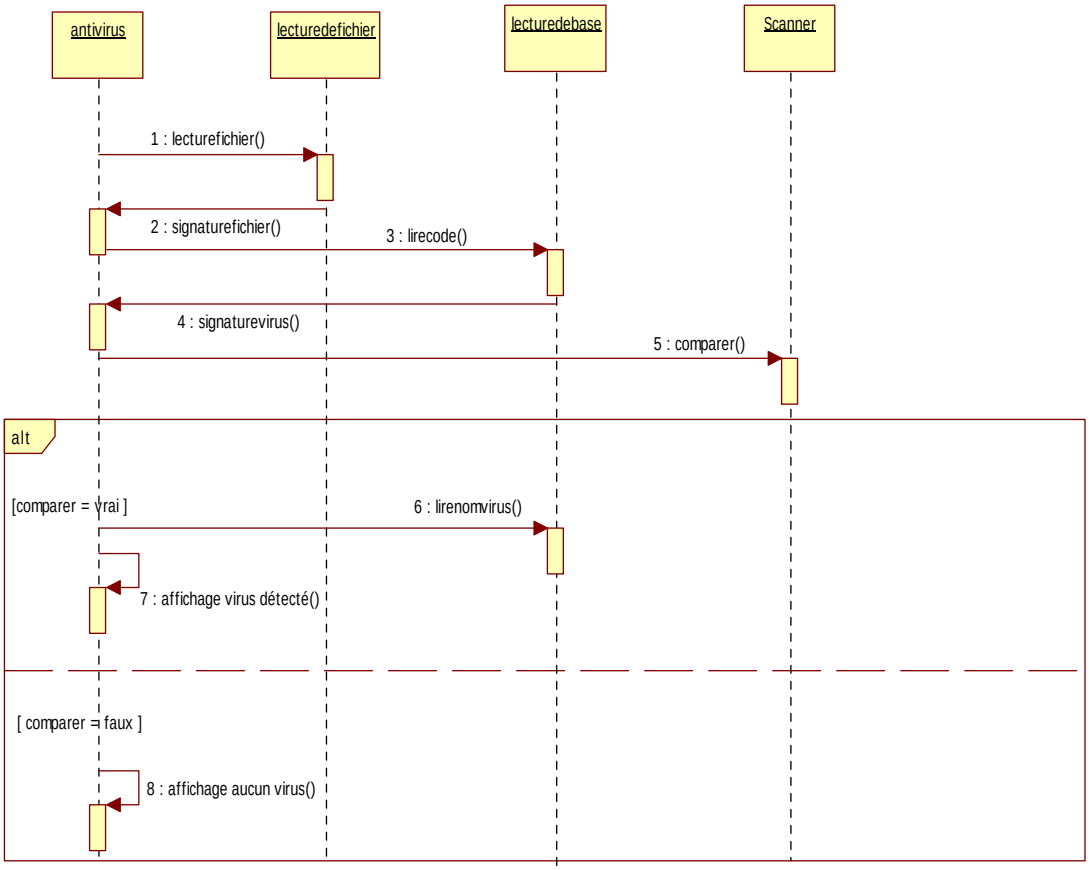

Figure II.3 : diagramme de séquence (scanner un fichier sans virus)

- Scanner un fichier avec virus :

  Le diagramme suivant (figure II.4) exprime le cas d'un fichier contenant un virus (le chemin de détection + le traitement).

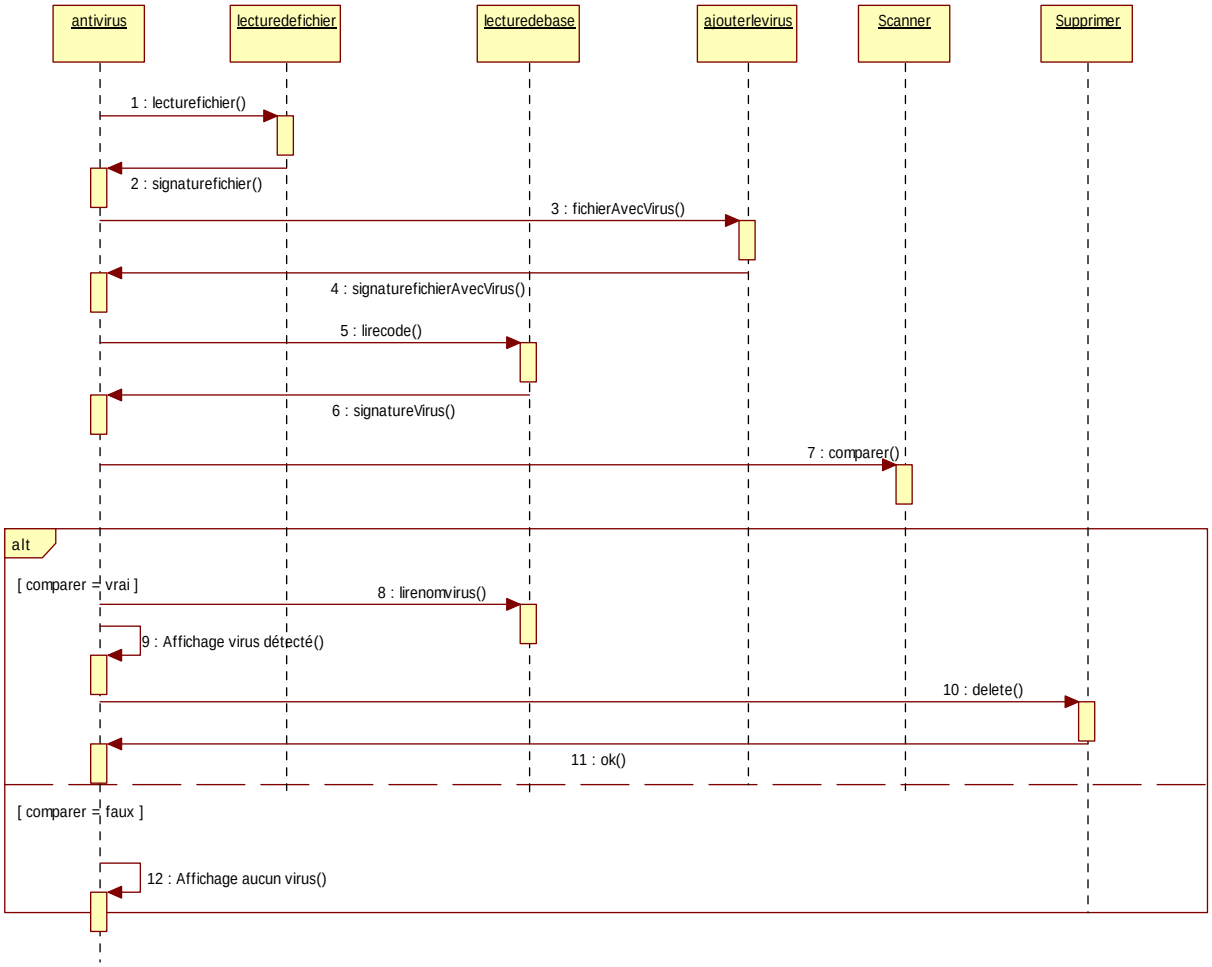

Figure II.4 : diagramme de séquence (scanner un fichier avec virus)

II.2. L'implémentation

II.2.1. Outils utilisés

- ✓ Netbeans 8.0.2 : NetBeans est un environnement de développement intégré (IDE) pour Java, placé en open source par **Sun**. En plus de Java, NetBeans permet également de supporter différents autres langages, comme C, C++, XML et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditer en couleur, projets multi-langage, éditeur graphiques d'interfaces et de pages web). NetBeans est disponible sous Windows, Linux et d'autres systèmes d'exploitation. Il est lui-même développé en Java, ce qui peut le rendre assez lent et gourmand en ressources mémoires.

- ✓ StarUml : est un outil de modélisation **UML**, Il est open source (libre). StarUML gère la plupart des diagrammes spécifiés dans la norme UML 2.0.

StarUML est écrit en delphi, et dépend de composants Delphi propriétaires (non open-source), ce qui explique peut-être pourquoi il n'est plus mis à jour.

II.2.2. Les étapes de l'implémentation de l'antivirus

Nous avons basé dans l'implémentation de notre application sur :

- Créer une base de signatures contenant quelques signatures des virus connus en hexadécimal. Dans notre application la base est un fichier de type txt.
- Faire un algorithme d'arborescence qui nous donne l'arborescence d'un répertoire, c'est-à-dire il affiche tous les sous répertoires et les fichiers contenus dans chaque sous répertoire.
- Lire les fichiers et comparer la signature d'un fichier avec les signatures de notre base.
- Détection de virus et le traitement (suppression).

II.2.3. Implémentation

Notre application contient trois partitions : Home, Scan et Paramètres.

- Home : donner des informations sur l'application.

Figure II.5 : Home

- Scan : permet de choisir un fichier pour le scanner, on peut aussi tester notre antivirus par l'ajout d'un virus ensuite le scanner.

Figure II.6 : Scan

- Paramètres : elle nous permet de changer le thème de notre application.

Figure II.7 : Paramètres

III. Conclusion

Dans ce chapitre nous avons présenté les principes de conception et d'implémentation des différentes parties de notre application.

L'exécution de notre antivirus a atteint son objectif, et la communication entre la base des signatures et l'antivirus s'est faites correctement, aussi la détection des virus a fourni des résultats fiables comme prévu.

Le travail présenté dans ce mémoire tourne autour une application antivirus, l'objectif était de créer un simple antivirus qui détecte les virus contenus dans un fichier à travers la signature virale.

Finalement, on a réussi à implémenter cette application d'une manière simple et compréhensible, même si elle est loin d'être utilisable sur le plan pratique mais elle reste une bonne expérience, cette dernière est un bon complément de notre formation de base, elle nous a permis d'enrichir nos connaissances théoriques et pratiques, et constitue la base de départ pour des futurs travaux.

Nos perspectives étant de continuer dans le domaine de la sécurité, de bâtir une base solide pour pouvoir développer des applications plus consistantes, et plus complètes.

Bibliographie et webographie

[1] Z.BENDELLA, «Gestion de la sécurité d'une application Web à l'aide d'un IDS comportemental optimisé par l'algorithme des K-means », Thèse de Master, Université de Tlemcen, 2013.

[2] G.CHARPENTIER, O.MONTIGNY, M.ROUSSEAU, « Virus / antivirus », janvier 2004.

[3] J. LEGRAND, « Virus et Antivirus », STS Informatique de Gestion.

[4]M.BERTIN, O.GUERIN, P.LOINTIER, et al. , « Les virus informatiques », club de la sécurité des systèmes d'information français, 2005.

[5] P.Ducrot, « Sécurité informatique »,2013.

[6] T. Tram DANG NGOC, « Introduction à la sécurité réseau », Universit_e de Cergy-Pontoise, 2013.

[7]https://www.academia.edu/4916366/Plan_INTRODUCTION_Partie_I_LES_VIRUS_INFORMATIQUES_GENERALITE_ET_HISTORIQUE_DEFINITION_TYPOLOGIE_ET_CLASSIFICATION_Types_Contenu_par_type_Les_virus_Programme_Principe_de_fonctionnement_Exemples. Consulté novembre 2015

[8] http://www.cybermafia.fr/structure-d-un-virus-informatique.html. Consulté octobre 2015

[9] http://tecfaetu.unige.ch/staf/staf-j/diego/staf14/ex8/virus.html . Consulté décembre 2015

[10] http://www.anti-virus1.com/les-6-diff%C3%A9rents-types-de-virus-informatique-les-plus-dangereux-expliquer . Consulté décembre 2015

[11] https://openclassrooms.com/courses/l-algorithme-rsa/crypter-et-decrypter. Consulté septembre 2015

[12] http://blog.thenetworkhardware.com/features-and-functions-of-firewalls/. Consulté novembre 2015

[13] http://www.frameip.com/vpn/. Consulté décembre 2015.

LISTE DES FIGURES

Chapitre I : Généralités sur les virus et les techniques de détection d'un virus

Chapitre II : La conception et l'implémentation

Résumé

Notre travail consiste à faire un simple antivirus, nous avons implémenté un algorithme qui fait l'analyse d'un fichier choisi par l'utilisateur, en utilisant la signature virale de ce fichier sélectionné. Puis on fait la comparaison entre cette signature et les différentes signatures des virus contenues dans notre base des signatures. Dès qu'il trouve deux signatures identiques, cela veut dire que notre fichier est infecté, sinon notre fichier est protégé.

Mots clés : antivirus, virus, signature virale, base des signatures, algorithme.

Abstract

Our work focus on making a simple antivirus, we are implemented an algorithm that makes the analysis of a file selected by the user, using the virus signature of this selected file. Then we make a comparison between this signature and the signatures of different viruses contained in our database signatures. As soon as he finds two identical signatures, it means that our file is infected, otherwise our file is protected.

Keywords: antivirus, viruses, signature virus, database signatures, algorithm.

ملخص:

يتمثل عملنا في تجسيد تطبيق خاص بمكافحة الفيروسات(أونتي فيروس)فذنا خوارزمية التي تقوم بتحليل الملف المحدد من قبل المستخدم، و ذلك بلستخدام التوقيع الفيروسي لهذا الملف. بعد ذلك يتم إجراء المقارنة بين التوقيع الخاص بالملف ومختلف التوقيعات الخاصة بالفيروسات الواردة في قاعدة البيانات الخاصة بالفيروسات. بمجرد أن يجد توقيعات متطابقة هذا يعني أن الملف مصاب بفيروس، وإذا وجد العكس فإن هذا الملف لا يحتوي على فيروس.

الكلمات الأساسية: أونتي فيروس،فيروس، التوقيع الفيروسي، قاعدة البيانات الخاصة بالفيروسات، خوارزمية.