

Virus informatiques et lutte anti-virus

J. HRUSKA

Préface de J.-C. Hoff

Traduit par M. Ginguay



004-90-1

 **MASSON**

PRENTICE HALL 

Table des matières

Préface.....	3
Avant-propos et remerciements	9
CHAPITRE 1 PRÉSENTATION - EXPOSÉ DES MENACES PESANT SUR LES SYSTÈMES INFORMATIQUES.....	11
1.1 Cheval de Troie	12
1.1.1 Exemple de Cheval de Troie n°1 : Fichiers BATCH	12
1.1.2 Exemple de Cheval de Troie n°2 : ANSI.SYS.....	13
1.1.3 Exemple de Cheval de Troie n°3 : Envoi par la poste d'une disquette d'informations sur le SIDA.....	14
1.2 Bombes logiques.....	15
1.3 Virus.....	16
1.4 Vers	17
1.4.1 Exemple de ver n°1 : L'Arbre de Noël sur IBM VM.....	17
1.4.2 Exemple de ver n°2 : Ver INTERNET sur UNIX.....	18
1.4.3 Exemple de ver n°3 : Ver SPAN sur VAX/VMS.....	19
CHAPITRE 2 COMMENT UN VIRUS PEUT-IL PÉNÉTRER DANS UN ORDINATEUR ?.....	21
2.1 PC contaminé et support contaminé	21
2.2 Chemin d'exécution.....	21
2.3 Vecteur de virus.....	25
2.3.1 Disquettes	25
2.3.2 Disques durs amovibles	26
2.3.3 Cartouches magnétiques.....	26
2.3.4 Autres supports de stockage.....	26
2.3.5 Modems	27
2.4 Voies et méthodes d'infiltration des virus.....	27
2.4.1 Logiciel piraté	27
2.4.2 Bulletins électroniques.....	27
2.4.3 Partagiciel.....	28
2.4.4 Logiciel du domaine public	29
2.4.5 PC partagés (PC domestiques)	29
2.4.6 Techniciens de maintenance.....	29
2.4.7 Logiciels « scellés ».....	30
2.4.8 Virus et réseaux de PC	31
CHAPITRE 3 STRUCTURE DES VIRUS.....	33
3.1 Types de virus en fonction du point d'attaque.....	34
3.1.1 Virus « secteur de démarrage ».....	34
3.1.2 Virus parasites	36
3.2 Comportement du virus après contamination du PC.....	37
3.2.1 Virus résidant en mémoire.....	37
3.2.2 Virus ne résidant pas en mémoire	38
3.2.3 Hybrides	38
3.3 Mécanismes de camouflage des virus.....	38
3.3.1 Cryptage	39

3.3.2	Interception des interruptions	40
3.3.3	Virus binaires	41
3.4	Effets secondaires des virus	42
CHAPITRE 4 VIRUS COURANTS SUR IBM PC		45
4.1	Noms de virus et pseudos	45
4.2	Configurations hexadécimales des virus	46
4.2.1	Virus recensés	47
4.2.2	Virus signalés	55
4.2.3	Cheval de Troie SIDA	58
CHAPITRE 5 D'OÙ VIENNENT LES VIRUS ?		61
5.1	Qui sont les auteurs de virus et quelles sont leurs motivations ?	61
5.1.1	Les pirates	61
5.1.2	Les psychopathes	62
5.1.3	Les étudiants d'université	63
5.1.4	Les employés	63
5.1.5	Clubs informatiques	64
5.1.6	Organisations terroristes	64
5.2	Dissection d'un virus capturé	64
5.2.1	Désassemblage d'un virus	65
5.2.2	Caractéristiques d'un virus	67
5.2.2.1	Quel assembleur ?	68
5.2.2.2	Instructions illégales	68
5.2.2.3	Style de programmation	68
5.2.2.4	Langue et orthographe	69
5.2.2.5	Lieu et heure de la détection initiale	69
5.2.2.6	Ancêtres	70
5.3	Mutation des virus	70
5.3.1	Modification des effets secondaires des virus	70
5.3.2	« Améliorations » de virus	71
5.3.3	Mutations visant à leurrer les programmes de recherche de configurations	71
5.3.4	Nouveaux virus	72
5.4	Statistiques des attaques de virus	72
CHAPITRE 6 PROCÉDURES ANTIVIRUS		73
6.1	Préparation	73
6.1.1	Sauvegardes régulières et saines	73
6.1.2	Disquette système protégée en écriture	74
6.1.3	Plan de secours	74
6.2	Prévention	75
6.2.1	Sensibilisation des utilisateurs	75
6.2.2	Règles d'hygiène	76
6.2.3	PC antivirus	77
6.3	Détection	77
6.3.1	Curieuses coïncidences	78
6.3.2	Identification d'un virus capturé	79
6.3.2.1	Virus parasites	79
6.3.2.2	Virus « secteur de démarrage »	79
6.4	Isolement	80
6.4.1	Accès au réseau	80
6.4.2	Echange de disquettes	80
6.4.3	Étiquettes d'interdiction d'écriture	81
6.5	Reprise	82
6.5.1	Suppression du virus sur les PC contaminés	82

6.5.2	Reprise après effets secondaires	83
6.5.3	Autres points	83
CHAPITRE 7 LOGICIELS ANTIVIRUS		85
7.1	Types de logiciels antivirus.....	85
7.1.1	Logiciel de contrôle de somme.....	86
7.1.2	Logiciel de balayage	87
7.1.3	Logiciel de surveillance.....	88
7.1.4	Autres logiciels antivirus.....	88
7.1.4.1	Shells d'intégrité.....	88
7.1.4.2	Logiciels de contrôle d'accès.....	89
7.1.5	Logiciel de suppression et d'inoculation de virus	90
7.2	Test des logiciels antivirus.....	90
7.3	Résumé des logiciels antivirus.....	91
ANNEXE A BIBLIOGRAPHIE		93
A.1	Ouvrages concernant les virus et les problèmes qui s'y rattachent.....	93
A.2	Périodiques sur les virus et la sécurité des données.....	94
A.3	Bulletins électroniques organisant des forums sur les virus.....	95
ANNEXE B PROGRAMME DE DÉTECTION SPÉCIFIQUE « SEARCH »		97
B.1	Description du programme SEARCH.....	97
B.2	Compilation du programme SEARCH.....	98
B.3	Codification SEARCH en langage « C ».....	99
ANNEXE C PROGRAMME DE DÉTECTION NON SPÉCIFIQUE « FINGER »		111
C.1	Description du programme FINGER.....	111
C.2	Compilation du programme FINGER	112
C.3	Codification FINGER en langage « C ».....	113
ANNEXE D FOURNISSEURS ET DISTRIBUTEURS DE LOGICIELS ANTIVIRUS.....		121
ANNEXE E GLOSSAIRE.....		125
ANNEXE F CARACTÈRES ASCII		137
ANNEXE G ÉDITEURS ET DISTRIBUTEURS DE LOGICIELS ANTIVIRUS EN FRANCE.....		141
INDEX		145

Virus informatiques et lutte anti-virus

J. HRUSKA

Cet ouvrage d'actualité explique la façon d'éviter les virus et de les combattre. Il s'attache aux solutions pratiques pouvant être immédiatement mises en œuvre par tous les utilisateurs.

L'auteur analyse la structure des virus, ainsi que les voies de pénétration et les vecteurs courants. Il s'intéresse également aux effets secondaires et aux mutations et donne des conseils pratiques concernant la prévention de l'infection virale. Il expose les armes anti-virus, notamment les logiciels de détection de virus, et préconise une approche progressive pour combattre les virus.

Les réseaux de PC, qui sont une voie de pénétration privilégiée pour les virus, sont traités en détail. L'ouvrage est complété par une liste de réalisateurs de logiciels anti-virus (français et étrangers) et par deux programmes en langage C qui détectent les virus sur IBM PC.

Cet ouvrage intéressera tous les utilisateurs de micro-informatique et plus particulièrement ceux du monde IBM et compatibles.

Jan HRUSKA, l'auteur, est directeur technique chez Sophos en Grande-Bretagne.

Michel GINGUAY, le traducteur, est l'auteur des dictionnaires d'informatique des éditions Masson et traducteur spécialisé en informatique.



ISBN: 2-225-82523-8