ECOLE SUPERIEURE PRIVEE D'INGENIERIE ET DE TECHNOLOGIES

EXPOSE SUR LA DETECTION DES VIRUS INFORMATIQUES

REALISE PAR : PATRICK MUKUTA

HAMDI

ENCADRE PAR :

TABLE DES MATIERES

INTRODUCTION

ANNEE-UNIVERSITAIRE 2009-2010

DETECTION DES VIRUS INFORMATIQUES

INTRODUCTION

La microinformatique a vu le développement d'un type nouveau d'agression, qui n'a pas à ce jour d'équivalent dans les autres domaines de l'informatique : le virus informatique. Lorsque l'on sait qu'un virus peut détruire tout un ordinateur, aussi bien au niveau matériel que logiciel, nous comprenons alors que les virus informatiques deviennent un fléau de plus en plus important dans notre société. Pour tenter de vaincre ou tout du moins de contrer ce fléau, il faut tout d'abord comprendre leur fonctionnement pour une meilleure protection d'informations stockées ainsi que de nos systèmes. Voilà la logique dans laquelle cet exposé s'inscrit.

Pour y répondre, nous développerons six points principaux. Tout d'abord nous nous attarderons (au premier point) non seulement sur la définition d'un virus, mais aussi sur sa structure. Ensuite, il s'agira au deuxième point, de situer dans le temps la naissance des virus informatiques. Au troisième point, nous dirons un mot sur les différents types des virus. Enfin ,les deux derniers points, répondront à deux grandes questions qui constituent l'axe autour duquel gravite le présent travail. Il s'agira donc de répondre aux questions suivantes :

Comment est–ce qu'un système d'exploitation parvient à détecter un virus ?

Comment est-ce qu'un système infecté se comporte-t-il ?

1. DEFINITION ET STRUCTURE D'UN VIRUS INFORMATIQUE

1.1 DEFINITION

Selon SYMANTEC NORTON, un virus informatique est un logiciel malveillant écrit dans le but de se dupliquer sur d'autres ordinateurs. Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB etc. Son appellation provient d'une analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire. On attribue le terme de « virus informatique » à l'informaticien et spécialiste en biologie moléculaire Leonard Adleman (Fred Cohen, Experiments with Computer Viruses, 1984).

Ainsi, le véritable nom donné aux virus est *CPA* soit *Code Auto Propageable*, mais par analogie avec le domaine médical, le nom de "virus" leur a été donné. Ils peuvent se répandre à travers tout moyen d'échange de données numériques comme l'internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc.

Il sont dotés des fonctions suivantes:

- Auto reproduction
  il s'agit de la faculté qu'a un virus de se dupliquer ou se recopier luimême soit de façon systématique, soit si certaines circonstances sont remplies.
- Infection
  Il s'agit de la contamination, c'est-à-dire le programme dupliqué va se loger de manière illégitime dans certaines parties du système informatique.
- Activation
  elle se produit uniquement si certaines conditions programmé par son auteur sont réunies : lors du nième lancement du virus ou toute autre conjonction arbitraire de certaines conditions.
- Altération
  Destruction du système ou de l'information stockée. Cette destruction est exécutée lorsque les conditions d'activation programmées par l'auteur (du code sont remplies) , le virus déclenche une fonction d'agression restée en sommeil.

Remarque : Les virus informatiques ne doivent pas être confondus avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer le programme hôte. Il convient donc de noter qu'un programme ne peut être appelé virus que s'il a la propriété de se reproduire et de passer d'un système à un autre.

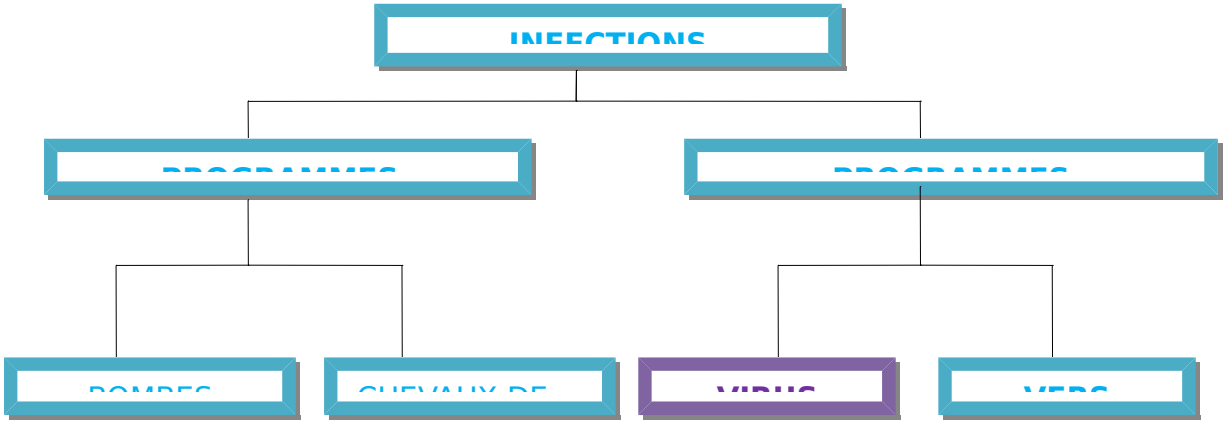


Figure 1: Classification des infections informatiques

1.2. STRUCURE DES VIRUS

Un virus se compose de 3 fonctionnalités principales et d'une quatrième optionnelle. La figure 2,en est une illustration.

Figure 2: Structure d'un virus

1.2.1. Séquence de reproduction

C'est l'objectif premier du virus. Elle inclut une fonctionnalité de recherche, qui permet de rechercher des fichiers à infecter. Elle permet aussi au virus de vérifier d'abord que le fichier n'est pas déjà infecté, pour ne l'infecter que le cas échéant. En effet, un virus ne doit pas se reproduire deux fois dans un fichier, car son comportement serait alors faussé.

1.2.2. Condition

Il s'agit tout simplement de la partie qui va coordonner le lancement de l'action qu'est censé accomplir le virus. En effet, le virus a toujours un objectif précis (détruire des fichiers, casser le système d'exploitation et bien d'autres choses encore).C'est la séquence de commande (ou de destruction) qui est chargée de cette action. Elle est déclenchée lorsque la condition est satisfaite. Cette dernière peut-être de diverses forme (une date, un action particulière de l'utilisateur, une réaction spécifique de l'ordinateur...).Les développeurs de virus font preuve de toujours plus d'imagination pour trouver des conditions de déclenchement de plus en plus originales et spécifiques. Cette condition peut aussi être à l'origine du bon fonctionnement ou non du virus. Par exemple, un développeur de virus voulant déclencher son virus un dimanche, avait spécifié dans l'instruction de se déclencher le jour numéro 7 (de la semaine).Or, en informatique, tout index commence à 0. Une semaine de 7 jours va donc du jour 0 au jour 6. Le virus ne s'est donc jamais déclenché ! Dans ce cas-là, le virus est certes présent sur le système, mais est inoffensif.

1.2.3 Séquence de commandes

Comme nous venons de le dire, c'est elle qui effectue l'action du virus. Cela peut être détruire des fichiers, formater une partition...

1.2.4. Séquence de camouflage

Malgré leur petite taille, les virus peut être vite repérés (pour certains). Les développeurs de virus ont donc élaboré plusieurs techniques pour cacher le virus. Il existe plusieurs techniques. Nous les aborderons en parlant des virus polymorphes.

2. ORIGINE DES VIRUS INFORMATIQUES

- Dès 1949 Von Neumann, auteur du principe sur lequel reposent les ordinateurs actuels, démontre théoriquement la possibilité de programmes auto copiables.

- Dans le début des années 60, quelques informaticiens des laboratoires Bell inventent le jeu Core War. Le principe consiste à implanter dans la mémoire d'un ordinateur deux programmes qui vont alors, sans aucune intervention humaine, lutter l'un contre l'autre en cherchant à se localiser et à se détruire mutuellement.
- En 1983 le terme «virus informatique» est défini officiellement pour la première fois par Leonard Adleman, chercheur en informatique théorique.
- En 1986 l'Arpanet, est victime du virus Brain qui renommait toutes les disquettes de démarrage de système. Les créateurs de ce virus y donnaient leur nom, adresse et numéro de téléphone car c'était une publicité pour eux.

3. TYPES DE VIRUS INFORMATIQUES

Il existe différents types de virus, les distinctions entre eux étant plus ou moins ténues. Avant d'en dresser la liste la plus exhaustive possible, signalons que les experts en virus ne sont pas tous d'accord quant à cette classification. Nous donnons donc ici une certaine topographie, qui peut différer d'autres topographies.

3.1. Les virus mutants

En réalité, la plupart des virus sont des clones, ou plus exactement des «***virus mutants***», c'est-à-dire des virus ayant été réécrits par d'autres utilisateurs afin d'en modifier leur comportement ou leur signature.

Le fait qu'il existe plusieurs versions (variantes) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données.

3.2. Les virus polymorphes

Le virus polymorphe est un virus dont le programme change à chaque reproduction, mais l'action pour lequel il a été créé est toujours la même. Par exemple, le virus peut intervertir l'ordre des instructions de son action en son sein, ou rajouter de fausses instructions, afin de tromper la vigilance de l'antivirus, qui lui, recherche une signature précise. Beaucoup de virus polymorphes sont aussi encryptés. Le virus encryptera son code et ne le décryptera que lorsqu'il doit infecter un nouveau fichier, le rendant encore plus difficile à détecter

3.3. Les rétrovirus

Le rétrovirus est un nouveau type de virus informatique ayant la capacité de désactiver les pare-feu et les logiciels anti-virus. Ce virus représente une menace croissante pour la sécurité informatique et les connexions internet.

3.4. Les virus de secteur d'amorçage

virus capable d'infecter le secteur de démarrage d'un disque dur c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.

3.5. Les virus trans- applicatifs (virus macros)

Peuvent être situé à l'intérieur d'un document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (généralement Windows).

4. MÉTHODE DE DÉTECTION DES VIRUS

L'antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, 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. Les antivirus utilisent principalement cinq techniques pour détecter les virus :

- *La recherche de signature ou scanning*
- *du moniteur de comportement*
- *du contrôleur d'intégrité*
- *la recherche heuristique*
- *Analyse spectrale*

4.1. RECHERCHE DE SIGNATURE (SCANNING)

Il s'agit de la méthode la plus ancienne et la plus utilisée. Son avantage est de permettre la détection des virus avant leur exécution en mémoire. Son principe consiste à rechercher sur le disque dur toute chaîne de caractères identifiés comme appartenant à un virus. Cependant, comme chaque virus a sa propre signature, il faut, pour le détecter avec un scanneur, que le concepteur de l'antivirus ait déjà été confronté au virus en question et l'ait intégré à une base

de données. Un scanneur n'est donc pas en mesure de détecter les nouveaux virus ou les virus dits polymorphes (car ils changent de signature à chaque réplication) ; toutefois, une mise à jour régulière de la base de donnée est recommandée.

On appelle donc ***signature*** d'un virus la caractéristique particulière à un virus, qui est stockée dans la base de données de l'antivirus et qui lui permet de l'identifier (c'est comme le fichier des empreintes digitales des criminels qui permettent aux enquêteurs de retrouver les criminels dont leurs empreintes se trouvent dans ledit fichier répertoriant les empreintes). La signature virale n'est autre que la trace laissée par le virus dans un fichier infesté.

Il peut s'agir de son nom, sa taille, ou d'une chaîne de caractères présente dans le code. Aujourd'hui, un antivirus repère plus de 70 000 signatures stockées dans sa base de données.

4.2. 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 associés quelques caractéristiques. Ces dernières peuvent prendre en compte :

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

Un CRC (Code de Redondance Cyclique), ou un algorithme de checksum avec un système de chiffrement propriétaire, pourra détecter toute modification ou altération des fichiers en recalculant le checksum à chaque démarrage de l'ordinateur (si l'antivirus n'est pas résident), ou dès qu'un fichier exécutable est ouvert par un programme (si l'antivirus est résident) ; en effet, si le checksum d'un programme avant et après son exécution est différent, c'est qu'un virus a modifié le fichier en question, l'utilisateur en est donc informé. D'autre part, l'antivirus peut aussi stocker la date et la taille de chaque fichier exécutable dans une base de données, et ainsi, tester les modifications éventuelles au cours du temps. Il est en effet rare de modifier la taille ou la date d'un fichier exécutable. La parade pour les virus est de sauvegarder la date du fichier avant la modification et de la rétablir après.

4.3. MÉTHODE HEURISTIQUE

L'analyse heuristique concerne la recherche de code correspondant à des fonctions virales. Elle est différente, dans son principe, d'un moniteur de comportement qui surveille des programmes ayant une action de type viral. L'analyse heuristique est comme le scanning, passive. Elle considère le code comme une simple donnée, et n'autorise jamais son exécution.

Un analyseur heuristique va donc rechercher le code dont l'action est suspecte, s'il vient à être exécuté. L'analyse heuristique permet par exemple, pour les virus Polymorphes, de chercher une routine de déchiffrement. En effet, une routine de déchiffrement consiste à parcourir le code pour ensuite le modifier. Ainsi, lors de l'analyse heuristique, l'antivirus essaie de rechercher non pas des séquences fixes d'instructions spécifiques au virus, mais un type d'instruction présent sous quelque forme que ce soit. Cette méthode vise à analyser les fonctions et instructions les plus souvent présentes et que l'on retrouve dans la majorité des virus. Elle permet ainsi, contrairement au scanning, de détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

4.4. 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.

4.5. ANALYSE SPECTRAL

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.

5. VIRUS INFORMATIQUE FACE AUX DIFFERENTS ENVIRONNEMENTS

Comme pour les virus biologiques, où la diversité génétique ralentit les chances de croissance d'un virus, en informatique ce sont les systèmes et logiciels les plus répandus qui sont les plus atteints par les virus. En revanche, aucun système n'est épargné par ces derniers.

Cependant, les systèmes à diffusion plus restreinte ne sont pas touchés proportionnellement. La majorité de ces systèmes, en tant que variantes de l'architecture UNIX (BSD, Mac OS X ou Linux), utilisent en standard une gestion des droits de chaque utilisateur leur permettant d'éviter les attaques les plus simples, les dégâts sont donc normalement circonscrits à des zones accessibles au seul utilisateur, épargnant ainsi la base du système d'exploitation.

6. VIRUS ET ANOMALIES FONCTIONNELLES

Comment savoir si son pc a "attrape" des virus ?

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

- Changement de taille et /ou de date de création d'un fichier
- Changement de somme logique de contrôle (checksum)
- Un simple ralentissement de la machine
- L'ordinateur a un comportement anormal
- La taille mémoire disponible pourra se révéler réduite par rapport à ce que l'on a tendance à observer (639 Ko au lieu de 640).
- Un message d'erreur indiquant qu'un périphérique n'a pas été reconnu
- La disparition de données jusque-là accessibles
- Des bruits inhabituels ou un dysfonctionnement du disque dur, etc.

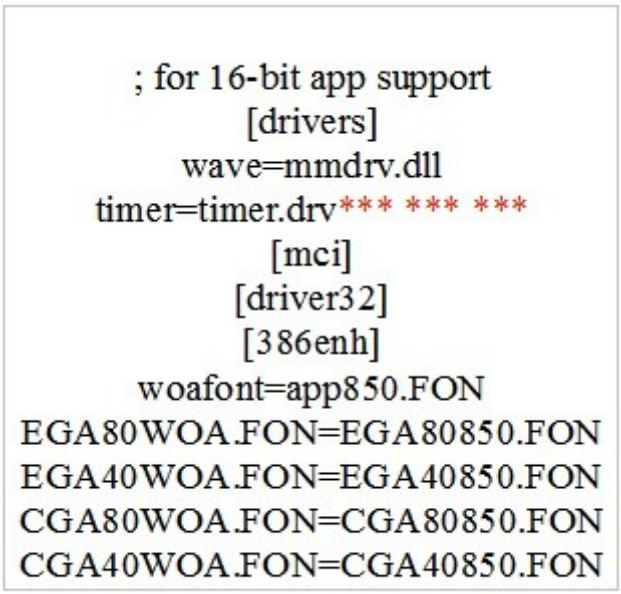
ASTUCE (astuce pour l'environnement Windows) :

En l'absence d'un anti-virus, il y a lieu de vérifier si votre PC est infecté. Il suffit de suivre les étapes ci-après :

Allez dans le menu Démarrer, recherchez "Exécuter", cliquez sur "Exécuter"
et tapez la commande system.ini, confirmez en cliquant sur OK.
Une fenêtre va s'ouvrir :
Si vous avez le message suivant :

- votre PC n'est pas infecté.

Par contre si vous avez ce message avec des étoiles rouges, c'est que le PC est infecté .



CONCLUSION

En manière de conclusion, il sied de noter qu'aucun logiciel anti-virus n'offre une garantie absolue de protection d'un système d'exploitation. On peut donc comparer l'anti-virus à un gilet pare-balles : celui-ci n'empêche pas la possibilité de blessures à la tête ou aux membres, mais il réduit fortement les risques.

C'est pourquoi, il appartient à l'utilisateur de prendre quotidiennement des précautions afin d'éviter que le système soit infecté par les virus informatiques :

- Ne pas ouvrir à « l'aveuglette » les fichiers qui vous sont envoyés en pièces-jointes
- Scanner toutes sources extérieures
- Activer un pare feu matériel et logiciel
- Débarrassez-vous des logiciels espions
- Ne pas installer de logiciels dont on n'est pas sûr à 100%
- Posséder un antivirus configuré et à jour
- Optimiser et nettoyer votre système (ex Ccleaner)
- Avoir un système d'exploitation toujours à jour ,etc.