République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab Blida

Faculté des sciences

Département d'informatique

Mémoire Présenté par :

Miraoui Akli

En vue d'obtenir le diplôme de master

Domaine : INFORMATIQUE

Spécialité : Génie des Systèmes Informatiques

Thème : Cryptage et détection de virus cryptés

Soutenu le : 20/09/2015

Membre des jurys

M.- Cherif Zehar
Mme - Tahahri
Mme - Arkam

Promotrice

Mme.Zahra Fatima

Promotion
2014 / 2015

Table des matières

Introduction générale 8

I Sécurité informatique **9**

1. Introduction 9
2. Définition de la sécurité informatique 9
3. Éléments d'une politique de sécurité 12
4. Objectif de la sécurité informatique 15
5. L'ampleur du problème 15
6. Les attaques informatiques 16
   - 6.1 Le système de fichiers en réseau 16
   - 6.2 Le social engineering 17
   - 6.3 Le crackage de mot de passe 17
   - 6.4 Le sniffing des mots de passe et des paquets 18
   - 6.5 L'IP spoofing 19
   - 6.6 Les chevaux de Troie 20
   - 6.7 Les vers 21
   - 6.8 Le TCP-SYN flooding 21
7. conclusion 22

II Les virus **23**

1. Introduction 23
2. Définition des virus 24
   - 2.1 Virus de type infection (chevaux de troie, botnet..) 24
   - 2.2 Virus de type CPA (Code Parasite Autopropageable) 24
3. Typologies et classification : 24

4. Cycle de vie d'un virus 26
5. Modes d'infection 27
6. Détection d'infection virale 29
6.1 Aspects techniques des Antivirus 29
6.2 Principales techniques de recherche virus 29
6.3 Recherche de la signature (SCANNING) 30
6.4 Utilisation d'un contrôleur d'intégrité 30
6.5 Moniteur de comportement 31
6.6 Démarche heuristique 31
6.7 Analyse spectrale 31
6.8 Technique d'éradication de virus 32
7. Conclusion 32

III La cryptographie **33**

1. Introduction 33
2. Définition générale 33
3. Aperçu historique 34
3.1 L'âge artisanal 34
3.2 L'âge technique 34
3.3 L'âge paradoxal 35
4. La cryptographie symétrique et asymétrique 36
4.1 Le cryptage symétrique 36
4.2 Le cryptage asymétrique 36
5. Avantages et inconvénients de la cryptographie 37
5.1 Cryptage symétrique 37
5.2 Cryptage asymétrique 37
6. Différents logiciels pour le cryptage 38
7. Conclusion 38

IV Techniques de propagation des virus et Cryptovirologie **39**

1. Introduction 39
2. Techniques de propagation des virus 39

2.1 Java drive-by 40
2.2 Infection par exploits 42
3. Propagation par réseaux 43
3.1 P2p spread 43
4. Cryptovirologie 46

V Technique de cryptage et détection des virus cryptés **48**
1. Introduction 48
2. Principe de fonctionnement 48
2.1 Le Runtime 48
2.2 Le Scantime 49
2.2.1 Crypter Scantime 49
3. Persistance Mode 52
3.1 Schtasks create 52
4. File joiner 53
5. Détection d'infection 53
5.1 Deuxième méthode de détection 56
6. Conclusion 56

VI Implémentation et tests **57**
1. Introduction 57
2. Logiciels et langages utilisés 57
2.1 Logiciels 57
2.2 Langages : 58
3. Application du principe 59
3.1 Le crypter 61
3.2 Application de l'exploit 64
4. Partie détection 66
4.1 Première technique 66
4.2 Deuxième technique 68
5. Conclusion 70
Conclusion générale 71

Bibliographie 73

Table des figures

I.1 Caractéristiques et exigences 10
I.2 SYN ACK 22

II.1 Infection par écrasement 27
II.2 Recouvrement de code 28
II.3 Virus par accompagnement de code. 28
II.4 Technique de recherche des virus. 30

III.1 Chiffrement de César 34
III.2 Machine enigma 35
III.3 Cryptographie à clé secrète 35
III.4 Cryptographie à clé publique 35

IV.1 Java drive-by pack. 40
IV.2 Softpedia 40
IV.3 Java drive-by 1. 41
IV.4 Java drive-by 2. 41
IV.5 Java drive-by 2. 42
IV.6 P2P 43
IV.7 Filenamer 44
IV.8 ApexDC++ 1. 44
IV.9 ApexDC++ 2. 45
IV.10 ApexDC++ 3. 45
IV.11 Cryptographie + virologie 46
IV.12 Les différents crypters et leur prix 47

V.1 Binary to text. 49
V.2 Stub. 50
V.3 Virus crypté. 51
V.4 Pack complet de cryptage. 51
V.5 Schtasks create. 52
V.6 Filejoiner 53
V.7 Scan du réseau avec Wireshark. 54
V.8 Wireshark filter DNS. 54
V.9 Communication du virus. 55
V.10 Partie du code du virus crypté 55
V.11 Scanner + générateur de signature. 56

VI.1 Njrat 1. 59
VI.2 Scan Njrat. 60
VI.3 Trojan vers Base 64 61
VI.4 Résultat du scan virus crypté 1. 62
VI.5 Résultat du scan virus crypté 2. 63
VI.6 Njrat 2. 64
VI.7 ScriptCryptor Compiler 65
VI.8 Fichiers joints. 65
VI.9 Fichiers joints après l'exécution 65
VI.10TCPView 67
VI.11TCPvcon 67
VI.12Résultat du test. 68
VI.13Database creator 69
VI.14Scanner. 69
VI.15Schéma explicatif. 70

Liste des tableaux

Introduction générale

Il est bien évidement important de contrôler ,maîtriser et de connaitre les droits des utilisateurs du système informatique ainsi connaitre les ressources de l'entreprise à protéger, et cela surtout lors de l'ouverture de l'accès sur internet de cette dernière donc il faut être au courant des différents dangers et risques qu'elle pourra faire face.

Les virus informatiques font partie des problèmes les plus anciens de la sécurité informatique. Pour détourner les anti-virus, les hackers malveillants ont inventé toute sorte de procédés. Un sujet bien à la mode dans le domaine du hacking consiste à crypter un fichier dans le but de le rendre indétectable par le plus grand nombre d'anti-virus possible Différents types de crypter ont vu le jour comme les Code Dom , cheikh crypter qui permettent de compiler du code source à la volée, par exemple dans le but de rendre unique les noms des variables et des fonctions, par la suite il permet au programme malveillant d'être exécuté dans une autre zone mémoire, notamment celle d'un processus considéré « de confiance » comme sv-chost.exe , sans oublier le changement de format et son intégration de cette dernière dans le Task Manager sous le même format.

L'objectif de notre travail consiste à déterminer quelles sont les différentes techniques de sécurité utiliser dans le domaine de divulgation d'information et comment les utilisateurs malveillants de la nouvelle technologie font pour contourner cette dernière pour y parvenir a leurs buts sur tout dans le domaine de chiffrement qui est utilisé pour contourner la sécurité anti virale de tout système d'exploitation , alors on se demande c'est quoi ses techniques ? et comment les grandes sociétés multinationales destinées à développer des Antivirus font pour les détecter ?

Chapitre I

Sécurité informatique

1. Introduction

Actuellement, les ordinateurs sont appréciables en tant que dispositifs autonomes , mais lorsqu'on dispose d'un ordinateur personnel sans connexion réseau, a t-on besoin d'une sécurité informatique ? Normalement L'endroit est assez sure pour protéger la machine, il en va plus tout a fait de même lorsque les ordinateurs sont reliés les uns aux autres via l'Internet. L'interconnexion des ordinateurs permet de tisser la toile du web , et celle ci repose d'abord sur la confiance mutuelle.Le problème est que cette confiance est régulièrement trahie avec différentes manières ou de techniques.

Mais toute nouvelle technologie possède ses bon et ses mauvais cotés. Si les opportunités offertes au niveau commercial sont considérables, de nombreuses entreprises s'exposent a un risque de sécurité énorme sans réellement en avoir conscience, des entreprises ont investi des millions de dollars dans ses outils et s'aperçoivent maintenant que la sécurité n'y a pas été correctement intégrée.

2. Définition de la sécurité informatique

C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier

les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [1] :

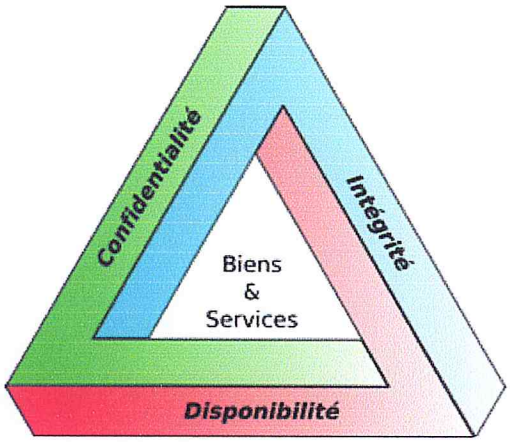


FIGURE I.1 – Caractéristiques et exigences [2].

- **disponibilité :**

  Toute information doit être disponible ; en gros le bon fonctionnement du système. Un pirate a besoin d'un accès à un système informatique dans ses attaques visant la confidentialité ou l'intégrité qui n'est pas le cas pour les attaques contre la disponibilité car ses dernières peuvent être réalisées contre n'importe quel système connecté à Internet ce qui rend la défense contre elles très difficile. Pour Pouvoir accomplir leur travail, de nombreux employés ont besoin de pouvoir accéder à des réseaux et à leur e-mail donc la connectivité Internet est essentielle et indispensable pour l'activité de beaucoup d'entreprises car les données, les informations, les serveurs et les réseaux doivent être disponible pour les utilisateurs légitimes. Par exemple un employé doit non seulement pouvoir s y connecter mais aussi accéder aux données en temps en heure afin de se procurer un document situé sur un serveur distant [3].

- **Confidentialité :**

  Le but est d'empêcher, de détecter et de dissuader les modifications non autoriser d'informations. Les gens pensent en premier lieu aux atteintes à la confidentialité des informations, lorsqu'ils se préoccupent de sécurité. Les intrusions dans les

bases de données, les fichiers clients sont les attaques les plus évidentes contre la confidentialité leur but majeur et de s'emparer de numéros de cartes de crédit, de données confidentielles, d'informations parfois vitales pour une entreprise. Cependant il existe des attaques contre la confidentialité qui ne sont pas aussi manifestes. Il peut s'agir d'erreurs commises par des employés qui ouvrent des trous de sécurité dans le système :

- Un administrateur qui oublie de redéfinir les permissions sur les fichiers après la restauration du système à partir de la copie de sauvegarde.
- Une personne qui ne détruit pas correctement des documents confidentiels.

La première chose pour remédier les plus gros trous de sécurité remettant en cause la confidentialité est d'examiner soigneusement la manière dont les permissions sont configurées toute en sensibilisant les employées aux principes de base de la sécurité. Lorsqu'un ordinateur est dérobé, la première atteinte est cette portée à la disponibilité de la ressource donc il s'agit d'une attaque par déni de service.

Par ailleurs puisque le disque dur de cet ordinateur est librement consultable par le voleur, on a affaire à l'accès d'un utilisateur non autorisé aux données de l'entreprise. Pour éluder ce type d'attaque, il faut d'abord assurer la sécurité des accès physique et du réseau. Une autre solution pour préserver la confidentialité des informations c'est le cryptage mais ce dernier ne protège pas la perte de données lors du vol d'un portable ou d'une unité Centrale. Donc a compléter par une solution de sauvegarde [3].

- **Intégrité :**

  Être sur que l'information n'a pas été modifiée que par des personne non autorisées à la modification. Il existe des attaques contre l'intégrité qui impliquent une atteinte a la confidentialité comme on peut aussi trouver des attaques qui impliquent toute les modifications malveillantes ou inappropriées des informations ou des données de l'entreprise pour bien comprendre on s'appuie sur l'exemple

[4]

4. Objectif de la sécurité informatique

L'objectif de la sécurité des systèmes informatique : est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité des gens des institutions, des entreprise etc... Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à limiter les atteintes ou dysfonctionnements induits et autoriser le retour à un fonctionnement normal à moindres coûts et dans des délais acceptables en cas de sinistre. La sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre. Ce n'est rien d'autre qu'une stratégie préventive qui s'inscrit dans une approche d'intelligence économique [5].

5. L'ampleur du problème

Il faudrait de nombreuses pages, voir même un livre entier pour établir la liste des sites piratés et les virus qui existe dans la toile du net. On en citera quelque-un plus bas ou on trouve des cites commerciaux , ou gouvernementaux , nationaux , internationaux ect.. car apparemment rien et aucun domaine n'est à l'abri.

Site :

- Banque d'Israël : Maures 2008 d'origine algerienne , Ali 2012 d'origine saudienne.
- Mosad :ismail-Man-54 dorigine algerienne 2015.
- Paris-tv, Mark zuckerberg account : Ismail-man-54 2012.
- tv5 : un autre algerien donc le pseudo est inconnu 2015.
- Hackingteam.it : societé italienne qui développe des logiciels d'espionnage pour les gouvernements (Maroc, Égypte, Italie,brésil) 2015
- CIA,FBI,Nokitel,Motorola,Nokia :Kevin Mitnik.

Virus :

- Spyeye : un des principaux Botnet développé par Bx1 ancien membre de darkode.com ¡BX1¿ fait face à 23 accusations selon le ministère de la Justice américain.
- Zeus :un autre Botnet don le Master Mind est Evgeniy Mikhailovich Bogachev.
- warbot :utiliser lors de l'attaque contre l'Estonie en 2009.

- njrat :cheval de Troie qui est connue par sa stabilité.
- RCS Gallileo : qui coute 355.000$ /licence , développé par hackingteam.it

6. Les attaques informatiques

Il existe plusieurs types d'attaques informatiques parmi lesquelles on peut citer [6] :

6.1 Le système de fichiers en réseau

Le système d'exploitation décide si oui ou non l'utilisateur à le droit d'accéder a un fichier, a chaque fois qu'un utilisateur fait une requête pour accéder au fichier en question. Les permissions d'accès mises par le propriétaire du fichier déterminent qui aura accès au fichier donc le système d'exploitation prend une décision basée sur qui ces permissions [6].

Deux causes principales derrière la protection de ses fichiers des autres utilisateurs :

- La première a pour but de cacher et protéger le contenu de ses fichiers des autres utilisateurs. on ne veut pas que les autres utilisateurs soit capable de lire ou de modifier le contenu du fichier parce qu'on considère le contenu de ce dernier comme privé.

- La seconde raison est que des tierces personnes peuvent obtenir l'accès au compte en modifiant des fichiers. Prenons l'exemple d'un utilisateur malintentionné qui a l'accès «écriture» dans le répertoire racine, il peut alors créer ou modifier le fichier «.rhost« (sous UNIX) donnant un accès illimité à n'importe quelle autre personne au compte. Il se dit, comme l'utilisateur est responsable de son compte, que tous les dégâts engendrés sont sous sa responsabilité directe.

l'obtention de l'accès administrateur (root) est le principal but d'une personne qui cherche à s'introduire dans un système car cet accès permet à la personne de tout faire sur ce système : effacer, modifier ou ajouter de nouveaux fichiers. Une fois sur la

machine en tant qu'utilisateur sans privilège particulier, le hacker peut alors lancer une attaque pour obtenir l'accès "super utilisateur" sur la machine en utilisant un trou de sécurité dans le système d'exploitation.

6.2 Le social engineering

Les hackers utilisent ce terme pour désigner une technique d'intrusion sur un système qui repose sur les points faibles des personnes qui sont en relation avec un système informatique plutôt que sur le logiciel. Ils révèlent le mot de passe ou toute autre information qui pourrait compromettre la sécurité du système informatique afin de piéger les gens [6].

Le piège classique est la demande urgente du mot de passe par le ou les techniciens afin de piéger les utilisateurs du système. Le hacker mentionnera qu'il a besoin du mot de passe pour d'importants travaux d'administration du système et il demandera à ce qu'on lui envoie le mot de passe par mail. Sachant qu'il est possible pour le hacker de créer un e-mail faisant croire qu'il provient de quelqu'un que l'on croit être le légitime administrateur réseau. Bien évidemment si la ruse se déroule par téléphone, le hacker imitera la voix du technicien.

Une autre forme de social engineering c'est de deviner le mot de passe d'un utilisateur. En connaissant des informations sur un utilisateur, peuvent les utiliser pour deviner le mot de passe de ce dernier. Par exemple, la plaque d'immatriculation de sa voiture, le prénom de ses enfants, leur date de naissance. Les hackers peuvent aller très loin pour deviner les mots de passe.

6.3 Le crackage de mot de passe

Les mots de passe sont la première ligne de défense contre les attaques sur un système d'où vient leur importance.

si un hacker n'arrive pas d'interagir sur un système distant et qu'il ne peut pas ni

lire ni écrire dans le fichier des mots de passe alors il n'a quasiment aucune chance de développer une attaque couronnée de succès sur ce système. Le hacker utilise le dictionnaire dans son attaque c'est la manière la plus classique utilisée pour obtenir un mot de passe [6].

Dans ce genre d'attaque, le hacker utilise un dictionnaire de mots et de noms propres, et il les essaie un à un pour vérifier si le mot de passe est valide. Bien évidemment, ces attaques ne se font pas à la main, mais avec des programmes qui peuvent deviner des centaines voire des milliers de mots de passe à la seconde. Ce procédé est d'autant plus facile, qu'il lui permet de tester des variations sur ces mots : mots écrits à l'envers, majuscules et minuscules dans le mot, ajout de chiffres à la fin du mot, etc..

6.4 Le sniffing des mots de passe et des paquets

Un hacker a d'autres outils pour obtenir le mot de passe si il na pas pu le deviner, la méthode la plus populaire est le sniffing de mots de passe. Chaque message (ou paquet) qu'un ordinateur transmet sur un réseau peut être lu par n'importe quel ordinateur situé sur le réseau ce qu'on appelle le broadcasting utilisé par la plus part des réseaux [6].

En pratique, tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message n'est pas destiné pour eux et vont donc l'ignorer. Mais par contre, beaucoup d'ordinateurs peuvent être programmés pour regarder chaque message qui traverse le réseau. Si une personne mal intentionnée fait ceci, alors elle pourra regarder les messages qui ne lui sont pas destinés.

Tous les messages qui circulent sur le réseau sont scannés par des hackers à l'aide des programmes qui utilise ce procédé tout en repérant les mots de passe. Une personne risque contre son gré de donner son mot de passe si quelqu'un se connecte sur un ordinateur à travers un réseau et que des ordinateurs ont été compromis par le procédé de sniffing.

Les personnes qui se connectent sur des ordinateurs distants (par exemple en utilisant Telnet) risquent une menace sérieuse. Toutefois, si quelqu'un se connecte sur la console d'un système (et non pas sur un terminal), son mot de passe ne circulera pas sur le réseau ou il pourrait faire l'objet d'un sniffing. Mais si une personne se connecte sur un autre réseau ou à partir d'un prestataire de service Internet, alors dans ce cas elle sera dépendante de la sécurité de ces réseaux. Les programmes de sniffing les plus connus sont :

- Esniff.c (programme source pour un sniffer ethernet).
- TCPDump

6.5 L'IP spoofing

On appelle l'adresse utilisée pour reconnaître un ordinateur sur Internet par l'adresse IP. Quand elle est certifiée par les services TCP et UDP on peut dire qu'elle est valide .Un des principaux problèmes est qu'en utilisant le routage source d'IP, l'ordinateur du hacker peut se faire croire comme étant un ordinateur connu [6].

le routage source d'IP utilisé pour spécifier une route directe à une destination et renvoyer le chemin de retour à l'expéditeur. pour faire suivre les paquets à la destination finale on utilise la route qui peut inclure l'utilisation d'autres routeurs ou de server qui n'auraient normalement pas été utilisés. Voici un exemple qui montre comment ceci peut être utilisé de telle façon que l'ordinateur de l'intrus apparaisse comme étant l'ordinateur certifié par le serveur :

- pour faire croire qu'il est un client certifié par le serveur l'agresseur change l'adresse IP de son ordinateur.
- Il va ensuite construire une route source jusqu'au serveur qui spécifiera le chemin de retour direct que les paquets IP devront prendre pour aller au serveur et qu'ils devront prendre pour retourner à l'ordinateur de l'agresseur en utilisant le client certifié comme dernière étape dans la route vers le serveur.
- en utilisant la route source , l'agresseur envoie une requête client au serveur.

- Le serveur accepte la requête du client comme si elle provenait directement du client certifié et retourne une réponse au client.
- Le client, fait suivre le paquet à l'ordinateur de l'agresseur en utilisant la route source.

Une autre manière encore plus simple pour spoofer un client est d'attendre que le système client ait éteint sa machine et de se faire passer ensuite passer pour ce dernier. Les employés dans beaucoup d'entreprises pour se connecter sur des serveurs locaux UNIX utilisent des PCs et des réseaux TCP/IP. Les PCs utilisent souvent NFS pour obtenir un accès aux répertoires et aux fichiers du serveur (NFS utilise les adresses IP uniquement pour authentifier les clients).

Les courriers électroniques sur Internet sont particulièrement sujets au spoofing car très facile à réaliser. Les courriers électroniques sans l'ajout d'une signature digitale ne peuvent pas être d'origine fiable.

D'autres services comme le Domain Name Service peuvent aussi être spoofés mais avec toutefois plus de difficultés que le courrier électronique. Ces services représentent une crainte qui mérite d'être considérée quand on les utilise.

6.6 Les chevaux de Troie

Quand la victime (l'utilisateur normal) lance ce programme, elle lance par la même le cheval de Troie caché car ce dernier c'est un programme qui se cache lui-même dans un autre programme pour éviter tout soupçon [6].

Il y a des exemples de chevaux de Troie UNIX sur l'Internet. Par exemple, en 1995, un serveur FTP bien connu a été pénétré et les agresseurs ont modifié un programme très populaire disponible sur ce site. Le cheval de Troie installé à l'intérieur du programme permettait quand il était exécuté d'ouvrir l'accès au système UNIX à n'importe qui.

Voici une petite explication de ce qui se produit pour l'établissement d'une connexion :

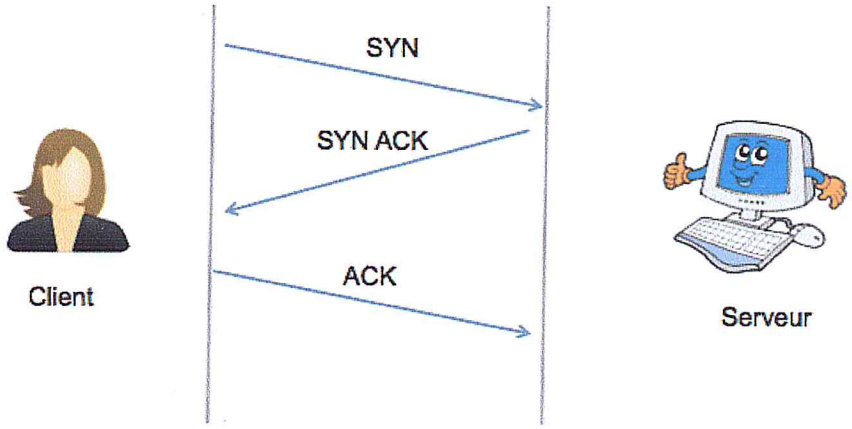


FIGURE I.2 – SYN ACK [7]

au moment où le serveur a renvoyé un accusé de réception du SYN (ACK-SYN) au client mais n'a pas reçu le ACK du client , les abus viennent. C'est alors une connexion à demi-ouverte. Le serveur construit dans sa mémoire système une structure de données décrivant toutes les connexions courantes. Cette structure de données est de taille finie, en créant intentionnellement trop de connexions partiellement ouvertes peut créer un dépassement de capacité (overflow).

7. conclusion

Il est impossible de construire des défenses solides tant que l'on ne sait pas contre quoi on se bat. C'est pour cela que la sécurité informatique est primordiale dans chaque système et donc beaucoup d'entreprises recrutent des spécialistes dans le domaine et dépensent beaucoup d'argent afin de se protéger.

Chapitre II

Les virus

1. Introduction

Une fois qu'un hacker s'introduit dans un système il voudra généralement d'y retourner quand il veut, prenons l'exemple d'un attaquant qui voudra accéder un site web une autre fois avec plus de facilité après l'avoir pénétré afin de l'utiliser pour des besoins bien spécifiques comme une rampe de lancement pour pénétrer d'autre systèmes après avoir mis tout ses fichier outils sur ce dernier. Donc il crée une porte dérobée (back-door) que lui et lui seul connaitra, donc c'est nécessaire pour lui de se procurer une voie d'accès pour cela il existe plusieurs techniques.

Grâce a la grande efficacité des Virus, ces derniers sont devenus très populaire car la majorité des utilisateurs quand ils ouvrent une pièce jointe a un e-mail ou lorsqu'ils téléchargent un logiciel depuis le web ignorent les dangers inhérents et pour mettre l'accent sur ce point faut se demandait "Quel serait le moyen rapide et simple qui permettrait à un attaquant de compromettre le plus de machines possible avec le minimum d'efforts ?" la réponse la plus convenable fut l'utilisation d'un programme original et attrayant possédant une interface graphique mais duquel serait dissimuler un programme mal veillant et l'envoyer aux plus grand nombre de personnes possible ou en utilisant des techniques de spread comme le JAVA DRIVE-BY.

Dans ce chapitre nous allons définir des généralités sur les virus ainsi que leurs

différents modes et techniques de propagation et modes d'infection.

2. Définition des virus

Les infections informatiques sont des programmes ou des sous-ensembles de programmes malveillants qui, à l'insu de l'utilisateur, sont destinées à perturber, à modifier ou à détruire tout ou partie des éléments indispensables au fonctionnement normal de l'ordinateur. On différencie les programmes simples et les programmes autoreproducteurs [8].

2.1 Virus de type infection (chevaux de troie, botnet..)

Dans son sens un virus offre a un pirate informatique d'y parvenir à ses fins, accéder aux informations, modifier, supprimer ,contrôler à distance sans oublier que certains types de ses dernier permettent a l'attaquant d'y avoir accès facilement et s'y introduire quand il veut [9].

2.2 Virus de type CPA (Code Parasite Autopropageable)

Se sont des programmes malveillants qui ont la particularité de s'autopropager et de détruire une cible bien définie. [9].

3. Typologies et classification :

Il existe plusieurs classifications de virus décrites dans ce qui suit [9] :

- **Virus mutants :**

  La plupart des nouveau virus sont un mélange ou clonage de plusieurs autres anciens mais avec plus de puissance, réécrit par d'autres utilisateurs pour avoir (leurs propre virus , ajouter des fonctionnalités tout ce résume à ne pas réinvente la roue ..) sachant que leurs comportement va changer ainsi leur signature ce qui rend leur détections plus difficile dans les conditions où les éditeurs d'antivirus

doivent ajouter ces nouvelles signatures à leurs bases de données.

- **Virus polymorphes :**

  Ce type de virus appelé virus polymorphes (mot provenant du grec signifiant la possibilité de prendre plusieurs formes). C'est des virus qui changent de signature a chaque exécution ça veut dire le changement de la clef du cryptage car ils sont dotés d'une fonction de chiffrement et déchiffrement à l'intérieur ainsi l'auto sauvegarde de la nouvelle forme, cette technique est appelée technique de camouflage.

- **Rétrovirus :**

  Appelé aussi virus flibustier (en anglais bounty hunter), dans la médecine c'est le genre de virus s'attaquent aux cellules après la suppression de la défense contrairement aux non rétroviraux dont le système immunitaires en charge, c'est le même principe dans l'informatique c'est un virus qui rend les signatures de l'antivirus inopérantes après les avoir modifiées.

- **Virus du secteur d'amorçage :**

  C'est tout virus qui s'exécute à chaque fois que le système démarre et cela après avoir infecté le secteur de démarrage d'un disque dur.

- **Virus trans-applicatifs (virus macros) :**

  Afin d'automatiser certaines taches efficacement un programme généralement court et simple on utilise une macro qui est une série de commandes et d'actions. Une fois crées, les macros doivent être exécutées par un système qui interprète les commandes emmagasinées. Il existe des systèmes macro qui sont des programmes autonomes, et d'autres on les trouve intégrés dans des applications complexes (par exemple pour les processeurs de mots) qui permet aux utilisateurs la répétition facile des séquences de commandes, ou bien pour les développeurs pour l'adaptation de l'application aux besoins Locaux. Microsoft a mis au point un langage de script commun pouvant être inséré dans la plu-

part des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic. Ces virus arrivent actuellement a' infecter les macros des documents Microsoft Office ou des attachements d'un e-mail.

4. Cycle de vie d'un virus

Les différents cycles de vie d'un virus sont présentés comme suit [10] :

- **Auto reproduction :**

  L'auto reproduction c'est la définition de tout programme qui a la capacité de se recopier lui-même sans intervention humaine, d'une façon systématique ou lorsque certaines circonstances ou conditions sont remplies.

- **Infection :**

  Lorsqu'un programme dupliqué se loge de manière illégitime dans certaines parties du système informatique on appelle ceci une Infection. Les cibles privilégiées sont 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), la mémoire centrale (ce n'est pas la seule cible car le virus ne se propagerait pas d'un ordinateur a' un autre, sauf à travers des réseaux, et disparaitrait à l'extinction de l'ordinateur) . Le programme viral contenant dans les instructions d'un ordinateur s'exécute lorsque l'ordinateur tentera d'exécuter ces instructions.

- **Activation :**

  Si certaines conditions sont réunies l'activation du virus se produira ou plus exactement celle de sa (ou de ses) fonction(s) pathogène(s) prenons l'exemple lors du lancement du virus, ou bien lors d'un double clic ou toute autre conjonction arbitraire de conditions.

- **Alteration :**

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

partiellement le contrôle du fonctionnement de l'ordinateur pour lui faire accomplir des actions diverses. Par exemple certains anciens virus pouvaient faire tomber les lettres en cascade de leur position normale sur l'écran vers les lignes du bas, afficher un message inattendu et ralentir fortement le fonctionnement de l'ordinateur. Très vite les virus sont devenus beaucoup plus pervers la plupart d'eux altèrent d'une manière étendue les fichiers enregistres sur les mémoires de masse contaminées.

5. Modes d'infection

Le processus d'infection d'un virus consiste à identifier l'exécutable cible et à intégrer dans son code binaire une copie du virus à la fin du processus d'infection d'un virus on aura un mélange du fichier exécutable original et du virus. On trouve quatre familles de virus qui définissent quatre modes d'infection d'un fichier exécutable [11].

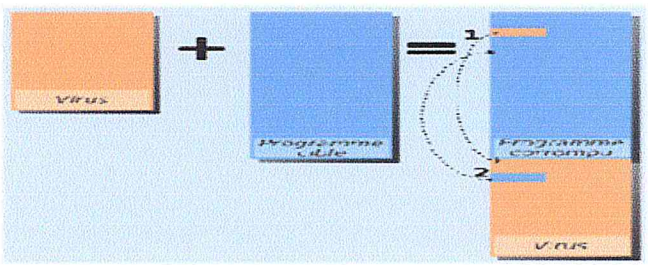


FIGURE II.1 – Infection par écrasement [11].

Un mode utilisé par de petits virus qui consiste sur le remplacement du code des fichiers exécutables cibles par le propre code du virus pour cela il existe trois situations [11] :

- Le programme infecté ne se lance pas ce qui attire l'attention de l'utilisateur on l'appelle mode d'infection viral car le virus écrase la partie initiale du code de la cible.
- Le programme infecté peut ne plus être fonctionnel car le virus écrase la partie centrale ou finale du code de la cible en écrivant une fonction de saut vers la zone de son propre code dans l'en-tête du programme cible ce qui provoque

l'exécution du virus une fois le programme est lancé puis redonnera la priorité au déroulement normal du programme.

– La taille des fichiers infectés est identique car la furtivité est nulle a cause du remplacement intégral du code du programme cible par le propre code du virus.

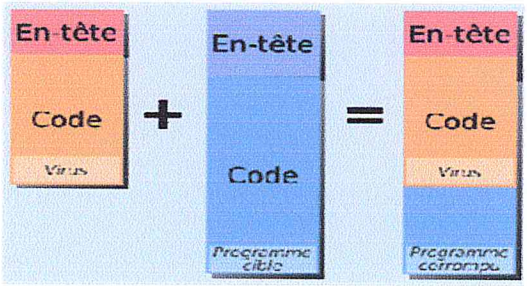


FIGURE II.2 – Recouvrement de code [11].

Le virus ajoute son code à celui du programme soit a l'en-tête (prepend consiste) en modifiant les adresses d'appel des fonctions et des données du programme cible ou bien a la fin code du programme cible (appelée append consiste) cette technique de recouvrement consiste a placer dans l'en-tête du programme cible une fonction de saut permettant d'exécuter le virus en premier, et de transférer ensuite le contrôle au programme infecté.

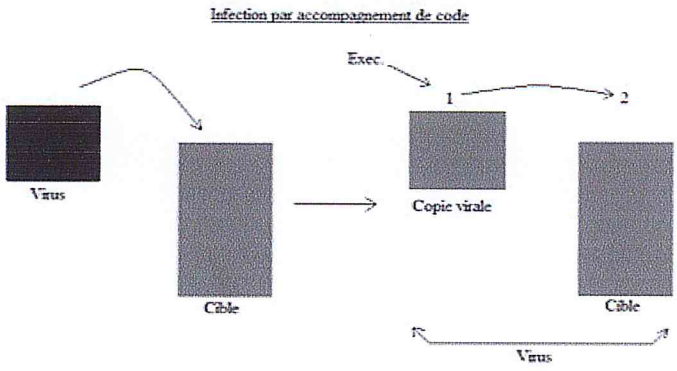


FIGURE II.3 – Virus par accompagnement de code.

Son principe consiste à repérer un fichier cible il se copie dans un fichier supplémentaire qu'il a crée auparavant sur le disque et qui va accompagné le programme cible. Alors le

programme cible n'est pas modifié et son intégrité est respectée et lorsque l'utilisateur exécute le programme cible, le virus contenu dans le fichier compagnon est exécuté en premier lieu, ensuite le virus exécute lui-même le programme cible qu'il accompagne.

plusieurs techniques sont envisageables, pour pouvoir parvenir à ce résultat [11] :

- La première technique est celle de l'exécution préemptive.
- La deuxième technique s'appuie sur la hiérarchisation des chemins de recherche des exécutables.
- La troisième technique consiste à renommer le programme cible

6. Détection d'infection virale

C'est quoi un Antivirus ? Comment fonctionne t il ? Pourquoi un Antivirus ?

En identifiant, neutralisant et éliminant des logiciels malveillants afin de sécuriser les ordinateurs et préserver l'intégrité de ses données, qui peuvent être importante [12].

6.1 Aspects techniques des Antivirus

Ce n'est pas toujours facile de localiser et combattre un virus pour cela les antivirus utilisent plusieurs techniques dans leur combats.

6.2 Principales techniques de recherche virus

Il existe plusieurs techniques pour la localisation d'un virus les plus souvent utilisées par les antivirus sont les suivantes (brièvement présenté) [12] :

1. **Le scanning de comportement :** surveille les actions menées par les virus.
2. **les contrôleurs d'intégrité :** signalent les changements intervenus dans les fichiers.
3. **la recherche heuristique :** recherche des instructions généralement utilisées par les virus.

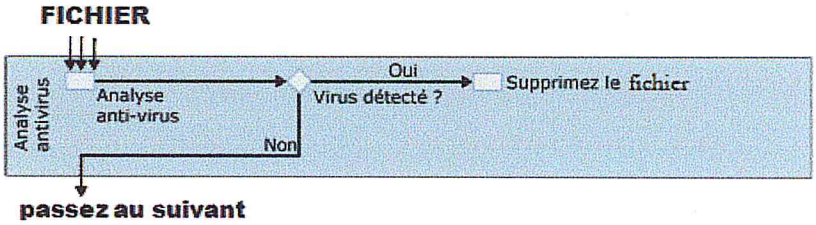


FIGURE II.4 – Technique de recherche des virus.

6.3 Recherche de la signature (SCANNING)

Repose sur la détection des virus avant leur exécution en mémoire pour cela il faut que L'Antivirus ait déjà été confronté au virus en question et l'ait intégré à une base de données. Donc le principe d'un scanneur est de rechercher sur le disque dur toute chaîne de caractères identifiés comme appartenant à un virus. Un scanneur n'est donc pas en mesure de détecter les nouveaux virus ou les virus polymorphes mais cette méthode est plus longue a mettre en œuvre car elle n'est utile que si elle recense tous les virus existant [13].

6.4 Utilisation d'un contrôleur d'intégrité

Consiste sur la construction d'un fichier avec les noms de tous les fichiers qui sont sur le disque dur en prenant en compte leurs caractéristiques différents comme la taille , la date et 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 en recalculant le checksum à chaque démarrage de l'ordinateur(si Antivirus n'est pas résident), il pourra détecter toute modification ou altération des fichiers 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 est donc informé [13].

D'autre part Antivirus stocke dans une base de données la date et la taille de chaque fichier exécutable et tester les modifications éventuelles au cours du temps.

6.5 Moniteur de comportement

Repose sur l'observation d'ordinateur pour prévenir l'utilisateur en cas d'activité de type virale ce moniteur est un programme qui reste actif et qui réside que l'utilisateur charge à partir du fichier AUTOEXEC.BAT [13].

6.6 Démarche heuristique

L'analyse heuristique est comme le scanning, passive. Elle considère le code comme une simple donnée, et n'autorise jamais son exécution. Mais contrairement au scanning elle peut détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

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

L'analyse heuristique permet aux virus polymorphes de chercher une routine de déchiffrement qui consiste a parcourir le code puis la modifiée , dans ce cas l'Antivirus cherche une suite d'instructions de lecture suivie d'une suite d'instructions d'écriture [14].

6.7 Analyse spectrale

Il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code et Tout code généré automatiquement est supposé contenir des signes révélateurs du compilateur utilisé. C'est grâce à ce principe qu'entre en jeu l'analyse spectrale qui vise à repérer les virus polymorphes qui sont indétectables autrement car leur signature changeant à chaque réplication.

En effet, la séquence en résultant contient certaines associations d'instructions que l'on ne trouve pas en temps normal lorsqu'un virus polymorphe crypte son code, c'est ce que va détecter l'analyse spectrale [14].

6.8 Technique d'éradication de virus

Que ce soit en mémoire ou sur le disque dur, une fois un virus est détecté, il est obligatoire de le supprimer, la suppression des virus est donc une fonction primordiale des Antivirus car ces derniers ont pour but de prévenir l'utilisateur de ce programme malveillant. Mais cela peut être impossible comme le cas des virus avec recouvrement qui détruisent une partie du programme sain lors de sa duplication pour remédier on a une solution unique qui est bien la le formatage du disque dur ou la destruction des fichiers infectés [14].

Pour d'autres il faut connaitre la localisation exacte du virus dans le fichier et c'est très ardue sachant que ce virus peut composé de plusieurs parties, ensuite il faut le supprimer, et enfin aller chercher la partie du programme dont le virus avait pris la place et la restaurer et toutes caractéristiques des différents virus doivent être Répertoriées dans une base de données mise à jour quotidiennement.

7. Conclusion

Nous avons aussi mis en exergue le fait que Windows soit le système d'exploitation le plus touché par les vers, mais avec l'expansion que connait Linux et aussi le fait que ses nouveaux utilisateurs soient de moins en moins expérimentés il est a prévoir que ce système d'exploitation soit de plus en plus la victime d'attaques cybernétique, bien qu'a l'heure actuelle cette menace est très faible comparé a l'autre OS.

On peut dire sans crainte alors que la batailles entre les créateurs d'anti virus et de virus n'est pas prête de s'arrêter bien que l'avantage est pour l'instant aux créateurs des virus qui innove a chaque fois et aussi parce qu'un virus est fait à la base pour passer indétecté.

Chapitre III

La cryptographie

1. Introduction

La cryptographie qui est devenue une science a part-entière et une partie importante de la technologie de l'information en même temps , qui consiste à chiffrer, coder des messages pour maintenir le secret de ses dernier et donner une certaine confiance à ceux dont l'anonymat est primordiale, littéralement cette science qui a eu un enjeu majeur dans les guerres d'espionnage depuis la nuit des temps a été bien éloignes des préoccupations du grand publique généralement et des scientifiques spécialement , mais avec l'évolution et l'envie que la vie privé ne soit pas tellement exposer l'envie de s'y mettre dedans a pris de l'ampleur.

"Ce qu'on appelle notre vie privée, c'est ce dont nous avons le droit de priver les autres. " Gilles Martin-Chauffier

2. Définition générale

D'après Jaques Stern [15], la cryptologie ou la science de messages secrets qu'on a fait remonter a césar ou parfois même auparavant. Elle est mieux représente par la trilogie fondamentale de la cryptologie :

- **Intégrité :** c'est de s'assurer qu'un message ou bien le fichier qu'on vient de recevoir n'a pas subi de modification, bien souvent des modifications malveillantes

que des modifications due au hasard.

- **Authenticité :** C'est généralement un procédé qui définit et prouve l'origine (l'identité) d'un message.
- **Confidentialité :** ce qu'on a tendance à décrire comme le cœur de la cryptologie qui consiste par exemple a envoyé un message dans un chemin non sécurisé sans qu'un tiers malveillant ne puisse accéder au vrai contenu.

3. Aperçu historique

Un petit aperçu historique, les trois ages de la cryptologie sont [15] :

- L'âge artisanal : jusqu'en 1918.
- L'âge technique : de 1919 a 1975
- L'âge paradoxal : de 1976 a nos jours

3.1 L'âge artisanal

C'est l'âge des substitutions (changer une lettre par une autre) et permutation, l'âge des cadrant et des cylindres ou chiffrement série qui est utiliser jusqu'à nos jours.

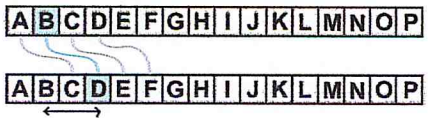


FIGURE III.1 – Chiffrement de César [16].

3.2 L'âge technique

C'est en utilisant des principes mécano électrique en général comme enigma lors de la seconde guerre mondiale, cet âge Se termine lors de la création de l'informatique.

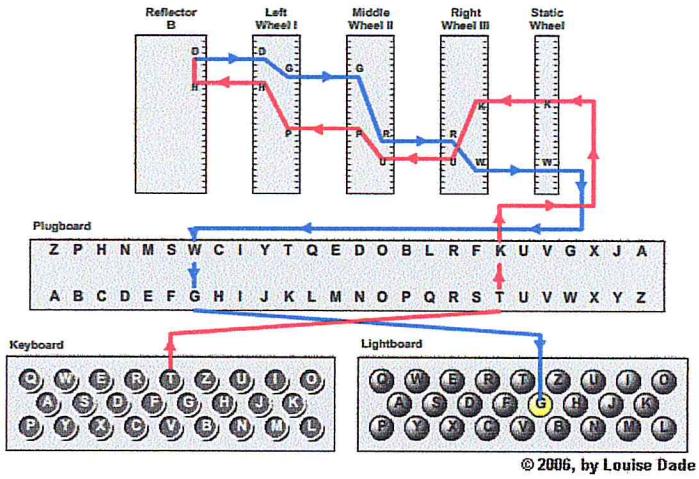


FIGURE III.2 – Machine enigma [17].

3.3 L'âge paradoxal

- Cryptographie à clé secrète(symétrique)

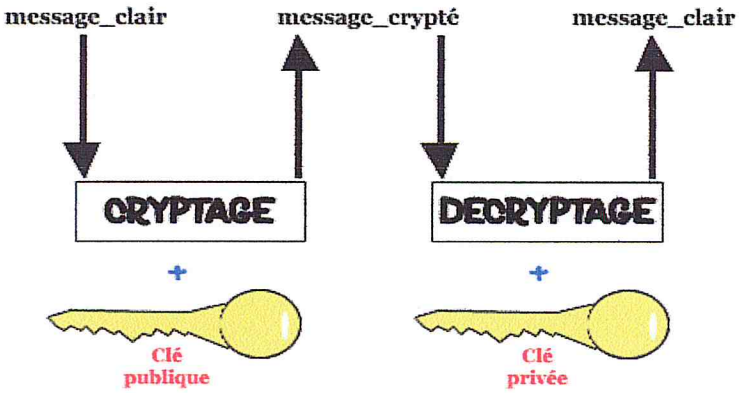


FIGURE III.3 – Cryptographie à clé secrète [18].

- Cryptographie à clé publique(asymétrique)

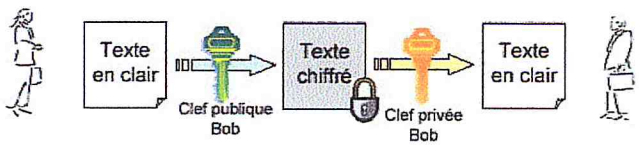


FIGURE III.4 – Cryptographie à clé publique [19].

4. La cryptographie symétrique et asymétrique

4.1 Le cryptage symétrique

Le cryptage symétrique est la technique la plus ancienne et la plus connue. A l'aide d'une clef qu'on appelle clef secrète qui peut être une suite de caractères ou des numéros l'essentiel c'est quelque chose qui nous guideras à avoir le message d'origine, est appliquée au texte d'un message pour modifier le contenu d'une certaine manière. Cela pourrait être aussi simple que de décaler chaque lettre d'un certain nombre d'emplacements dans l'alphabet. Tant que l'expéditeur et le destinataire connaissent la clé secrète, ils peuvent crypter et décrypter tous les messages qui utilisent cette clé [20].

4.2 Le cryptage asymétrique

La notion d'asymétrie [21] dans la cryptographie est apparue en 1976 lorsque deux cryptologues américains Whitfield Diffie et Martin Hellman ont publié un article mettant en œuvre le principe d'asymétrie en cryptologie.

Leur principe repose sur le fait qu'il n y pas nécessité, pour que tout se passe bien, que la clé de chiffrement soit la même que pour le déchiffrement.

De plus, les deux cryptologues ont constaté que, pour la protection de données en confidentialité par exemple, le chiffrement d'un message pourrait être effectué par tous alors que le déchiffrement devrait être effectué seulement par le destinataire du message.

L'intérêt de l'asymétrie serait alors que la clé de chiffrement pourrait être rendue publique, donc utilisable par tous ceux qui voudraient chiffrer un message, on parle alors de clé publique, alors que la clé de déchiffrement serait propre au destinataire, on parle de clé privée.

L'idée de Diffie et Hellman est alors apparue comme une petite révolution dans le

monde de la cryptographie et il restait maintenant à trouver les outils mathématiques adéquats, des problèmes mathématiques dont la solution serait extrêmement difficile à trouver, et ce, par les ordinateurs les plus puissants au monde.

5. Avantages et inconvénients de la cryptographie

Les différents avantages et inconvénients du cryptage symétrique et asymétrique sont les suivants [22] :

5.1 Cryptage symétrique

Avantages

- Impossibilité de substitution du destinataire : clef privée connue de lui seul.
- Aucun transfert de clef privée : confidentialité assurée
- Un seul couple de clés pour plusieurs expéditeurs

Inconvénients

- Complexe.
- Requiert beaucoup d'opérations, donc peu recommandé pour transférer de grandes quantités de données.
- Authentification incertaine de l'expéditeur.

5.2 Cryptage asymétrique

Avantages

- Impossibilité de substitution du destinataire : clé privée connue de lui seul.
- Aucun transfert de clé privée : confidentialité assurée.
- Un seul couple de clés pour plusieurs expéditeurs.

Inconvénients

- Sa complexité.
- Elle requiert beaucoup d'opérations, donc peu recommandé pour transférer de grandes quantités de données.
- Authentification incertaine de l'expéditeur.

6. Différents logiciels pour le cryptage

Il existe plusieurs logiciels aujourd'hui pour le cryptage, parmis lesquelles on peut citer :

- Private Disk Light
- AxCrypter
- Crypt3
- PenProtect
- dm-crypt
- GnuPG

7. Conclusion

Cette science ne s'arrêtera jamais car elle est devenue primordiale et ses chercheurs dits les cryptographes essayent toujours de trouver une nouvelle méthodes pour de l'argent comme pour de la gloire ou juste pour l'anonymat comme les crypto-anarchiste le font dans les réseaux tor, I2p et qu'ils n'ont pas cessé de faire évoluer cette science qui est la cryptographie.

Chapitre IV

Techniques de propagation des virus et Cryptovirologie

1. Introduction

Afin de prendre en main les virus on devrait parler absolument de quelques techniques d'infection utilisées par les pirates informatiques spécialisés dans la virologie afin d'infecter leurs cibles visées ou juste pour avoir une armée de zombies et théoriquement c'est quoi cette technique qui contourne la sécurité pour laquelle les gens payent cher. C'est dans cette optique que j ai choisit ce thème afin d'obtenir le diplôme de fin de cycle, alors dans se chapitre on va parler des techniques de propagation des virus et de la cryptovirologie d'un coté théorique.

2. Techniques de propagation des virus

On croise beaucoup de gens sur la toile du net qui se posent la question comment peut on être infectés juste en accédant a un site web ou un e-mail, un torrent,etc. C'est bizarre car on a rien fait à par accéder à un site à l'apparence inoffensif, on va maintenant donner quelques exemple de techniques de propagations via le web (Web Spread)

2.1 Java drive-by

Comme tout types d'attaques via le web on a pas un accès direct ou physique à la machine de la victime, mais ce type d'attaque n'a pas besoin d'une faille dans le moteur de recherche, juste un petit plugin particulier et vulnérable et un peu de social engineering pour inciter la victime à accéder à la page en question, en totalité on a besoin d'un pack special, ce dernier contient :

- Un nom de domaine + hébergement web, il vaut mieux qu'ils soient payant question de crédibilité, uploader la totalité des fichier suivants

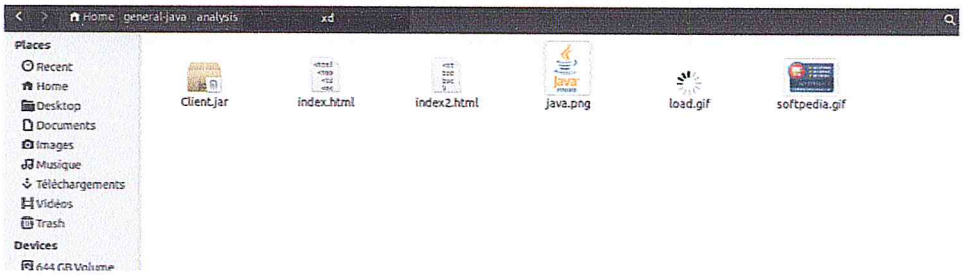


FIGURE IV.1 – Java drive-by pack.

- le fameux fichier ,jar coder spécialement pour sa
- Deux interface web :
  - la première qui est une fausse page avec des éléments qui doivent attirer l'attention de la victime et la rassurer.

FIGURE IV.2 – Softpedia

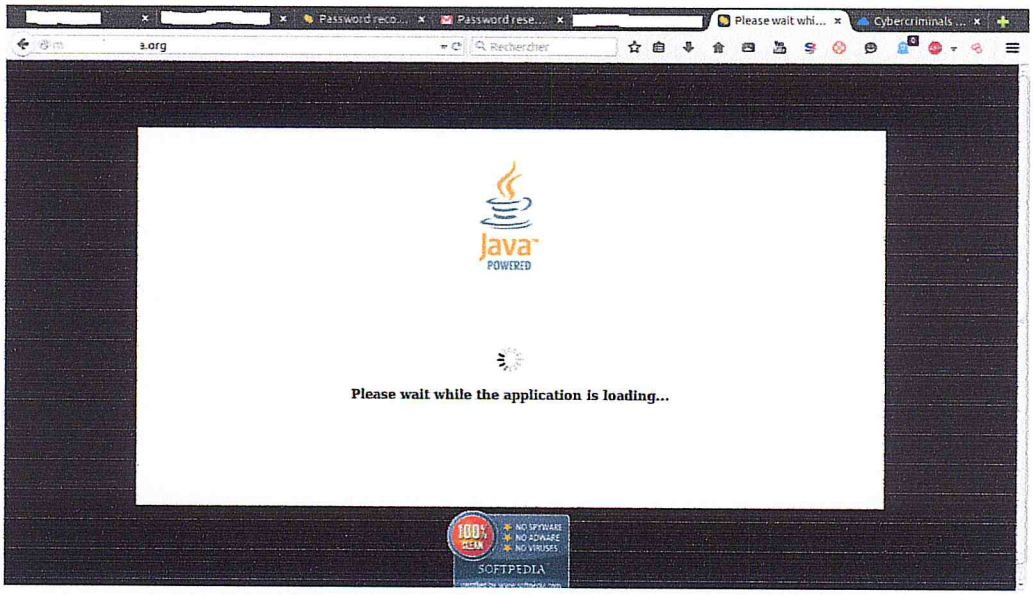


FIGURE IV.3 – Java drive-by 1.

- Après une redirection vers notre 2 ème page ou il faut remplacer *YOUR URL HERE* par l'emplacement de votre virus *.exe* pour qu'il soit exécuté.

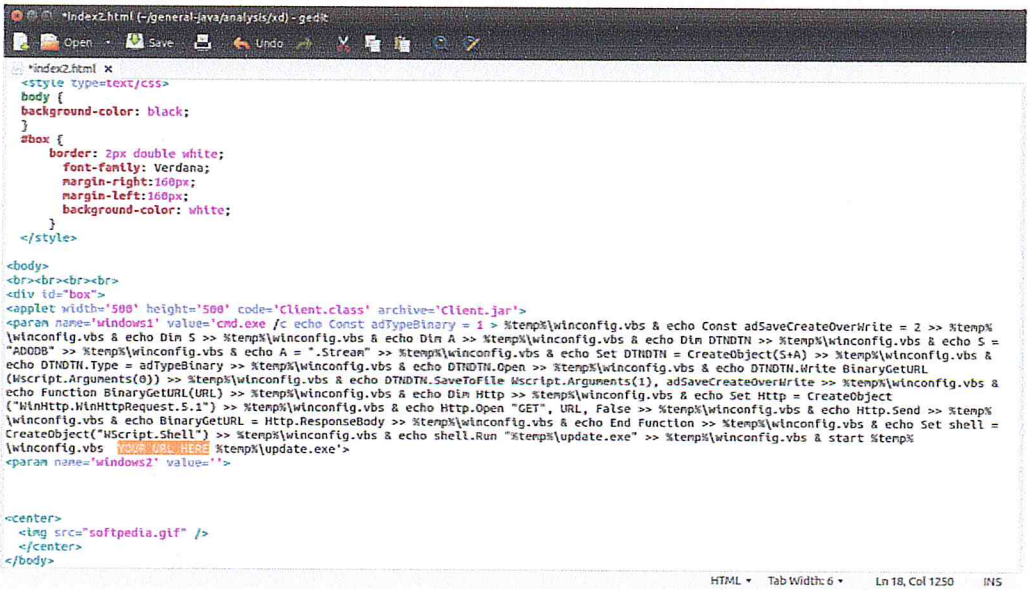


FIGURE IV.4 – Java drive-by 2.

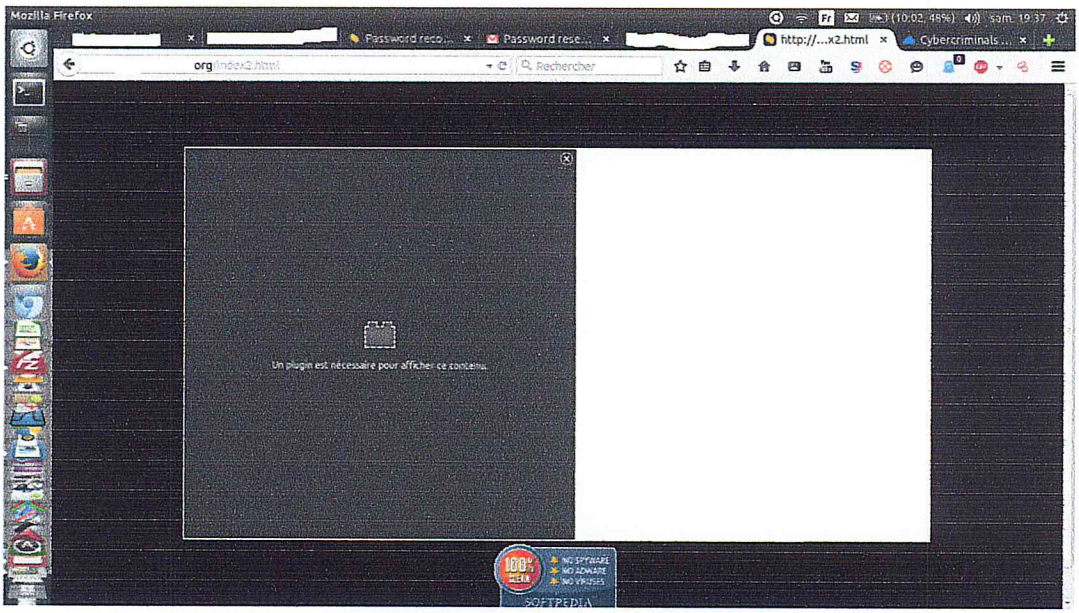


FIGURE IV.5 – Java drive-by 2.

Dans cette étape il suffit que la victime clique sur la partie ou il est écrit "un plugin est nécessaire pour afficher le contenu"

2.2 Infection par exploits

Dans son origine un exploit n'a pas été utilisé pour propager des programmes malveillants sur le net, mais aujourd'hui, il est l'un des plus efficaces , mais aussi une des méthodes les plus chére c'est ce qu'on appelle *0-Day* exploits qu'on peut trouver dans des sites comme *www.mitnicksecurity.com* qui est le site officiel de kevin Mitnik et le prix minimal d'un exploit dit premium est de 100,000 $.

Cependant , la diffusion par d'exploits peuvent être très très réussies, mais aussi peut avoir très très peu de succès . Il y a beaucoup d'entreprises qui mettent à niveau (à jour) leurs programmes comme Adobe Reader.

Utilisation :

Comme on l'a déjà dis, l'exploitation peut être très facile. Vous n'avez qu'à envoyer votre esclave à une adresse web spécifique qui correspond aux exigence de l'exploit. Ceci est un grand avantage. Mais cela ne fonctionnera pas à chaque fois. Pour mettre en place notre propre exploit paquet y a des sites comme *0days* ou *exploiter-DB* et faire la recherche de quelque chose comme lecteur Adobe. Voir le code source et d'apprendre à l'utiliser. Quand c'est déjà fait, il est temps de préparer votre exploit-kit, vous pouvez prendre une qui est publique donc pas 0-day et de le modifier ou vous pouvez faire votre propre exploit, ou acheté-en un.

3. Propagation par réseaux

3.1 P2p spread

Voici une image qui explique bien le fonctionnement du P2P.

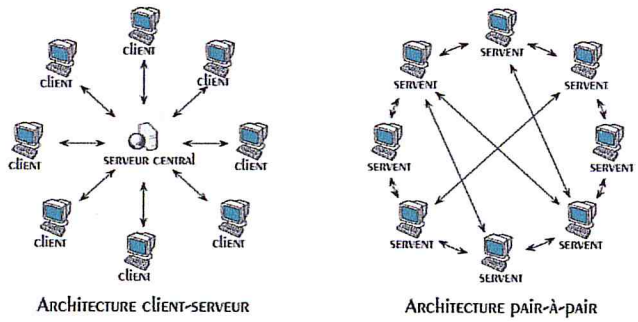


FIGURE IV.6 – P2P [23]

On va expliquer dans cette étape deux techniques différentes de propagation via p2p :

1. on va utilisé un filenamer, qui va simplement renommer notre serveur.

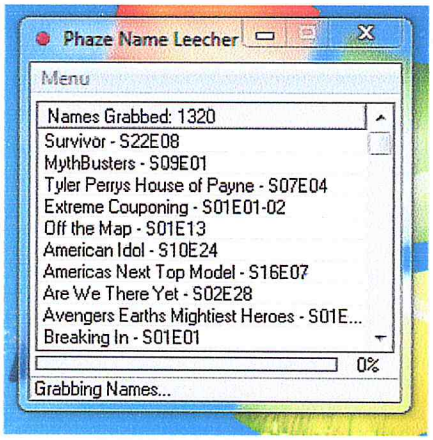


FIGURE IV.7 – Filenamer

On attend d'avoir 12K environ de names, puis on clique sur menu, start copy, sélectionner votre rat, puis créer un dossier et sauvez le tout dans un dossier. On va le voir ce remplir avec votre serveur en 12K fois. Il nous faut un client P2P, n'importe le quel feras l'affaire. On va utiliser ApexDC++, on clique sur Shares dans le menu settings qui s'ouvre a la fin de l'installation :

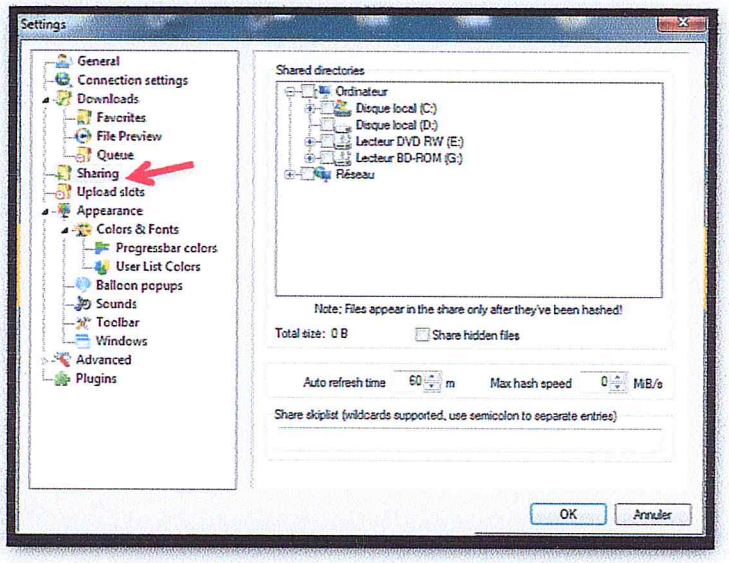


FIGURE IV.8 – ApexDC++ 1.

puis on sélectionne le chemin du dossier que nous avons créer dans l'onglet général on met un pseudo et définir une vitesse de transfert : vous devez peut

être ouvrir les ports dans votre routeur dans mon cas c'est RDP avec VPN donc pas besoin.

Maintenant que tout est configuré, partageons.

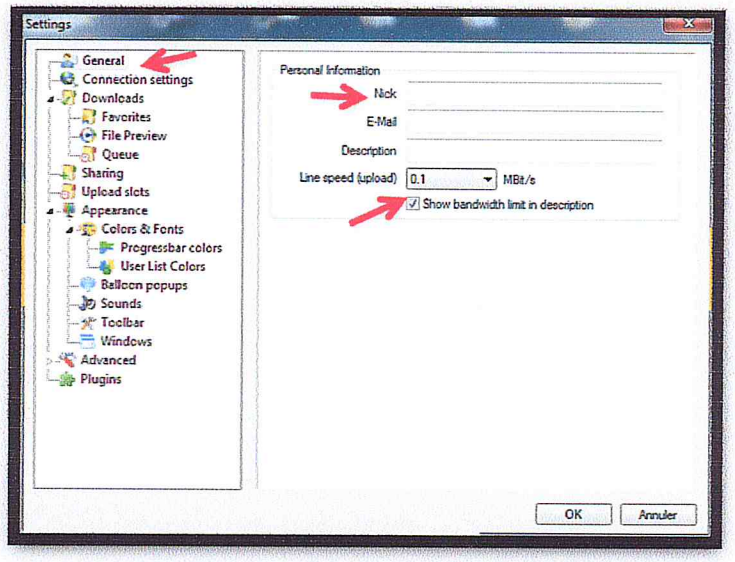


FIGURE IV.9 – ApexDC++ 2.

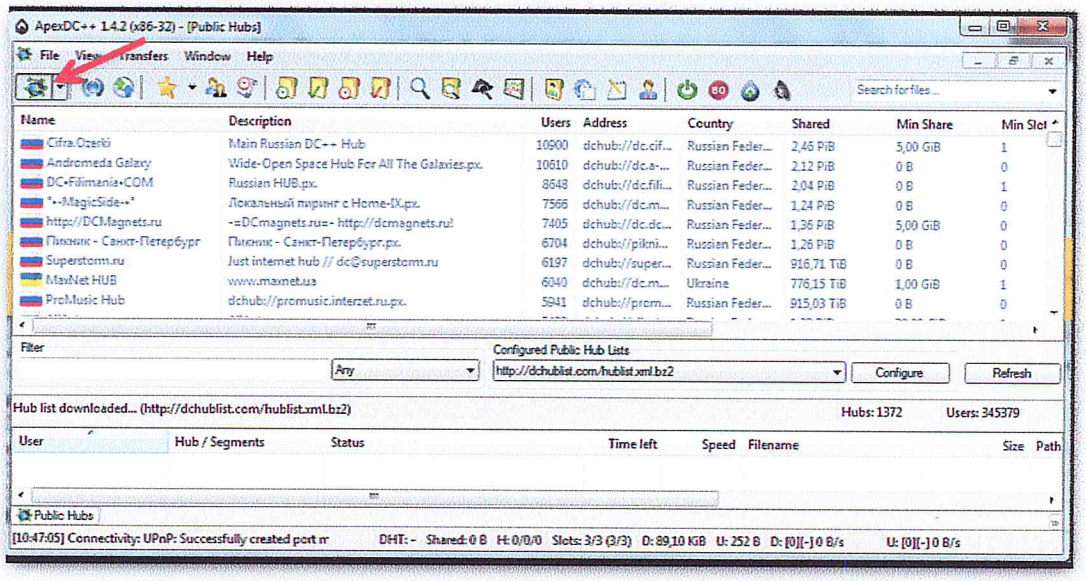


FIGURE IV.10 – ApexDC++ 3.

Un clic sur "public hub", maintenant on a plus qu'a attendre et laissez les autres télécharger nos fichier.

2. Sinon y a une autre technique, il suffit de télécharger un film on le met dans un dossier en lui ajoutant notre virus sous format jpg avec le nom de *description.jpg* et on crée un fichier torrent et l'upoader dans un des sites comme :

   - www.t411.io
   - frenchtorrentdb.com
   - rutracker.org

4. Cryptovirologie

On a parlé dans la précédente partie quelques techniques de propagations des virus et et d'infection mais la question qui les gens se posent c'est, pour quoi mon antivirus ne me protège pas ? Qu'est ce que les pirates informatique qui se sont spécialisent dans la virologie font pour contourner cette sécurité dans un marché plein de concurrence à coup de milliards ?

Une des techniques utilisées c'est la cryptovirologie, c'est quoi ce domaine ?

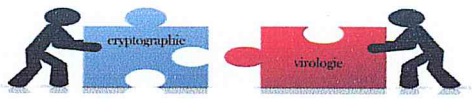


FIGURE IV.11 – Cryptographie + virologie

- Cryptage : science du secret ou science de protection d'informations.
- Virologie : science qui traite et manipule le phénomène des infections informatique.
- Virus : programme informatique qui utilise une technique spécifique pour prendre le contrôle du système qui ont comme option la spécificité de propagation rapide.

Donc la cryptovirologie est une science développez principalement par des chercheurs (Blackhat) qui et une association entre la virologie et cryptographie dans le but de découvrir des failles et des techniques afin d'être utiliser pour contourner la sécurité des host (par-feu,antivirus etc.) en général dans le but d'obtenir les informations voulu ou d'avoir accès complet qui est appelé (root), amélioration de la furtivité des virus , avoir un contrôle plus précis des virus.

Sous windows elle est implémenté à l'aide de cryptography API de Microsoft (CAPI) qui peut être appliqué sur différents formats .exe .vbs ...

Les principales techniques utilisées dans la cryptovirologie sont :

- Technique mystification dans le code source comme les fake-functions.
- Technique de camouflage en utilisant des fonctions qu'on appelle junk-code.
- Modifications des variables.
- Utiliser le camouflage et faire appel à nos fonctions depuis d'autres classes.

Dans le marché, il existe plusieurs crypter dont les prix diffèrent des uns aux autres, comme montré dans la figure ci-dessous :

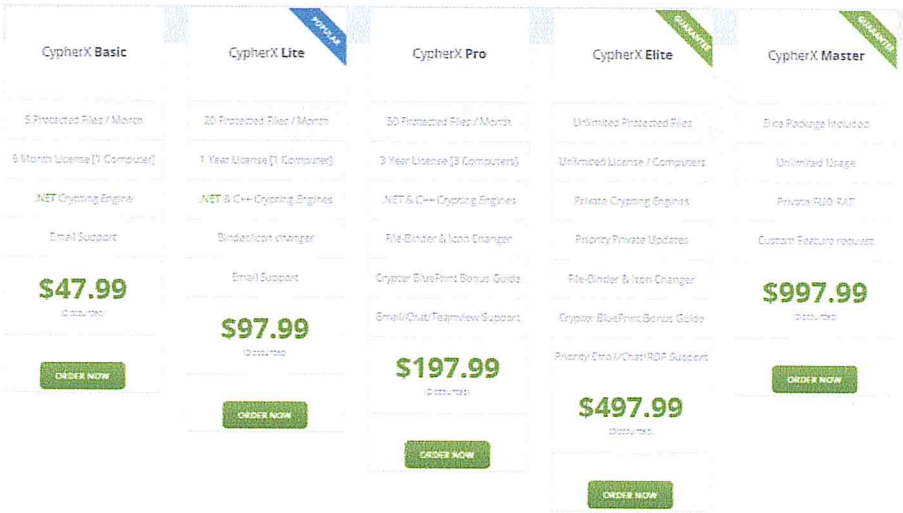


FIGURE IV.12 – Les différents crypters et leur prix [24]

Chapitre V

Technique de cryptage et détection des virus cryptés

1. Introduction

Une grande partie de mon travail a été consacrée a trouver un moyen pour contourner la sécurité des antivirus en utilisant des manipulation qui reste inconnue du grand public ,ce dernier qui pense être a l'abri de tout danger avec son antivirus c'est dans se conteste se résume le travail sans oublier d'opter pour une manière de détection afin d'y remédier a cette dernière.

2. Principe de fonctionnement

Dans le domaine de la cryptovirologie il existe 2 types de crypter :

- Crypter Runtime.
- Crypter Scantime

2.1 Le Runtime

Lorsque le virus sera exécuter le Cryptage FUD (Fully UnDetectable) Runtime va rendre ce virus indétectable. Le décryptage en mémoire du .exe crypté se fait dans le même processus que le stub ou il va être injecté et exécuté et il sera indétectable par

l'antivirus.

2.2 Le Scantime

Lors d'un scan d'un antivirus par exemple, le FUD Scantime permet de rendre virus indétectable.

2.2.1 Crypter Scantime

Cette technique consiste à chiffrer le virus en d'autres termes le chiffrement du *.exe* et tout le code contenant qui va devenir une suite de différents caractères sélectionnés au hasard cela est remarquable une fois ouvrir le *.exe* avec un éditeur.

Le virus chiffré n'est plus considéré comme un programme, car il sera considéré par Windows et par l'anti-virus comme une suite de caractère aléatoire.

Il existe plusieurs méthodes de chiffrement : Rc4, Base64, AES etc...

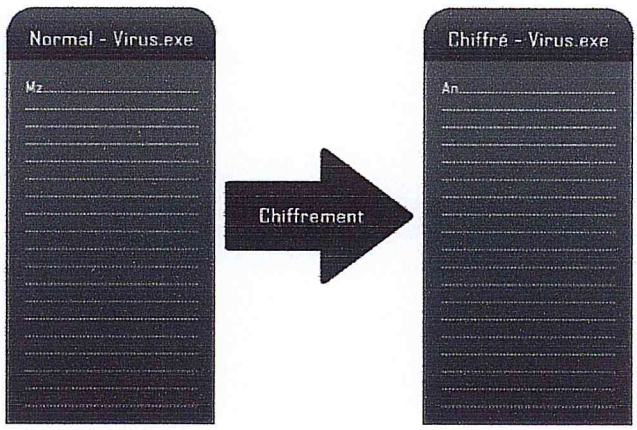


FIGURE V.1 – Binary to text.

Une fois le virus est chiffré, pour le lancer faut le déchiffrer cela se fait laide d'un stub qui va simplement lire le *.exe* du virus chiffré et le déchiffrer en créant un nouveau *.exe* (du virus déchiffré). A la fin il le lancera.

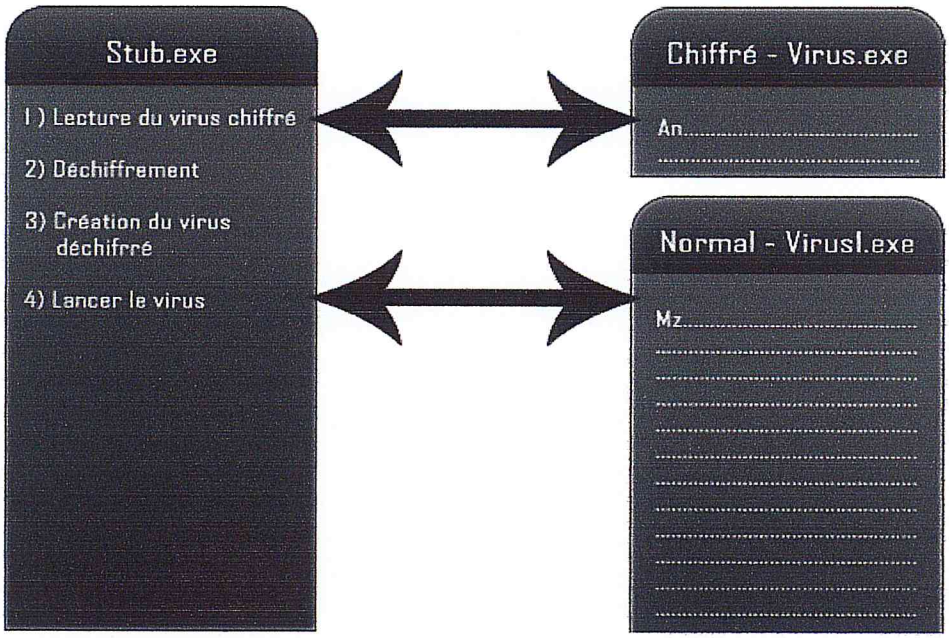


FIGURE V.2 – Stub.

Dans ce cas il faut envoyer 2 fichiers à la victime. le *stub.exe* et le *virus.exe* chiffré mais il existe un meilleur choix c'est de cacher le virus chiffré a la fin du *stub.exe*. Cette opération ne va pas altérer le fonctionnement de ce dernier.

Ensuite le stub va s'auto-lire et chercher le virus chiffré à la fin de son .exe. La suite reste ne change pas ,On auras plus qu'un fichier qui sera notre virus crypté.

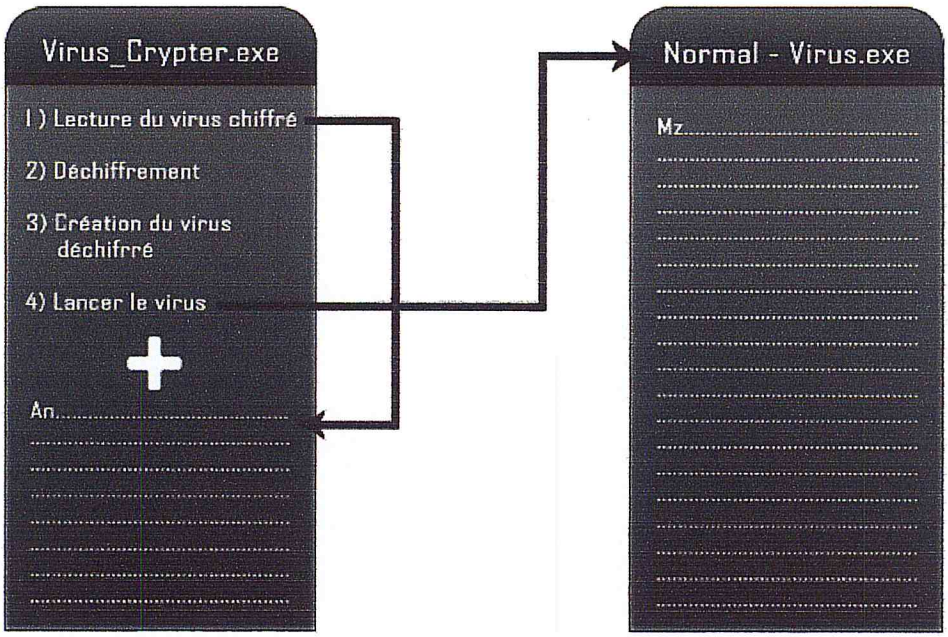


FIGURE V.3 – Virus crypté.

Afin d'automatiser le tous il faut utiliser le Builder qui va lire le virus et le chiffrer puis lire le stub en plaçant le virus crypté à la suite du stub pour créer le virus crypté.

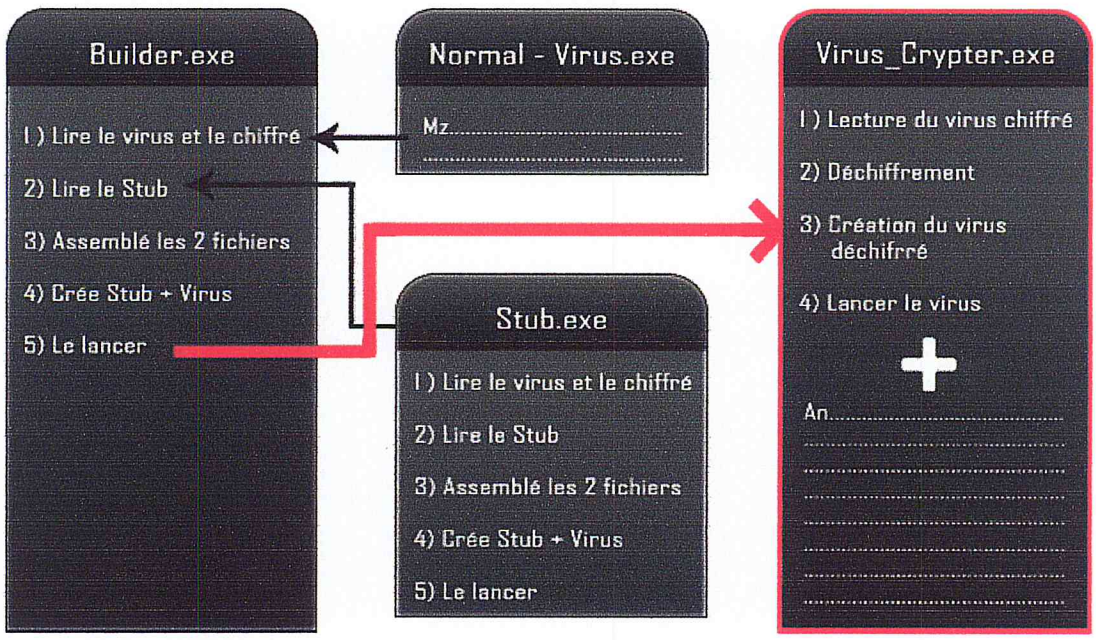


FIGURE V.4 – Pack complet de cryptage.

Après il faut essayer d'avoir un crypter FUD (complètement indétectable) c'est-à-dire qu'aucun anti-virus ne le détecte comme un virus cela se fait en modifiant le stub et en utilisant d'autre techniques de codage ou en changeant les noms des variables et des fonctions, encoder le tout, faire un RunPE unique etc...

3. Persistance Mode

3.1 Schtasks create

Schtasks [25] utilise différentes combinaisons de paramètres pour chaque type de planification. Pour afficher la syntaxe combinée pour la création de tâches ou pour afficher la syntaxe de création d'une tâche avec un type de planification particulier. Plus précisément planification minute.

Syntaxe de planification :

```
schtasks /create /tn <TaskName>/TR <TaskRun>/SC minute [/mo {1-1439}] [/st <HH:MM>]
[/sd <StartDate>] [/ed <EndDate>] [{/et <HH:MM>| /du <HHHH:MM>} [/ k]] [/it] [/ru
{[<Domain> \] <User>[/rp <Password>] | Système}] [/ s <Computer>[/u [<Domain> \]
<User>[/p <Password>]]]
```

FIGURE V.5 – Schtasks create. [25]

Dans une planification minute, le paramètre /sc minute est obligatoire. Le paramètre /mo (modificateur) est facultatif et spécifie le nombre de minutes entre chaque exécution de la tâche. La valeur par défaut de /mo est 1 (toutes les minutes). Le SD (heure de fin) et les paramètres de /du (durée) sont facultatifs et peuvent être utilisés avec ou sans le paramètre /k. Pour l'exécution chaque 10 min on auras schtasks /create /sc minute /mo 10 /tn « Script de sécurité » /tr

4. File joiner

Dans le Net on peut trouver plusieurs logiciel pour joindre des fichier avec le même format (Mp3,Avi,Txt..). Mais non pas un fichier exe avec un autre du même format ou un fichier .Txt avec un .exe.

Donc dans cette partie nous allons joindre 2 fichier avec un format diffèrent afin de nous donner 1 seul fichier qui sera exécuté dans le « Temp » sans oublier que la victime ne verra que le fichier .Txt s'afficher et le virus prendre contrôle de la machine.

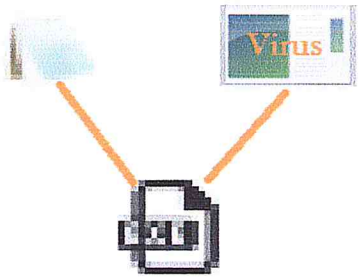


FIGURE V.6 – Filejoiner

5. Détection d'infection

Un Virus Mode infection a besoin d'envoyer des informations vers la destinations de son générateur (trojan generator), donc il va utiliser le réseau internet pour cela. Une méthode qui est assez connue dans le monde du Malware Analytique c'est d'utiliser un outille qui s'appelle wireshark afin d'intercepter tout les paquets entrants et sortants.

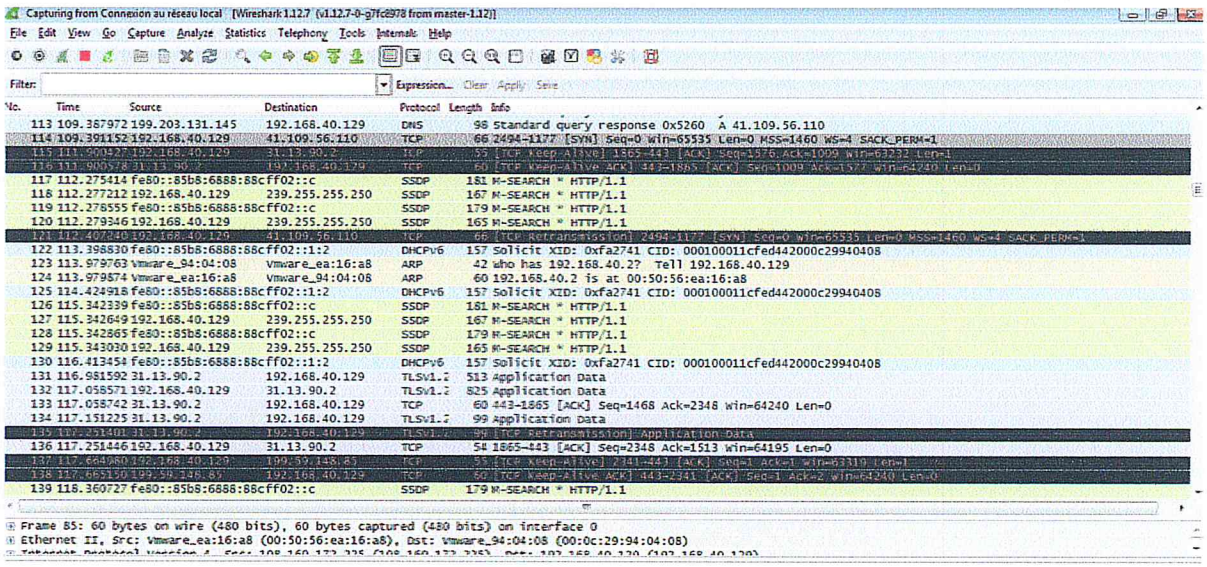


FIGURE V.7 – Scan du réseau avec Wireshark.

Dans la barre de recherche Filter il suffit d'écrire DNS car la majorité des chevaux de Troie utilise un Dns prédéfinis pour relier la machine du pirate à celle de la victime.

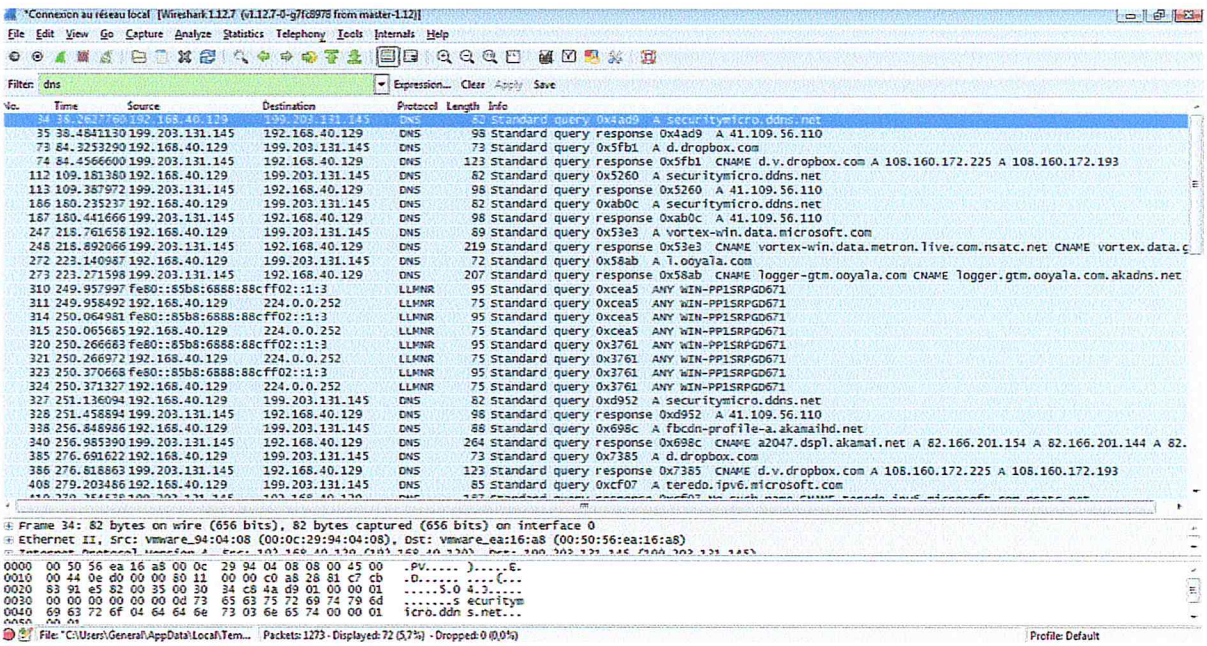


FIGURE V.8 – Wireshark filter DNS.

Pour ma part je me suis laisser infecter par un cheval de Troie il utiliser « securitymicro.ddns.net » pour relier les deux bout vers l'adresse 199.168.40.128 qui est américaine.

Une petite remarque s'impose, la même adresse communique avec un sous domaine l.ooyala.com

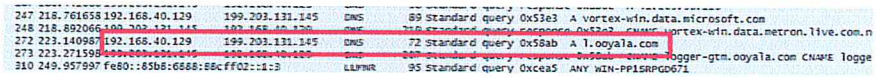


FIGURE V.9 – Communication du virus.

Sachant que ce dernier offre un service du genre Cloud vidéo Streaming, c'est un peu (bizarre) que le virus communique avec cette adresse alors un accès a se sous domaine s'impose

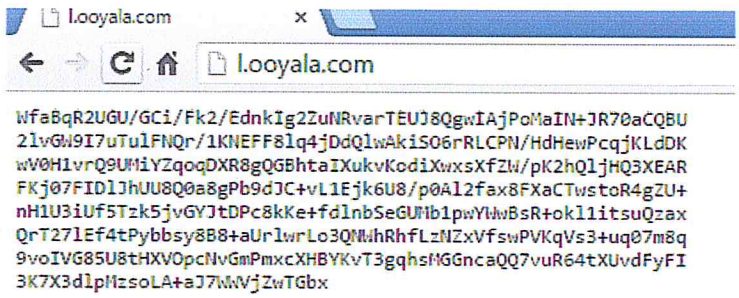


FIGURE V.10 – Partie du code du virus crypté

Comme par hasard c'est du texte, Donc le pirate utilise se sous domaine et plusieurs d'autres sites pour mettre à jour ses virus avec le même principe que notre étude avec un Downloader intégrer dans ses dernier.

C'est dans se principe que la première partie de détection est basé : donc pour la partie présentations nous aurons besoin d'un outille qui fera le tri avec une Liste des hosts connue pour faire Dynamics DNS service.

5.1 Deuxième méthode de détection

Elle est décomposée en deux parties :

- 1 database creator qui extrait la signature numérique du fichier et l'enregistre dans une sorte de base de donnée qui est database.txt.
- 2 scanners qui parcoure les fichiers d'un répertoire et il les compare par rapport à sa base de donner.

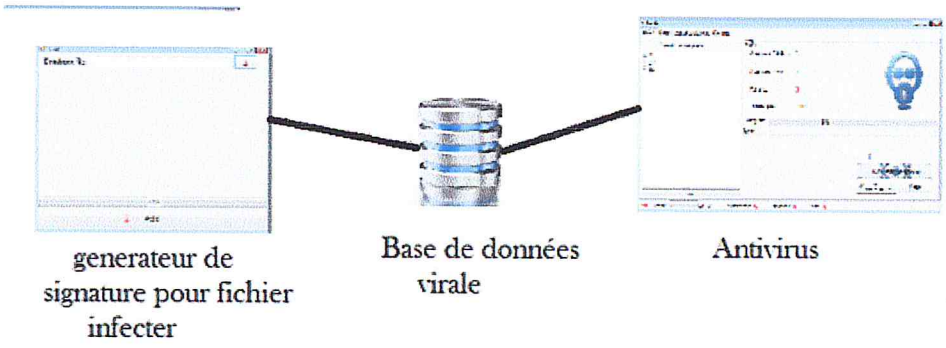


FIGURE V.11 – Scanner + générateur de signature.

6. Conclusion

Maintenant que nous avons expliqué plus ou moins en détail en quoi est basée en théorie notre étude, nous allons appliquer ces différentes notions dans le prochain chapitre.

Chapitre VI

Implémentation et tests

1. Introduction

Dans ce chapitre, nous allons appliquer la partie théorique étudiée précédemment. Pour cela, nous allons commencer par présenter les différents logiciels et langages utilisés pour ensuite entrer dans le vif du sujet à travers l'application du principe de l'application.

2. Logiciels et langages utilisés

2.1 Logiciels

- **VisualStudio .NET :**

  Visual Studio .NET [26] est un jeu complet d'outils de développement permettant de générer des applications Web ASP, des services Web XML, des applications bureautiques et des applications mobiles. Visual Basic .NET, Visual C++ .NET, Visual C# .NET et Visual J# .NET utilisent tous le même environnement de développement intégré (IDE, integrated development environment), qui leur permet de partager des outils et facilite la création de solutions faisant appel à plusieurs langages. Par ailleurs, ces langages permettent de mieux tirer parti des fonctionnalités du .NET Framework, qui fournit un accès à des technologies clés simplifiant le développement d'applications Web ASP et de services Web XML.

- **AutoIt Script Editor** compilateur de language Antoit (prononcer aow-toh-it).

- **ScriptCryptor Compiler**.

2.2 Langages :

- **VisualBasic .NET :**

  Visual Basic .NET [27] est un langage de programmation à la syntaxe similaire à celle de Visual Basic 6 .Néanmoins, ces deux langages sont assez peu comparables dans la pratique tant l'évolution entre ceux-ci est énorme. Le principal changement étant sans conteste l'introduction de l'orientation objet dans le langage.VB.NET permet de développer en .NET via Visual Studio, c'est-à-dire seulement sur les systèmes d'exploitation Windows (98, 2000, XP, Vista, 7, 8). Il existe cependant un projet visant à porter la plateforme DotNet (et donc VB.NET) sous Linux, MacOS et OpenBSD. Ce projet s'appelle Mono et il permet déjà de faire tourner nativement des applications .NET 2.0.Il est important de rappeler que tout programme VB.NET est compilé dans le même langage intermédiaire (IL) que C# ou tout autre langage de la plateforme DotNet.Les tutoriels de Visual Basic seront sous forme de vidéo afin de faciliter l'apprentissage.

- **AutoIt :**

  AutoIT [28] est un langage de script freeware permettant une automatisation sous le système d'exploitation Microsoft Windows. Dans ses premières versions, le logiciel a été principalement destiné à créer des scripts d'automatisation (parfois appelés macros) pour des programmes Microsoft Windows. De tels scripts ont prouvé leur utilité dans l'automatisation de tâches fortement répétitives, comme le déploiement d'un grand nombre de PC avec des instructions d'installation identiques. Avec les versions successives, AutoIt s'est développé pour inclure des améliorations tant dans la conception du langage de programmation que dans les fonctionnalités générales.

- **VBScript :**

  VBScript [29] il a été conçu par Microsoft pour donner un peu de vie ou d'interactivité aux pages HTML (tout comme le JavaScript chez Netscape). Il reste particulièrement intéressant pour faire de petits programmes destinés à tourner "en local". En fait, VBScript peut être considéré comme un VB édulcoré et ...gratuit. Contrairement à VB, les scripts ne sont pas compilés.

3. Application du principe

Pour tester le bon fonctionnement de l'application il nous faut choisir un virus donc j'ai opter pour un générateur de chevaux de Troie don le nom est Njrat car il est disponible en ligne et connu pour sa stabilité.

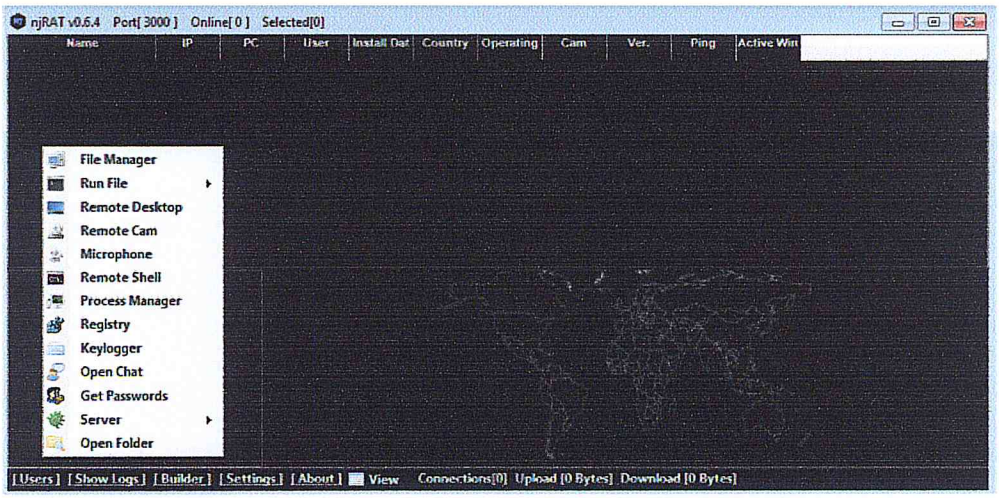


FIGURE VI.1 – Njrat 1.

Après avoir générer un cheval de Troie, le résultat de son scan dans le site Refud.me par rapport à 35 antivirus.

FIGURE VI.2 – Scan Njrat.

3.1 Le crypter

Il est connue dans le domaine de la cryptovirologie qu'il est difficile d'obtenir un résultat FUD en utilisant seulement la BASE-64. L'application a été divisé en plusieurs parties afin de se simplifier la tâche dans l'explication.

1. **Crypter**

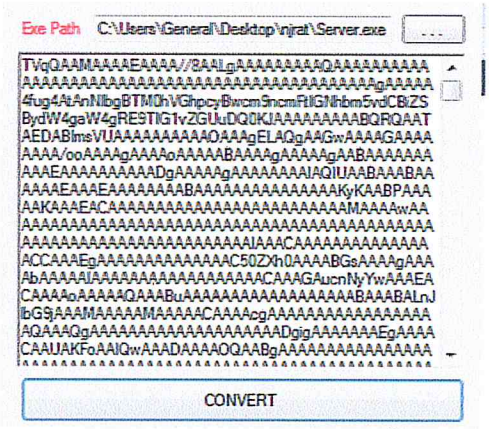


FIGURE VI.3 – Trojan vers Base 64

Ou il suffit de sélectionner le fichier exécutable à crypter pour cette étape on a choisis la base 64 qui sert à transformer un fichier binaire en fichier texte afin de l'utiliser dans notre fichier .vbs qui sert de plateforme de lancement de notre virus.

2. **Virus crypté**

Il suffit d'ajouter le texte en base-64 au point d'entrée qui reçoit se dernier afin qu'il soit décrypter a la fin avec des manipulations comme :

- La création d'un bloc « Set » afin qu'il puisse être récupérer sous la forme d'un objet en wscript.shell.
- création d'objet en Msxml2.DOMDocument.3.0 afin qu'il reçoit les éléments en base-64.
- variable.text pour récupérer le code en Base-64.

– association du bloc avec en Msxml2 avec la variable.text pour qu'ils puissent faire le décryptage a la fin.
– exécution du programme.

Le résultat lors du scan de notre fichier .vbs

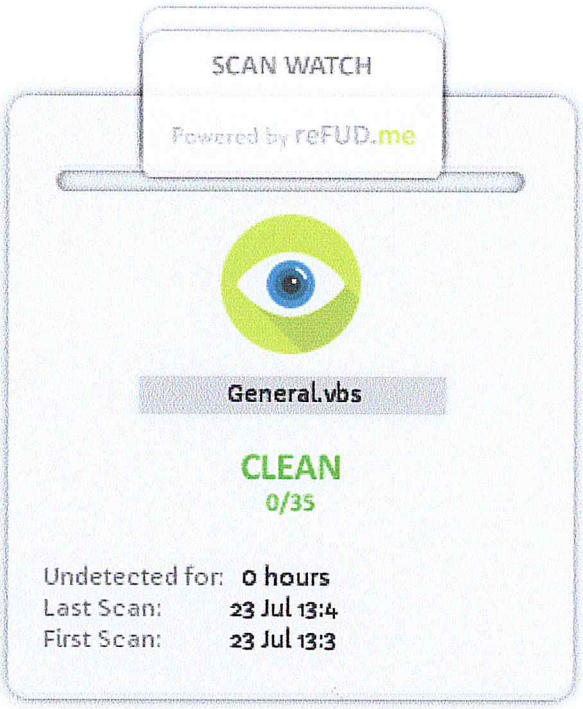


FIGURE VI.4 – Résultat du scan virus crypté 1.

FIGURE VI.5 – Résultat du scan virus crypté 2.

Exécution du fichier General.vbs :

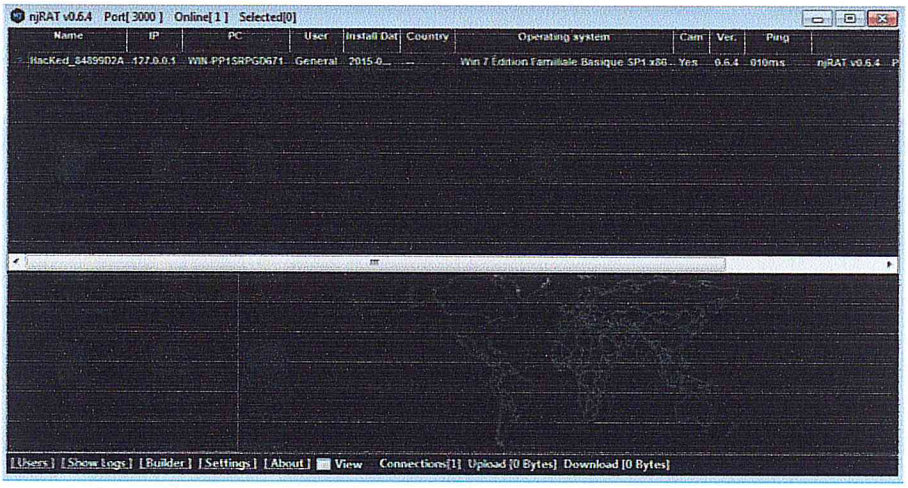


FIGURE VI.6 – Njrat 2.

3.2 Application de l'exploit

Dans cette partie on va présenter l'exploit. Il sert à joindre le virus dans et un fichier .txt ou autres , ce qui est idéal pour la propagation.

Pour cela nous aurons besoin d'un compilateur de script comme ScriptCryptor Compiler qui va nous changer le .vbs en .exe pour appliquer l'exploit.

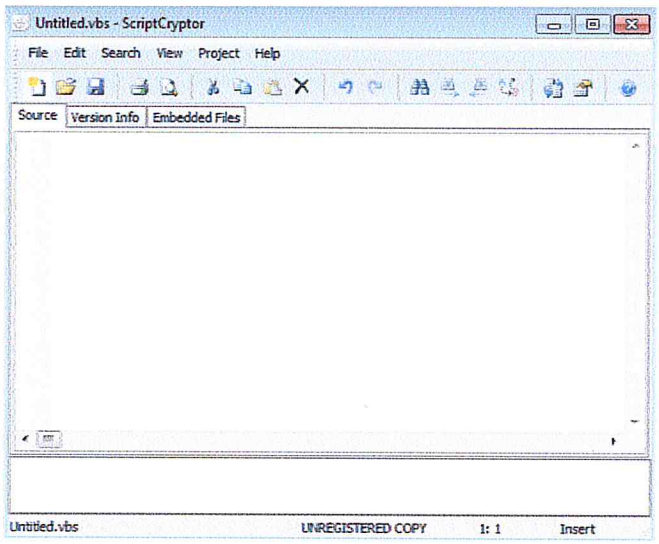


FIGURE VI.7 – ScriptCryptor Compiler

Après qu'on a finis on met dans le même répertoire notre virus crypté en .exe + script autoIt (qui représente l'exploit)+ le fichier text

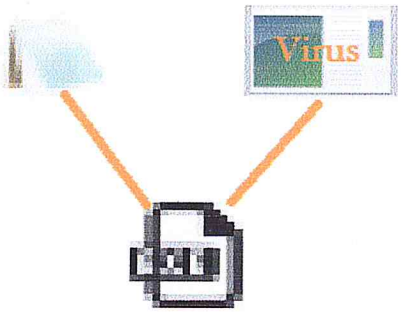


FIGURE VI.8 – Fichiers joints.

L'exploit en lui-même est un script en autoit qui exécute dans temporary file dit (Temp) les deux fichiers qui sont joint dans le nouveau .exe générer.

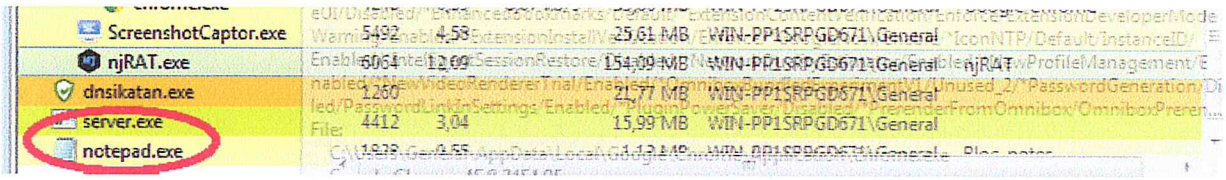


FIGURE VI.9 – Fichiers joints après l'exécution

Après ses manipulation c'est-à-dire conversion et l'ajout de l'exploit serte sa va touché beaucoup de monde mais le virus va perdre dans la détection car il a subi beaucoup de modifications qui se résume sur :

L'utilisation d'un outil pour la conversion du .vbs en .exe qui est utiliser par beaucoup de hacker pour propager leurs vers dans des ordinateurs ou le REG, VBS ou WSF ont été désactivé.

4. Partie détection

4.1 Première technique

Dans le chapitre précédant nous avons parlé de wireshark et comment détecter un cheval de Troie à travers sa communication avec le host du pirate don ce dernier utilise un service qui s'appelle Dns Dynamic Host. On va employer le même principe mais avec des outils Bien spécifiques :

TCPView est un programme Windows qui va vous montrer des listes détaillées de toutes les connexions TCP et UDP paramètres sur votre système , y compris les adresses et état des connexions TCP locaux et distants . Sur Windows Server 2008 , Vista et XP , TCPView signale également le nom du processus qui possède le point de terminaison . TCPView fournit un sous-ensemble plus informatif et plus commodément présenté du programme Netstat fourni avec Windows.

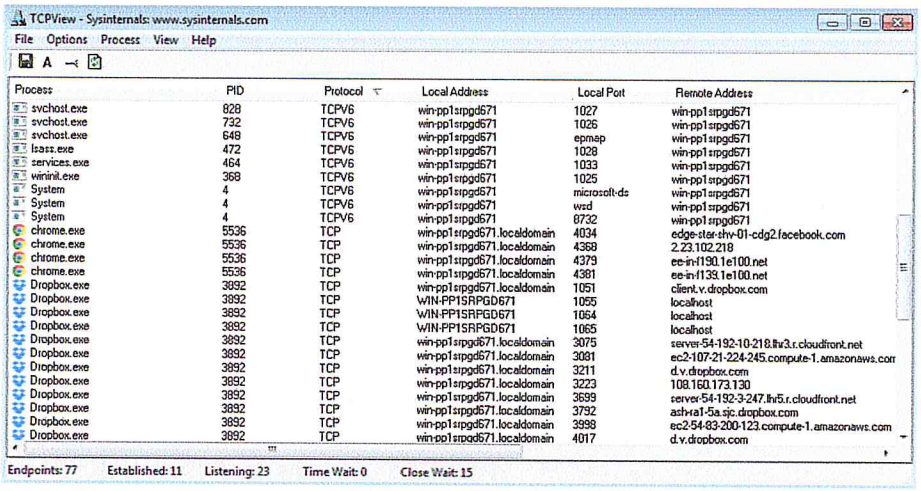


FIGURE VI.10 – TCPView

On sait que tcpview est l'interface graphique d'un programme qui s'appelle Tcpv-con :

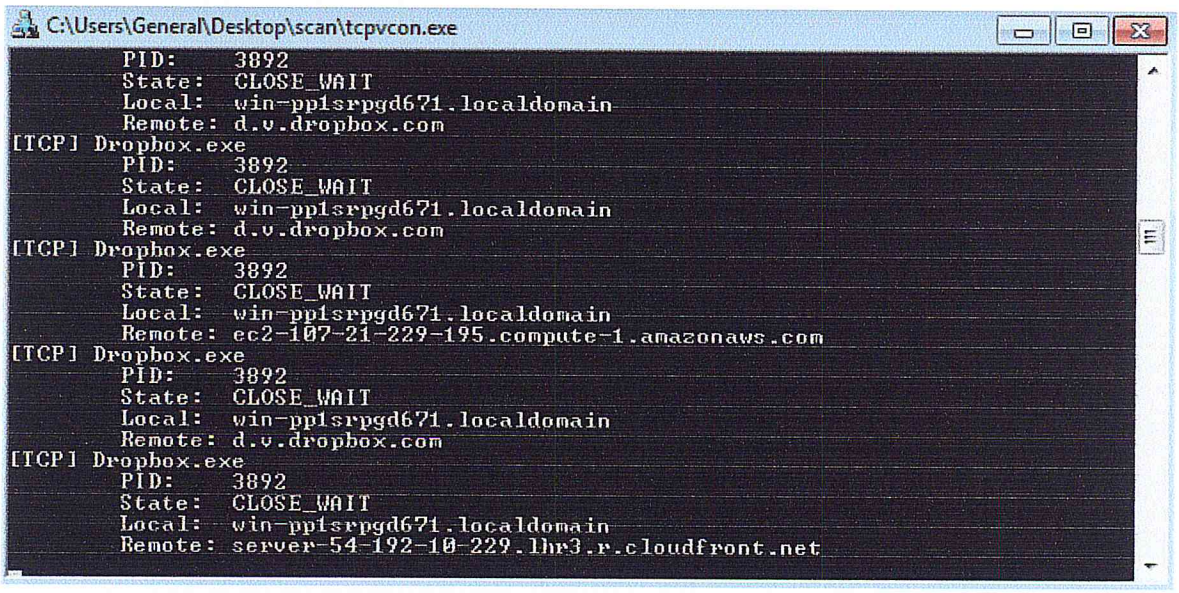


FIGURE VI.11 – TCPvcon

Donc l'idée est de faire une liste avec les noms de domaine qui servent comme Dynamics Dns host et la comparer aux adresses de sortie (Remote adresse). Pour cela on a besoin d'un script qui prend comme ressource le programme tcpvcon.exe et Dn-

shost.txt pour nous donner un résultat s'il y'a une infection. Étant donné que notre système est infecté, c'est ce que l'analyse avec wireshak a prouver. Le teste avec notre script à donné :

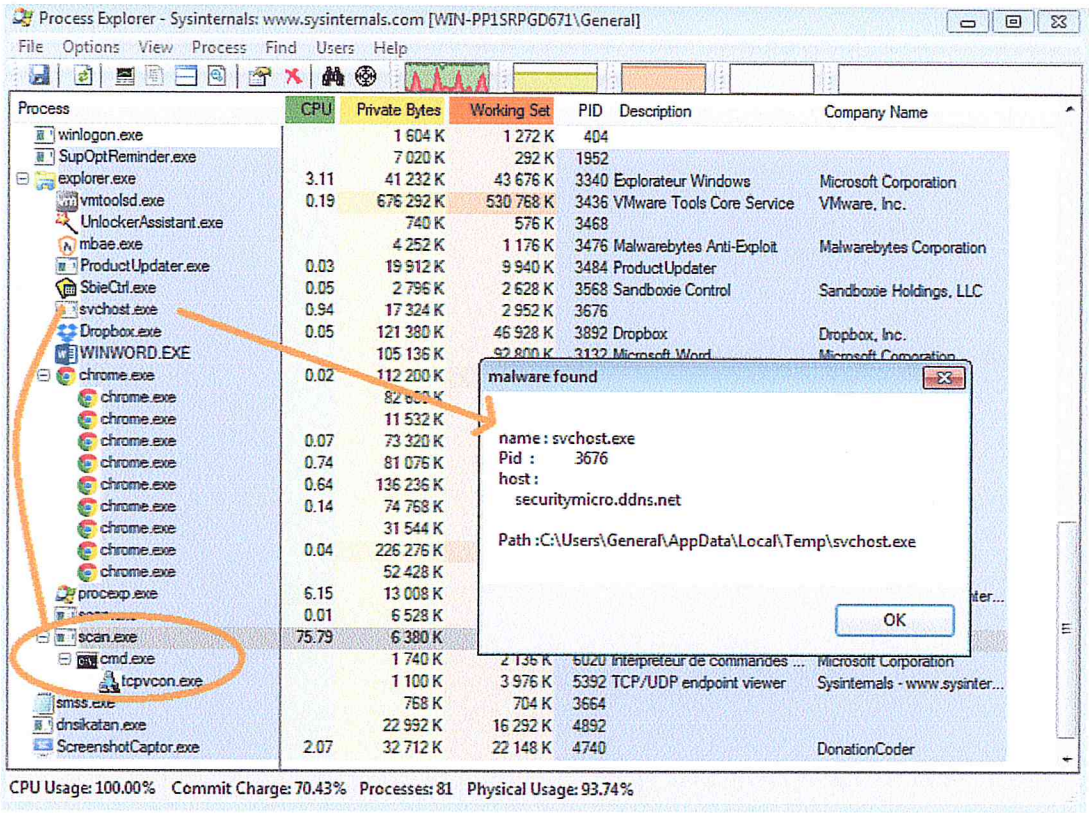
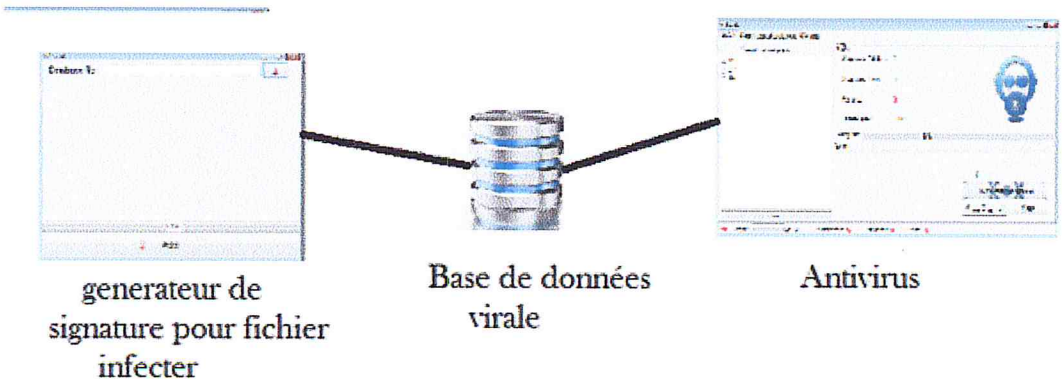


FIGURE VI.12 – Résultat du test.

4.2 Deuxième technique



1. Choisir le fichier infecté.
2. Ajouter sa signature Md5 à la database.

Remarque : cette fonctionnalité est faite chez les développeurs d'Antivirus, les utilisateurs ne reçoivent qu'une mise à jour de leur base de données.

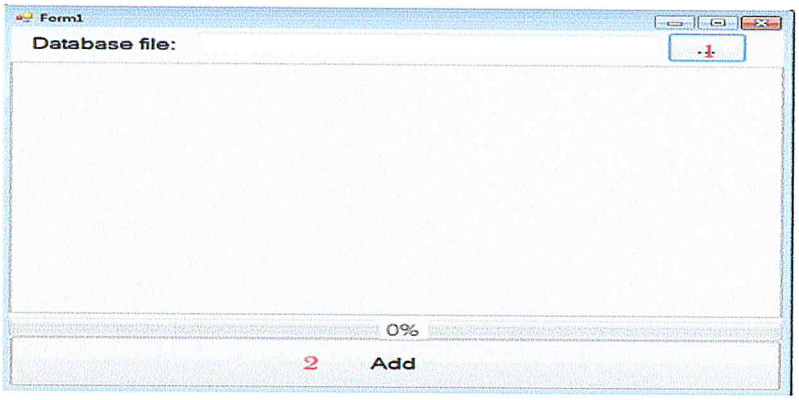


FIGURE VI.13 – Database creator

La deuxième partie :

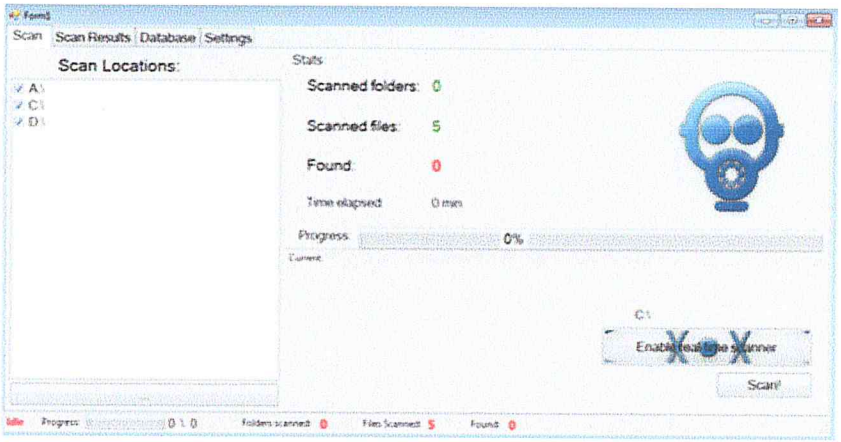


FIGURE VI.14 – Scanner.

Ses spécificités :

- Relier à notre base de données précédemment expliqué.
- Détection automatique des périphériques (Scan Locations).

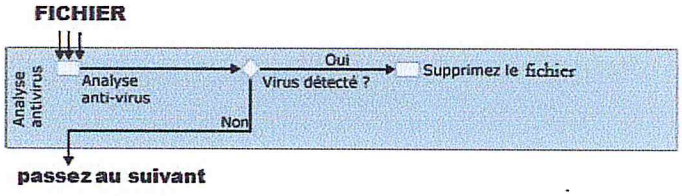


FIGURE VI.15 – Schéma explicatif.

- scanner (choisir le répertoire).
- Affichage de résultats (S'il y a une infection, vous aurez le choix de supprimer ou pas le fichier)

5. Conclusion

Tout au long de ce chapitre, on a présenté des applications afin de rendre des virus indétectables et de les détecter en utilisant des techniques cryptage ainsi que d'autre méthodes qui nous ont permit de résoudre notre problématique posée au tout début de ce présent travail.

Conclusion générale

Dans ce mémoire nous avons traité l'une des problématiques majeures de la sécurité informatique : les virus. Nous avons remarqué qu'il existe beaucoup types de virus, dont la naissance remonte à des époques différentes, et qui s'occasionne avec les grandes phases de l'informatique. On est témoin de la multiplication de ses dernier avec l'accès facile du grand public à internet.

Sachant que Windows est le système d'exploitation majoritairement touché, mais il est à craindre qu'avec l'explosion de Linux, et le taux élevé de son utilisation, fait augmenter les attaques tournées vers ce système. Surtout s'il est utilisé par des gens non expérimentés. Il a cependant une bonne marge d'avance, puisque le nombre de virus en activité sous Linux est minime comparées à ceux pour l'OS de Microsoft car contrairement à Linux, il est difficile d'avoir l'accès au mode super admin (root).

Étant donné que le problème des virus cryptés représente le cœur de notre travail, et malgré les difficultés existantes telles que rendre les virus cryptés indétectables par rapport aux différentes antivirus, nous avons essayé de présenter une solution qui pourrait palier ce problème.

Par conséquent, les anti-virus ne sont pas prêts de disparaitre dans le futur proche. Il leurs faut donc travailler avec intermittence afin de trouver (ou améliorer) de nouvelles solutions pour combattre ce fléau car les virus franchissent aussi un cap à chaque innovation des anti-virus avec un avantage majeur à l'heure actuelle qui est l'obligation de découvrir le virus avant de pouvoir l'écraser.

Ce présent travail m'a personnellement permis de renforcer mes connaissances dans ce vaste domaine, et ainsi d'acquérir de nouvelles notions qui vont sans doute me servir dans le futur proche.

Bibliographie

[1] Yves Lescop. *La Securite informatique*. 2002.

[2] Christophe Toulemonde. La triade de la sécurité de l'information,http://www.jemmvision.com/blog/3/la-triade-de-la-securite-de-l-information. 2013.

[3] Eric Cole. *Hackers Beware*. 2001.

[4] Marco Bertolini. *Vie privée : 10 mythes à propos de la sécurité informatique, http://format30.com/2013/06/17/vie-privee-10-mythes-a-propos-de-la-securite-informatique/.* 2013.

[5] Solange Ghernaouti-Hélie. *Professeur à l'Institut d'informatique et d'organisation, HEC-Lausanne, http://dit-archives.epfl.ch/FI00/fi-sp-00/sp-00-page20.html*. 2000.

[6] Ludovic Blin. *La Sécurité Informatique*. 1999.

[7] http://www-igm.univ-mlv.fr/~dr/XPOSE2013/panoramas_des_attaques_reseaux/~~img/tcp.png~~.

[8] Michel Bertin. Virus informatiques. Master's thesis, CLUSIF, 2005.

[9] Jean-François PILLOU. Virus informatique, http://www.commentcamarche.net/contents/1235-virus-informatique.

[10] A. Rasolondrainibe. La protection contre les virus informatiques, 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.

[11] Michel Dubois. Définition des virus - les virus informatiques- , http://vaccin.sourceforge.net/docs/definition2.html, paris-sorbonne.

[12] http://vaccin.sourceforge.net/docs/definition2.html.

[13] http://letoilecybercafe.free.fr/antivirus.html.

[14] http://kenebegni.skyrock.com/.

[15] Jaques Stern. *La science du secret.* 1998.

[16] http://fr.academic.ru/dic.nsf/frwiki/353474.

[17] http://emigma.louisedade.co.uk/howitworks.html.

[18] https://openclassrooms.com/courses/1-algorithme-rsa/crypter-et-decrypter.

[19] http://www-igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html.

[20] https://support.microsoft.com/fr-fr/kb/246071.

[21] T. De pujo and A. Roger. *Panorama des algorithmes de cryptage de l'information.* 2013.

[22] H. Nasser, M. Fangayoumani, and S. Debras. Vérification formelle d'un protocole de sécurité à l'aide d'un outil d'analyse automatique des failles de sécurité. Technical report, ENAC.

[23] http://mtyas.com/.

[24] http://cypherx.org/buy-crypter.

[25] https://technet.microsoft.com/fr-fr/library/cc725744(v=ws.10).aspx.

[26] https://msdn.microsoft.com/fr-fr/library/aa291755(v=vs.71).aspx.

[27] BOUTGAYOUT Abdessamad. Rapport de stage sous thème didactiel d'une application. Technical report, Idrissi, 2011.

[28] http://www.automation-sense.com/blog/informatique/cours-visual-basic-net-vb-net.html.

[29] http://jacxl.free.fr/cours_xl/cours_xl_jac.html#accueil_vbs.