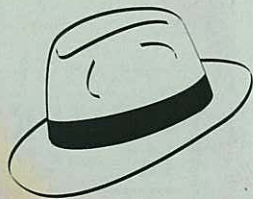


LA SÉCURITÉ INFORMATIQUE SIMPLE ET PRATIQUE

the **HACKADEMY**

N°1 BIMESTRIEL 4,5€ **mini PRATIK**



100% white hat hacking

NOUVEAU
ACCESSIBLE À TOUS!

VIRUS: LE MODE D'EMPLOI

LES RÈGLES POUR SE PROTÉGER
INSTALLER ET CONFIGURER UN ANTIVIRUS
DETECTER UNE FAUSSE ALERTE
SE DÉFENDRE D'UNE ATTAQUE
LE DICTIONNAIRE DES VIRUS
LES BOMBES LOGIQUES
L'INDEX DES SITES WEB

POUR EN FINIR DÉFINITIVEMENT

L 16430 - 1 - F: 4,50 € - RD



LA BIBLE DE L'ANTI VIRUS INFORMATIQUE

TOUT, TOUT, TOUT SUR LES VIRUS ! Conçu comme un guide pratique, ce 1er numéro de Mini Pratik vous dit tout ce qu'il faut absolument savoir sur les virus informatiques pour mieux s'en protéger. Vous verrez comment les différents types de virus fonctionnent de l'intérieur et comment ils se propagent. Pas à pas, vous apprendrez surtout à mettre en œuvre les stratégies de protection les plus efficaces : installation et configuration d'antivirus adaptés, test Eicar, nomenclature des programmes offensifs... Vous verrez aussi comment fabriquer vous-même un virus Windows très simple et, faut-il le préciser... inoffensif !

Le but de cette nouvelle collection au format de poche est de mettre à la disposition du grand public les meilleures informations sur la sécurité informatique. Dans un esprit didactique et pratique, les mini Pratik sont réalisés par des experts du secteur.

“ L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'1 an d'emprisonnement, et de 100 000 francs d'amende ”.

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique ». Ce texte prévoit notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ». Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même invo-

lontaire ou par maladresse, les peines sont doublées. Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisés, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourrent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

Les personnes morales, comme les entreprises ou les associations, peuvent, elles aussi, être déclarées responsables pénalement et encourrent les peines prévues à l'article 131-39 du nouveau Code pénal.



SOMMAIRE

- 6 **COMPRENDRE** LES VIRUS ET LES ANTIVIRUS
Partie 1
- 14 **COMPRENDRE** LES VIRUS ET LES ANTIVIRUS
Partie 2
- 19 **LES VIRUS** : MYTHES ET RÉALITÉS...
- 22 **LE MEILLEUR ANTIVIRUS**, C'EST VOUS !
- 28 **SAVOIR RECONNAÎTRE** UNE ALERTE BIDON
- 34 **INSTALLER ET CONFIGURER** UN ANTIVIRUS
- 46 **VÉRIFIEZ** QUE VOTRE ANTIVIRUS FONCTIONNE BIEN
- 53 **J'AI ÉTÉ ATTAQUÉ**, QUE FAIRE ?
- 53 **LE TEST EICAR**
- 54 **NE PAS TOUT CONFONDRE**...
- 56 **NOMENCLATURE DES VIRUS ET DES PROGRAMMES OFFENSIFS**
- 58 **UN VRAI VIRUS WINDOWS**... TRÈS SIMPLE ET INOFFENSIF !
- 66 **LE PROBLÈME DES BOMBES LOGIQUES**
- 68 **WEB WEB WEB**



COMPRENDRE LES VIRUS ET LES ANTIVIRUS

PREMIER ROUND :

LES FONDEMENTS DES VIRUS, LES ANTIVIRUS ANCIENNE GÉNÉRATION

Part 1

Le mot virus pour désigner un programme informatique se reproduisant est apparu en 1985 mais l'idée, elle, est bien plus vieille puisque c'est John Von Neumann qui a, le premier, imaginé le principe d'un automate autoreproducteur. A l'heure actuelle, le mot virus est chargé d'une connotation négative, due principalement aux dégâts subis par un certain nombre de personnes. Cependant, peu de personnes savent ce qu'est réellement un virus.

En parallèle, nous aborderons les techniques antivirales mises au point pour contrer les virus. Nous allons en fait remonter à la source et avancer de manière chronologique.

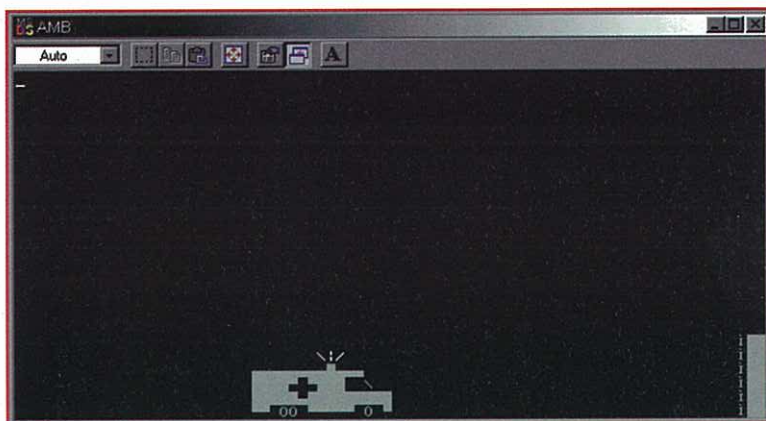
QUELQUES MISES AU POINT PRÉLIMINAIRES

Il est important de savoir de quoi on parle avant d'attaquer des explications un peu plus techniques. Faisons une mise au point dès le début pour clarifier les propos de cette section.

Ce nous appellerons "virus" est simplement le programme ou la partie du programme chargé de la reproduction, c'est-à-dire qu'un virus n'a pas d'autres buts que de se reproduire, comme le suggère l'expression "automate reproducteur". On peut faire le parallèle avec le virus biologique dont la fonction principale est de se multiplier.

Sur un autre plan, nous appellerons "bombe logique" ou "charge" la partie du programme qui produit un effet non lié à la reproduction. Attention, malgré l'emploi d'un mot à connotation négative, une fois de plus, une bombe logique n'est pas nécessai-

rement destructive. Ne nions pas que des bombes destructives existent, ce sont celles dont les gens se souviennent en général. Mais il existe également d'autres bombes, totalement inoffensives. Donnons deux exemples : le virus DOS Ambulance faisait traverser une ambulance en ASCII art en bas de l'écran et faisait le bruit de la sirène avec le haut parleur interne du PC ; les virus de Spanska étaient connus pour leur bombe graphique qui montrait une petite démo. Pour continuer le parallèle avec les virus biologiques, la bombe logique pourrait être comparée à la maladie que le virus provoque. Mais ça reste un effet secondaire. Il est enfin à noter que certains virus ne contiennent pas de bombes logiques et se contentent de leur fonction principale.



UNE BOMBE
INOFFENSIVE :
UNE AMBULAN-
CE TRAVERSE
VOTRE ÉCRAN...

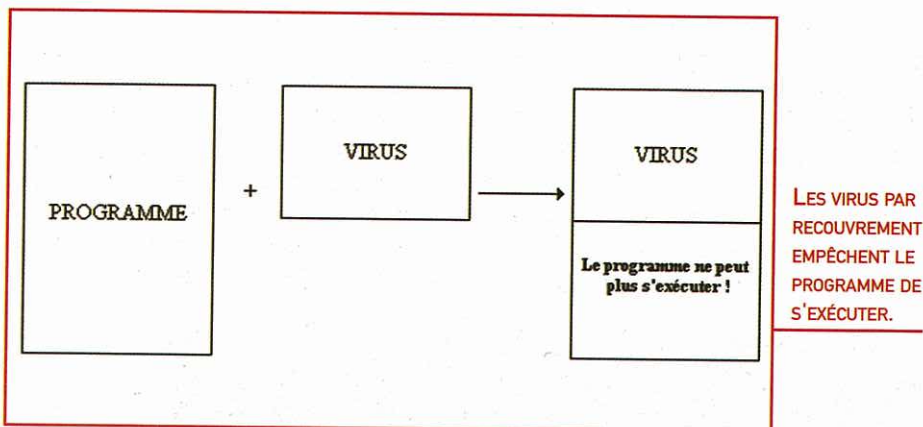
Pour qu'un virus puisse se reproduire, il a besoin de deux parties : une partie qui recherche les fichiers à infecter, et une partie qui s'occupe de l'infection elle-même, c'est-à-dire de la modification du programme cible. Il est important de bien séparer ces deux parties car les techniques les concernant sont radicalement différentes.

TECHNIQUES DE BASE POUR LES VIRUS

Il y a plein de manières pour infecter un programme. Nous n'allons pas en faire une liste exhaustive, ça ne servirait à rien. Cependant, il existe des techniques qui sont à la base de toutes les autres. Elles permettent également de faire une classification des virus.

• Les virus par recouvrement

Ce sont des virus très simples à faire. Il s'agit simplement d'écraser le programme cible avec le code du virus. Avec un tel virus, le programme cible ne peut plus s'exécuter, il est définitivement perdu. Cependant, ce type de virus est très peu utilisé car il se repère très facilement.



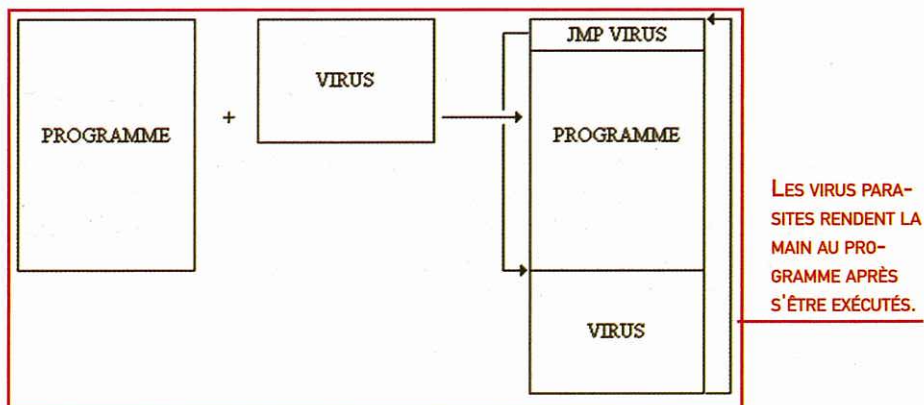
• Les virus compagnons

C'est une autre catégorie de virus très simple à programmer. Une autre section montre d'ailleurs le code d'un tel virus. Le principe est de renommer le programme cible, le cacher, et faire une copie du virus avec son nom original. Par exemple, imaginons qu'on ait un programme cible.exe : le virus le repère, change son nom en cible.xex par exemple et crée une copie de lui-même en cible.exe. Ainsi, quand on clique sur cible.exe, on lance le virus qui se reproduira quelques fois et lancera ensuite cible.xex pour faire croire à l'utilisateur que c'est bien le vrai cible.exe qu'il lance. Ainsi, le virus sera parfaitement invisible aux yeux de l'utilisateur.

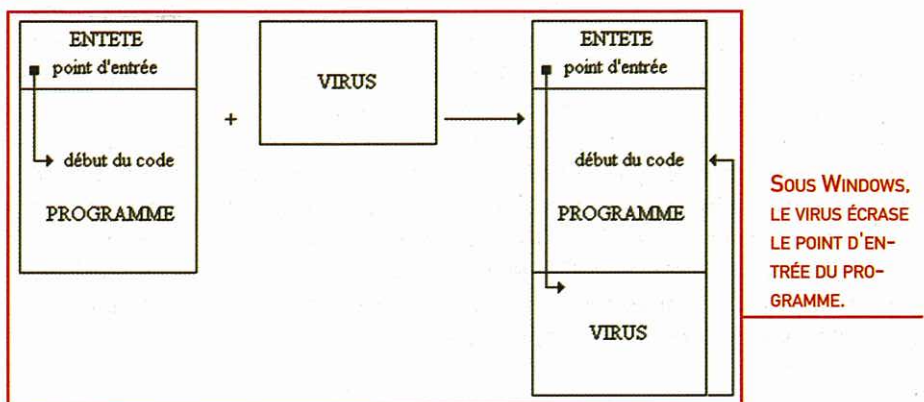
• Les virus parasites

Cette technique est, de loin, la plus employée. Elle consiste à attacher le virus au programme (comme un parasite) mais tout n'est pas si simple car il faut faire exécuter le virus puis le programme, ce qui pose des problèmes techniques qui dépassent le cadre de ce guide. Cependant, on peut distinguer deux cas.

Au temps du DOS, les programmes COM (Copy Of Memory pour les intimes) étaient très simples, le virus pouvait se coller directement à la fin. Pour avoir la main, le virus sauvegardait les premiers octets du programme et les écrasait par un saut sur son propre code. Ainsi, lors de l'exécution, le programme sautait sur le code du virus qui infectait d'autres programmes, il remettait les premiers octets originaux en place (tout cela se faisait en mémoire et ne modifiait pas la copie infectée sur le disque) et sautait au début du programme. Encore une fois, l'utilisateur ne s'apercevait de rien puisque son programme paraissait s'exécuter normalement.



Mais maintenant, les programmes sont beaucoup plus compliqués. Un EXE n'est pas que du code, il y a plein de choses qui servent à son bon fonctionnement et notamment des entêtes. D'ailleurs, si vous éditez un EXE avec un éditeur hexadécimal, vous verrez qu'il commencent toujours par "MZ" (c'est la marque d'un EXE DOS) et qu'un peu plus loin, on trouve "PE" (qui veut dire Portable Executable et qui est la marque des exécutables Win32). Dans ces entêtes, se trouve notamment l'adresse du code à exécuter, on l'appelle le point d'entrée du programme. Donc, au lieu de mettre un saut au début du programme, le virus sauvegarde simplement le point d'entrée original et l'écrase par son propre point d'entrée. Voilà en gros comment fonctionnent 80% des virus actuels.



Les trois techniques précédentes concernaient en fait la partie infection de la reproduction. Mais il existe également diverses techniques pour la recherche des cibles. Nous allons en voir les deux principales.

• Les virus à action directe

Pour ce type de virus, la recherche s'effectue directement grâce aux fonctions de recherche incluses dans Windows. Le virus fait donc une recherche sur *.EXE et infecte tous les programmes qu'il trouve. Cependant, ceci peut poser un problème : en effet, si le nombre de programmes à infecter est très grand, alors, l'infection va prendre du temps et l'utilisateur pourra le remarquer. Cette technique n'est, pour cette raison, pas très employée. Mais c'est celle que nous utiliserons dans le virus de démonstration, car c'est la plus simple.

• Les virus résidants

Le terme "résidant" regroupe en fait plein de catégories de virus dont il n'est pas nécessaire de donner le détail. Dans sa définition la plus globale, il signifie "qui reste en mémoire", ou qui "réside en mémoire". Le principe général est de placer le virus en mémoire pour qu'il infecte les programmes à la volée, quand ceux ci sont appelés par exemple. Il y a plusieurs manières de le faire. Nous allons tenter de donner un aperçu sans entrer dans la technique.

Sous DOS, le virus pouvait détourner l'interruption 21h (l'interruption DOS), c'est-à-dire traiter les appels au système DOS avant le système DOS, comme les appels d'ouverture de fichiers, ou de lecture de fichiers, que font la plupart des programmes.

Sous Windows, le virus peut faire l'équivalent. En effet, il existe en permanence une copie de kernel32.dll (la bibliothèque de fonctions "noyau" de Windows qui gère toutes les fonctions de bases du système) en mémoire. Il suffit alors que le virus modifie l'adresse de certaines fonctions (comme les fonctions d'ouverture de fichiers) en mémoire pour qu'elles pointent sur son propre code.

Il existe une autre technique qui a été utilisée une fois dans un virus. Vous avez sans doute remarqué que Windows savait en général quel programme appeler suivant l'extension du fichier que vous cliquez (par exemple, il ouvrira un navigateur Internet si vous cliquez sur un fichier HTML). Toutes ces informations sont stockées dans la base de registre de Windows. Et bien, il suffit que le virus dise à Windows qu'il faut l'appeler quand l'utilisateur clique sur un programme et tous les programmes que vous exécuterez seront "traités" par le virus avant d'être exécutés.

RÉCAPITULATIF

Voilà donc les techniques de base pour les virus. Tous les virus actuels utilisent ces principes, d'une manière plus ou moins complexe. Vous avez dû remarquer qu'un