"Viruses & Rootkits"

Synthese de cours

par Nathalie Lessart
et Mahmoud Ghaddar

responsable: Emmanuel Fleury

6 décembre 2007

Université de Sciences
et Technologies
Bordeaux I

Master Informatique:
***C**rytologie et **S**ecurité*
***I**nformatique*

"Viruses & Rootkits"

Citations :

Virus : « Art de programmation destinée à détruire les systèmes des crétins », *Dark Angel*.

Virus : « a program that can infect other programs by modifying them to include a.... version of itself », *Fred Cohen*.

Rootkit : « ensemble de programmes permettant à un pirate de maintenir dans le temps un accès frauduleux à un système informatique », *Wikipédia*.

« Know your enemy », *Sun Tzu's, The Art of War*.

Mots clés : Rootkits, Virus, Anti-virus, Malware

Sommaire

Introduction

Depuis l'avènement de l'informatique, les moyens de communication se sont fortement développés notamment grâce à internet. Aujourd'hui, on peut instantanément envoyer des messages à l'autre bout du globe, surfer sur le web, télécharger des applications ...
Ces innovations nous facilitent grandement la vie, malheureusement leur utilisation n'est pas sans risque. En effet, tous les utilisateurs ne sont pas forcément bien intentionnés, et certains d'entre eux diffusent par ce biais des programmes malveillants (malwares), ou tentent de prendre illégalement le contrôle de machines.
Nous allons nous intéresser plus particulièrement à 2 types de malware : les virus et les rootkits, et nous décrirons des moyens utilisés pour s'en prémunir.

Chapitre 1

Les Virus

1.1 Quand est apparu le premier virus ?

Les virus émergent à partir des années 60, lorsque 3 informaticiens américains créent un jeu (Core War) dont le but est de détruire en premier son adversaire en lâchant des programmes dans la mémoire vive de l'ordinateur. Plus tard, 2 italiens ajoutent à ce jeu une procédure permettant la copie de programmes sur la mémoire de masse. Même si leur découverte s'avère très destructrice, on ne peut pas encore parler de virus.

On doit la création du premier virus à Fred Cohen, en 1983. Cet étudiant en informatique devait mettre en place un programme parasite pouvant se reproduire et pervertir des programmes(une sorte de vie artificielle autonome), pour un système Unix. Son idée sera reprise par la suite à des fins malhonnêtes.

Le premier virus qui fut clairement identifié fut le virus Brain, en 1986. Depuis lors, de nombreux virus sont en circulation, et tout le monde connaît leur existence, bien que la plupart des gens ne savent pas concrètement ce qu'ils sont.

1.2 Définition générale

Les virus sont des programmes malveillants qui se propagent et se reproduisent dans des ordinateurs en s'insérant dans des programmes hôtes. Ils se chargent en mémoire et s'exécutent lorsque le programme hôte est exécuté. Mais, ils ne sont pas capables d'effectuer ces actions par eux-mêmes : l'intervention involontaire d'un utilisateur est en général la cause de l'infection.

1.3 Comment fonctionne un virus ?

1.3.1 Composition d'un virus

Un virus est composé des parties suivantes :
- la séquence de reproduction, destinée à la recherche des fichiers cibles et la contamination,
- la séquence de commandes, destinée à la destruction,

– une condition (de déclenchement),
– la séquence de camouflage (facultative)

Séquence de reproduction
Condition
Séquence de commandes
Séquence de camouflage

Tab. 1.1 – Schéma type du virus

1.3.2 Fonctionnement

La mise en place d'un virus se compose de 3 étapes principales :
– l'infection : le virus est injecté dans le système visé,
– la contamination : le virus se duplique et infecte d'autres fichiers, mais ne perturbe pas encore le système,
– la destruction : le virus s'exécute et remplit ses fonctions lorsque les conditions sont réunies

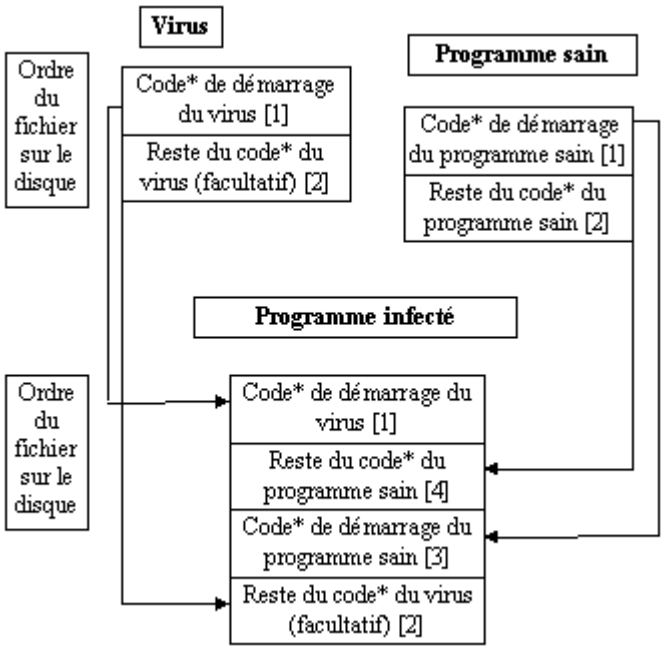

Fig. 1.1 – Fonctionnement d'un virus

1.4 Types de virus

1.4.1 Le virus classique

Le virus classique est aussi appelé virus exécutable ou encore virus programme. Il est, en général, écrit en assembleur. C'est un morceau de programme qui s'intègre dans un programme classique. Il agit principalement par ajout, et entraîne donc une augmentation de taille des exécutables que l'on peut facilement détecter. Il peut être résident ou non-résident.

Le virus de type non-résident est le plus répandu. Il est éliminé lors d'un reboot. Ce virus est activé à chaque fois que l'utilisateur exécute le programme hôte. A ce moment là, il va choisir d'autres fichiers et s'y répliquer. C'est le virus qui se lance en premier, puis le programme infecté s'exécute normalement.

Si un virus est de type résident (i.e. il reste présent dans la mémoire vive), il pourra infecter d'autres programmes lors de leur exécution par l'utilisateur qui va alors spécifier lui-même les cibles. Il n'est pas chassé par le reboot.

On peut citer comme exemple Boza, qui infectait les exécutables Windows 95, apparu en 1996.

1.4.2 Le virus de boot

Le virus de boot est aussi appelé virus système.
Il s'installe au niveau de l'un des secteurs de boot d'un périphérique de démarrage : disque dur, disquette, ...
A la différence d'un virus classique, il ne modifie pas le programme existant : en fait, il remplace le programme de démarrage déjà présent et le déplace vers une autre partie du disque. Ce virus est résident en mémoire et est chargé à chaque démarrage.
L'infection se fait en général via une disquette ou un CD-rom bootable. Tous les supports amovibles insérés par la suite seront infectés. Il est très difficile à détecter.
Ce type de virus est de moins en moins répandu, vu le taux diminuant du nombre d'échange de disquettes et leur moindre utilisation pour booter une machine.

Le virus système le plus célèbre est Michelangelo, apparu en 1992.

1.4.3 Le macro-virus

Le macro-virus cible les macros de logiciels du type Microsoft Office. Lorsqu'un document infecté est ouvert, il va contaminer le document par défaut de l'application, puis tous les documents qui seront ouverts par cette application.
Un virus de ce type se conçoit très facilement en VBA (Visual Basic for Application), et se répand très rapidement.

On peut citer comme exemple CONCEPT, premier macro virus Word, apparu en 1995.

1.4.4 Les vers

Les vers sont aussi appelés virus de messagerie. Bien qu'ils possèdent les caractéristiques principales des virus, certains experts ne considèrent pas qu'ils en font partie.
Ce sont des virus réseau. La plupart du temps, ils se servent des failles de certains logiciels de messagerie pour se propager via les courriers électroniques. Cependant, l'exploitation de ports ouverts, la connection réseau avec une machine infectée, sont d'autres moyens de propagation.
Pour infecter un ordinateur, ils se copient en mémoire, puis se répandent en s'envoyant eux-mêmes aux adresses contenues dans le répertoire du logiciel de messagerie.
Leur effet principal est la saturation des réseaux, mais ils peuvent aussi accomplir des actions malveillantes sur les ordinateurs contaminés.

Le premier vers fut le vers Morris, apparu en 1988.

Ce sont là les 4 principaux types de virus, cependant, la plupart du temps, des caractéristiques leur sont rajoutées.

1.5 Caractéristiques supplémentaires des virus

1.5.1 Le cryptage

On parle de virus crypté lorsque son code est crypté à chaque duplication de code. Le programme de cryptage peut lui aussi être crypté. Le code devient alors suffisamment complexe pour rendre son analyse par l'anti-virus très difficile.

Le premier virus crypté fut CASCADE, apparu en 1988.

1.5.2 Le polymorphisme

Il s'agit aussi de cryptage, mais cette fois, il diffère à chaque infection d'un nouveau fichier. Le virus change donc constamment d'aspect. Il est donc difficile à détecter par recherche de signature s'il n'a pas été décrypté au préalable.

Le premier virus crypté polymorphe fut 1260, apparu en 1990.

1.5.3 Le métamorphisme

Un virus métamorphe est capable de se modifier lui-même, c'est-à-dire les instructions qui le composent, mais en conservant ses propriétés infectieuses. Il est donc difficile à détecter pour les anti-virus.

Bolzano est un des premier virus métamorphe, apparu en 1999.

1.5.4 La furtivité

Un virus furtif est capable de tromper le système sur l'état des fichiers infectés. Pour cela, il envoie au système d'exploitation une information erronée lorsque

celui-ci fait une requête. Il est donc très difficile à détecter. Ils peuvent être crées grâce à des rootkits.

Le premier virus furtif fut FRODO, apparu en 1990.

Les virus représentent une menace conséquente en informatique, il est donc nécessaire de trouver des moyens afin de s'en prémunir.

1.6 Comment s'en protéger ?

1.6.1 Prévention

Pour éviter d'être infecté par un virus, il est nécessaire de prendre garde aux programmes et fichiers dont la source est douteuse. Avant d'exécuter un programme quelconque, mieux vaut être sûr de son origine.
Cependant, même en prenant des précaution, on peut introduire, par mégarde, des virus dans notre système. Heureusement, il existe des logiciels capable de nous offrir une assez bonne protection contre ces "malwares" : ce sont les anti-virus.

1.6.2 Antivirus

Un anti-virus est un logiciel qui parcourt le disque dur à la recherche de virus. Pour les dénicher, il utilise diverses techniques :

1. la recherche d'une signature : c'est un morceau de code qui permet d'identifier un virus particulier, si l'anti-virus l'a répertorié dans sa base de données (qu'il faut mettre régulièrement à jour),
2. l'analyse heuristique : il s'agit d'analyser le code de programmes inconnus pour déceler la présence de virus qui ne sont pas forcément répertoriés par l'anti-virus,
3. la surveillance du comportement des logiciels actifs : l'anti-virus recherche des anomalies au niveau des fichiers crées ou modifiés

C'est la première méthode qui est la plus utilisée, mais la deuxième est la plus puissante bien qu'elle puisse donner de fausses alertes. La troisième est nécessaire si on navigue internet, et vient en complément de l'une des deux autres.

Une fois le virus détecté, 3 choix s'offrent à l'anti-virus :

1. réparer les fichiers infectés quand cela est possible,
2. supprimer ces fichiers s'ils ne sont pas très importants,
3. les mettre en quarantaine en attendant qu'il puisse les réparer

Il existe 2 types d'anti-virus :
– les scanners : ils sont activés à la demande,
– les moniteurs : ils sont actifs en permanence en arrière-plan.

1.7 Quelques chiffres

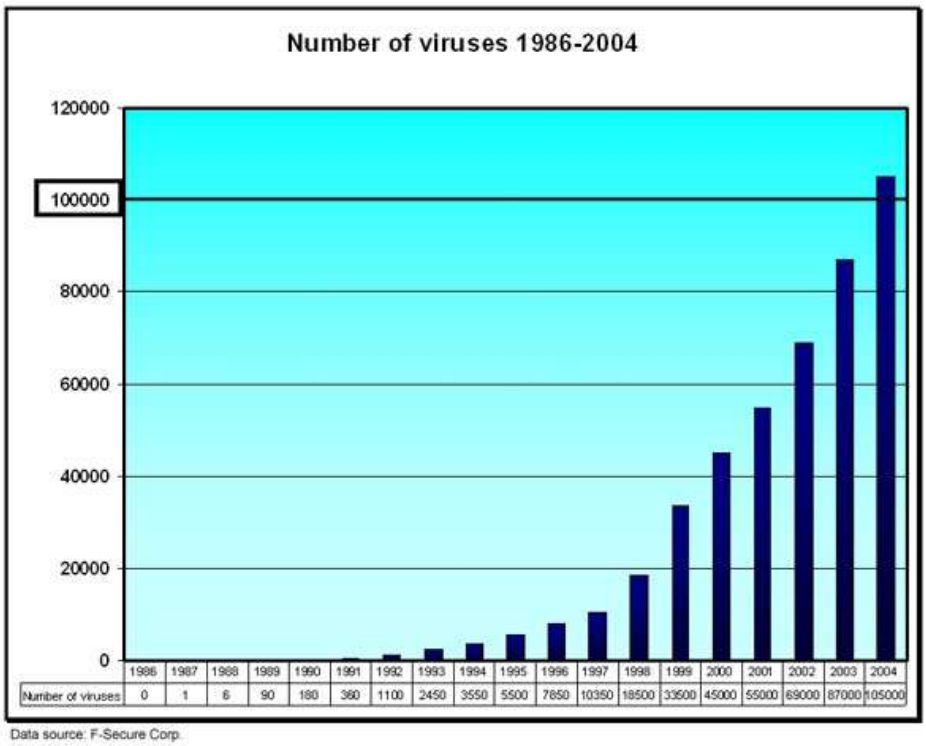

FIG. 1.2 – Évolution du nombre de virus entre 1986 et 2004

Chapitre 2

Les Rootkits

2.1 Quand sont apparus les premiers rootkits ?

Les rootkits existent depuis plusieurs années. Au début des années 1990, les hackers commencent à créer des kits leur permettant d'établir de manière stable le contrôle sur des machines (de type unix à l'époque) qu'ils sont parvenus à infiltrer : ce sont les premiers rootkits. Ces rootkits, qui utilisaient les appels systèmes, sont maintenant détectables. Cependant, d'autres méthodes, et donc types de rootkits, se sont développés au cours des années, et on en est, à l'heure actuelle, à la troisième génération de rootkits.

2.2 Définition générale

La fonction principale du rootkit est de camoufler la mise en place d'une ou plusieurs "portes dérobées". Ces portes dérobées permettent au pirate de s'introduire à nouveau au coeur de la machine sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès frauduleux initial, qui serait tôt ou tard comblée.

2.3 Comment fonctionne un rootkit ?

Les rootkits opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau (kernel). À la différence d'un virus informatique ou d'un ver de nouvelle génération, un rootkit ne se réplique pas.
L'installation d'un rootkit nécessite des droits administrateur sur la machine, notamment à cause des modifications profondes du système qu'il engendre. Cela signifie que le pirate doit initialement disposer d'un accès frauduleux, avec les droits « root » (sous Linux par exemple), afin de mettre en place son rootkit.
Un rootkit ne permet pas en tant que tel de s'introduire de manière frauduleuse sur une machine saine. En revanche, certains rootkits permettent la collecte des mots de passe qui transitent par la machine corrompue. Ainsi, un rootkit peut indirectement donner l'accès à d'autres machines.
Certains rootkits sont également livrés avec des collections d'exploits, ces petits bouts de code dédiés à l'exploitation d'une faille bien déterminée. Le but est

d'aider les pirates dans leur conquête de machines encore vierges.
Un rootkit a pour but principal la furtivité, il permet par exemple de cacher certains processus, certains fichiers et clefs de registre, etc. Il opère au niveau du noyau (la plupart du temps chargé en tant que driver) et peut donc tromper à sa guise les programmes qui sont exécutés en mode utilisateur (antivirus, firewalls). Le rootkit est souvent couplé à d'autres programmes tel qu'un sniffeur de frappe, de paquets...
Le rootkit n'a de raison d'être que si une faille est présente, si les conditions sont réunies pour que son exploitation soit réussie et si elle permet un accès avec les droits administrateur.

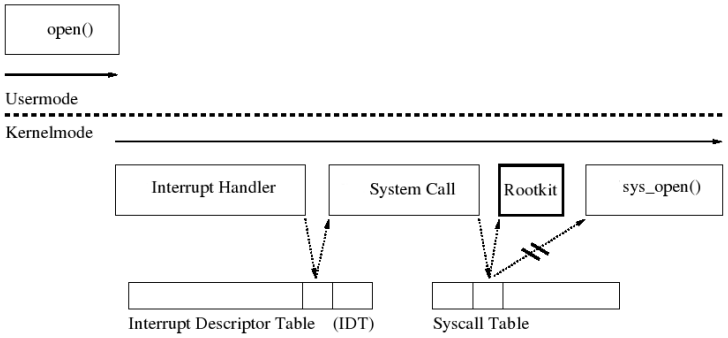

FIG. 2.1 – Exemple de fonctionnement d'un rootkit

2.4 Types de rootkits

2.4.1 La première génération

Ces kits étaient généralement crées pour les systèmes unix alors plus nombreux sur Internet. Les hackers, après avoir réalisé un exploit (i.e. après avoir utilisé avec succès une faille découverte dans un logiciel utilisé par la machine cible, ou une faille directement présente dans le système d'exploitation de celle ci, et avoir ainsi obtenu un accès "root", lui conférant ainsi tous les droits), pouvaient alors installer leur kit afin de pouvoir de nouveau obtenir un accès administrateur par la suite sans avoir à réaliser un nouvel exploit.
Ce programme installé leur permettait de se réapproprier ces droits d'accès si dévastateurs, sans difficultée, et en plus avec transparence en trafiquant les commandes systèmes.
En modifiant la commande "ls" qui permet de lister le contenu d'un répertoire ou en la remplaçant par une version modifiée, il leur est possible de rendre invisible certains dossiers ou fichiers.
Et d'autres commandes, comme "netstat" qui liste l'état des ports sur une machine, permettent, une fois modifiées, de masquer certains ports afin de pouvoir ouvrir des canaux de communication sur la machine cible. Les modifications sur la commande "ps" permettaient de cacher des processus actif.
On commence alors à réaliser le danger que représentaient ces kits qui permettaient de rendre aveugle l'administrateur ou les utilisateurs d'un système.

Heureusement, ce genre de manipulations ont pu, au bout d'un certain temps, être détectées et éradiquées, grâce notamment à des outils comme Tripwire qui surveille les changements intervenant sur les binaires des commandes.

2.4.2 La deuxième génération

Une fois que les administrateurs ont réussi à protéger les binaires des commandes de leurs systèmes, les hackers ont développé une deuxième génération de kits, s'attaquant cette fois ci aux bibliothèques partagées utilisées par les commandes systèmes. Une fois ces bibliothèques corrompues, le comportement de certaines commandes était alors modifié aboutissant ainsi au même résultat que pour la première génération.

2.4.3 La troisième génération

Une fois la seconde aisément détectée par les administrateurs, la troisième génération a vu le jour, s'attaquant alors directement au noyau. C'est principalement celle-ci qui est utilisée de nos jours.
Le principe de fonctionnement de ces rootkits consiste en la modification d'éléments importants du système, comme des fichiers de commande, des librairies ou encore, dans le cas le plus extrême, en une modification du comportement du noyau via des modules.

2.5 Quelques exemples bien connus

2.5.1 Rootkit Sony-BMG

En octobre 2005, le spécialiste en sécurité Mark Russinovich (compagnie Sysinternals) a découvert un rootkit installé comme composant de gestion numérique des droits (DRM), lors de son écoute, par un CD audio de marque Sony-BMG 1 2 3 . Ce rootkit permettait, une fois chargé, de cacher au niveau du noyau tous les fichiers dont le nom commençait par sys. Cette fonctionnalité a été exploitée par des virus pour cacher leur code malveillant et échapper ainsi aux programmes anti-virus. Cette affaire a fait un tort important à Sony, aussi bien au niveau de sa réputation, que financièrement. Dans plusieurs pays, Sony a été obligé de reprendre ses CD avec rootkit et de dédommager les clients.

2.5.2 Rootkit clé USB Sony

En 2007, Sony révèle la présence d'un rootkit dans ses clés usb biométrique 5 6 7. Cela a été développé par leur sous-traitant FineArt Technology à la demande de Sony. La faille a été découverte par F-Secure.
Sony se défend et affirme qu'il n'aurait pas eu pour objectif de fournir des renseignements à certains organismes, ou leur permettre d'accéder aux informations des entreprises... D'après plusieurs éditeurs de solutions anti-virus, cette affaire est en effet moins grave que celle du rootkit se trouvant sur leurs CD Audio. Le principal risque et reproche est que ce rootkit crée un répertoire caché du système, un endroit idéal pouvant être exploité par des virus pour échapper aux moyens de détection habituels.

2.6 Comment s'en protéger ?

2.6.1 Définition et fonctionnement

Tout comme pour les virus, il existe des programmes pour ce proteger des rootkits, les "anti-rootkits". Ces programmes verifient généralement l'integrité des binaires en se basant sur une base de signatures. Ils peuvent aussi comparer le kernel par rapport à une date ultérieure, et voir s'il existe des changement "importants" dans le système.

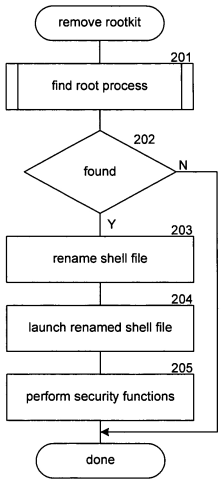

Fig. 2.2 – Fonctionnement d'un anti-rootkit

2.6.2 Quelques exemples

Windows

1. RootkitRevealer de Windows Sysinternals
2. IceSword
3. DarkSpy
4. RkU
5. NOD32
6. Blacklight F-secure
7. Rootkit Hook Analyzer

UNIX / Linux

1. chkrootkit de Nelson Murilo et Klaus Steding-Jessen (UNIX/Linux)
2. rkhunter de Michael Boelen (UNIX/Linux)
3. Zeppoo de ZeppooTeam (UNIX/Linux), renomé kernsh le 15 mai 2007, ce projet est maintenant intégré dans le framework ERESI (18 septembre 2007).

2.6.3 La meilleure protection

Le nombre de programmes malveillants étant en croissance exponentielle (voir figure 2.3), on ne pourrait pas construire un logiciel "anti-rootkits" par excellence. Les rootkits sont des codes capables de se transformer, et pour les arrêter, il faudrait un logiciel capable de se transformer aussi. Ceci impliquerait une intelligence artificielle bien au-delà de nos connaissances actuelles. Pour le moment, le meilleur moyen de se protéger des rootkits est de se prémunir contre les failles. Pour effectuer cela, il suffit de sensibiliser les utilisateurs sur les risques possibles de contamination.

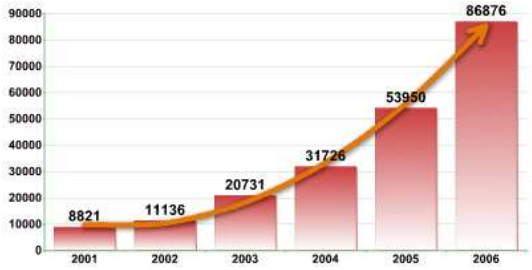

FIG. 2.3 – Croissance du nombre de programmes malveillant

Conclusion

Comme on l'a vu, les virus et les rootkits ne datent pas d'hier, et sont en constante évolution. Ces deux moyens de "piratage", le premier destiné à la destrucion, le second pour l'espionnage, revèlent les faiblesses de conception des systèmes informatiques actuels. Leur conception est de plus en plus sophistiquée afin de les dissimuler au mieux aux yeux des utilisateurs.
Cependant, il est possible d'en détecter la majorité par diverses méthodes. Pour cela, il suffit de bien comprendre comment ils fonctionnent. Mais, sachant que ces "spywares" sont en constante évolution, on ne peut pas être sûr de la sécurité des systèmes.
"Le seul système informatique qui est vraiment sûr est un système éteint et débranché, enfermé dans un blauckhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parirais pas ma vie dessus." *Gene Spafford, fondateur et directeur du Computer Operations, Audit and Security Technology Laboratory.*
De nouvelles voies sont explorées de nos jours, comme par exemple les virus et les rootkits qui profitent du système de virtualisation. Par contre, il est difficile de dire si ces types d'attaques ont de l'avenir dans le monde réel.

Bibliographie

[1] Misc 34, noyau et rootkit, 2007.

[2] Vie Artificielle. Description d'un virus informatique. http ://www.vieartificielle.com/article/ ?id=132.

[3] clashinfo.com. Les virus informatiques. http ://www.clashinfo.com/dossier/Les-virus-informatiques,168.html.

[4] Université de Toulouse 1. Les virus. http ://cri.univ-tlse1.fr/documentations/virus.

[5] Jean-Claude DEMONET. Les virus informatique. http ://www.anlbbs.com/anlbbs/Virus.htm.

[6] Eric Filiol. Les virus informatiques : théorie, pratique et applications, 2004.

[7] Jamie Butler Greg Hoglund. Rootkits : Subverting the windows kernel, 2005.

[8] Inoculer.com. Virus : typologie. http ://www.inoculer.com/virustypo.php3.

[9] Joseph Kong. Designing bsd rootkits : An introduction to kernel hacking, 2007.

[10] l0t3k.org. Rootkit : The complete documentation. http ://www.l0t3k.org/security/docs/rootkit.

[11] Nancy Altholz Larry Stevenson. Rootkits for dummies, 2007.

[12] le SEGI. Les virus informatiques. http ://www.ulg.ac.be/segi/internet/virus/index.html.

[13] Toby Miller. Analyse du root kit knark. http ://www.ouah.org/RootkitKNARKfr.htm.

[14] projet7.org. Linux et la sécurité : Retirer les failles et se proteger des outils des pirates. http ://www.projet7.org/warehouse/seculinux.html.

[15] Daniel L. Robichaud. Virus informatique 101. http ://www.cyberacadie.com/virus.htm.

[16] Peter Szor. The art of computer virus research and defense, 2005.

[17] Ric Vieler. Professional rootkits (programmer to programmer), 2007.

[18] Wikipedia. Virus informatique. http ://fr.wikipedia.org/wiki/Virus_informatique.

[19] woden.free.fr. Dictionnaire. http ://woden.free.fr/main_differentsvirus.htm#virus_furtif.

[20] Oleg Zaytsev. Rootkits, spyware/adware, keyloggers and backdoors : Detection and neutralization, 2006.

[21] Éric Filiol. Techniques virales avancées, 2007.