

VERS & VIRUS

Classification, lutte anti-virale
et perspectives



François Paget

DUNOD

VERS & VIRUS

**Classification,
lutte anti-virale
et perspectives**

Consultez nos catalogues sur le Web

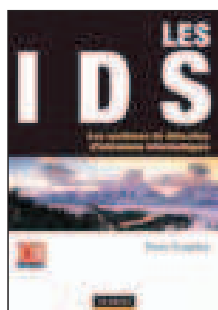
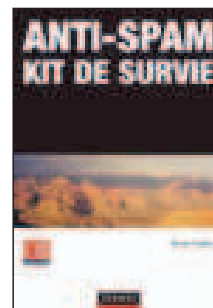


www.dunod.com



Sécurité des Architectures Web
Plouin, Soyer, Trioullier
496 pages
Dunod, 2004

Anti Spam : Kit de survie
Kevin Gallot
208 pages
Dunod, 2004



Les IDS
Les systèmes de détection
d'intrusions informatiques
Thierry Evangelista
272 pages
Dunod, 2004

Sous la direction de
Philippe Rosé

VERS & VIRUS

**Classification,
lutte anti-virale
et perspectives**

François Paget

*Chercheur anti-virus chez McAfee
Membre fondateur de l'AVERT*

DUNOD

Illustration de couverture : Jeremy Woodhouse/Iguazu Falls, Brazil
Source : digitalvision®

<p>Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.</p> <p>Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements</p>		<p>d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.</p> <p>Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).</p>
--	---	--

© Dunod, Paris, 2005
ISBN 2 10 008311 2

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

Table des matières

Avant propos	IX
Chapitre 1 – Les multiples aspects de la malveillance.	1
1.1 La sécurité des systèmes d'information	1
1.1.1 <i>Les menaces</i>	2
1.1.2 <i>La malveillance</i>	3
1.1.3 <i>Les attaques logiques</i>	4
1.2 Les messages non sollicités (sans pièce jointe)	5
1.2.1 <i>Les rumeurs ou hoaxes</i>	6
1.2.2 <i>Les lettres chaînes</i>	8
1.2.3 <i>Le spamming</i>	11
1.2.4 <i>Le scam africain</i>	14
1.2.5 <i>Le phishing</i>	15
1.3 Les messages non sollicités (avec pièce jointe)	17
1.4 Farces et canulars.	18
1.5 Les infections informatiques	19
1.5.1 <i>Les programmes simples</i>	19
1.5.2 <i>Les programmes auto reproducteurs</i>	33
Chapitre 2 – Historique – de l'innocence à la tentation criminelle	35
2.1 John Louis von Neumann	35
2.2 Les premières expériences	36
2.2.1 <i>CREEPER & REAPER</i>	37
2.2.2 <i>Animal et Pervade</i>	37
2.2.3 <i>Maintenance et télédistribution</i>	38

2.3	La science-fiction	38
2.3.1	<i>Harlie avait un an</i>	39
2.3.2	<i>Sur l'onde choc</i>	39
2.4	APPLE II	40
2.4.1	<i>Elk Cloner</i>	40
2.4.2	<i>Anti-Congo</i>	41
2.5	Fred Cohen	41
2.6	Les premiers vers	43
2.6.1	<i>BITNET : IBM Christmas Tree</i>	43
2.6.2	<i>INTERNET : RTM Worm</i>	43
2.6.3	<i>DECNET : Father Christmas Worm</i>	44
2.6.4	<i>DECNET : Worms Against Nuclear Killers</i>	44
2.7	1986-1987 : Premières infections	45
2.7.1	<i>BRAIN</i>	45
2.7.2	<i>Ralf Burger & Berdn Fix</i>	46
2.7.3	<i>Les universités en première ligne</i>	46
2.7.4	<i>L'arrivée du cryptage</i>	47
2.8	1988 : Les premiers antivirus pour ibm pc	47
2.8.1	<i>Virus Antivirus</i>	47
2.8.2	<i>Monitoring de programme</i>	48
2.8.3	<i>DATA CRIME : L'antivirus est au commissariat !</i>	48
2.8.4	<i>Recherche par signature</i>	50
2.9	L'énigme du premier macro-virus	51
2.10	1989 – 1992 : Investigation et challenge	52
2.10.1	<i>Le vengeur ténébreux</i>	53
2.10.2	<i>1260 : Le premier virus polymorphe</i>	54
2.10.3	<i>Flip, Tequila ET Maltese Amoeba</i>	54
2.10.4	<i>Tous azimuts pour les virus et les anti-virus</i>	56
2.10.5	<i>La riposte des chercheurs</i>	58
2.10.6	<i>Michelangelo</i>	59
2.11	1992 – 1995 : Générateurs et sophistication	59
2.11.1	<i>Natas, One_Half et les autres</i>	61
2.11.2	<i>Quelques arrestations</i>	63
2.11.3	<i>Goodtimes & Gt-Spoof</i>	64
2.12	1995 – 1999 – L'arrivée des virus interprètes	64
2.12.1	<i>WM/Concept</i>	65
2.12.2	<i>W95/Boza & Linux/Staog by Quantum</i>	66

2.12.3	<i>L'invasion des macro-virus</i>	67
2.12.4	<i>La naissance de Network Associates Inc.</i>	69
2.12.5	<i>Le retour des virus programme</i>	70
2.12.6	<i>Rabbit : Le lapin !</i>	71
2.13	1999 – 2000 – L'invasion des « MASS-MAILERS »	72
2.13.1	<i>Happy 99.</i>	72
2.13.2	<i>Melissa</i>	74
2.13.3	<i>LoveLetter</i>	75
2.13.4	<i>Kak, le Cagou contre Bubbleboy</i>	78
2.13.5	<i>VBS/Timofonica</i>	79
2.13.6	<i>Autour des PDA – PalmOS/Phage</i>	79
2.14	2001 – 2003 – Un discret changement de cap	80
2.15	L'été 2003 : ce sont principalement les particuliers qui trinquent !	81
2.16	Janvier 2004 : W32/MYDOOM.A@MM	83
2.17	À suivre...	84
Chapitre 3 – Notions fondamentales.		87
3.1	Les virus par cibles	87
3.1.1	<i>Virus système</i>	88
3.1.2	<i>Virus interprètes</i>	89
3.1.3	<i>Virus programme</i>	92
3.2	Les vers par types.	94
3.2.1	<i>Vers ou virus</i>	94
3.2.2	<i>Vers de disquettes</i>	96
3.2.3	<i>Vers de réseaux locaux</i>	96
3.2.4	<i>Vers de messagerie.</i>	97
3.2.5	<i>Vers en mode poste à poste</i>	99
3.2.6	<i>Vers de l'Internet</i>	100
3.3	Les virus/vers par fonctionnalité.	101
3.3.1	<i>Anti-debugging</i>	101
3.3.2	<i>Du cryptage au metamorphisme</i>	101
3.3.3	<i>Virus défensif – Retro-virus</i>	104
3.3.4	<i>Furtivité</i>	106
3.3.5	<i>Infecteur rapide</i>	107
3.3.6	<i>Cocktail</i>	107
3.4	La classification des virus	107
3.4.1	<i>Les virus de première génération.</i>	107
3.4.2	<i>L'effort de standardisation actuel</i>	111

3.5	Les autres environnements	127
3.5.1	OS/2	127
3.5.2	MacOS.	128
3.5.3	UNIX	129
Chapitre 4 – Les virus système		131
4.1	Mise en marche d'un micro-ordinateur.	131
4.1.1	<i>L'organisation de la mémoire</i>	133
4.1.2	<i>Les interruptions</i>	134
4.2	Mode de propagation	136
4.3	Attaque du boot.	137
4.3.1	<i>Secteur d'amorce d'une disquette</i>	137
4.3.2	<i>Secteur d'amorce d'un disque dur.</i>	139
4.3.3	<i>Structure d'une disquette</i>	140
4.3.4	<i>Structure d'un disque dur.</i>	141
4.3.5	<i>Le virus Form</i>	142
4.4	Attaque du MBR	146
4.4.1	<i>Structure du secteur des partitions</i>	146
4.4.2	<i>Le virus Jumper.B</i>	148
4.5	Techniques avancées	150
4.5.1	<i>Modification de la CMOS</i>	150
4.5.2	<i>Furtivité</i>	151
4.5.3	<i>Inaccessibilité au disque.</i>	151
4.5.4	<i>Utilisation de secteurs supplémentaires</i>	153
4.5.5	<i>Non-sauvegarde du secteur d'origine</i>	154
4.5.6	<i>Multipartisme</i>	154
4.5.7	<i>Polymorphie</i>	154
4.6	Spécificité des OS.	154
Chapitre 5 – Les virus programme		157
5.1	Modes d'infection	157
5.1.1	<i>Recouvrement</i>	158
5.1.2	<i>Ajout.</i>	159
5.1.3	<i>Infection par cavité simple</i>	162
5.1.4	<i>Infection par fractionnement</i>	163
5.1.5	<i>Délocalisés</i>	164
5.1.6	<i>Compagnons</i>	164

5.2	L'environnement 32 bits	165
5.2.1	Structure d'un fichier 32 bits	166
5.2.2	Quelques méthodes d'infection	173
Chapitre 6 – Les vers		193
6.1	Activation	193
6.2	Classification	194
6.2.1	Langage interprète	194
6.2.2	Langage compilé	203
6.2.3	Méthodes de réplication	204
Chapitre 7 – Macro-virus et virus de script		211
7.1	Macro-virus	211
7.1.1	Mode de Fonctionnement sous Word	213
7.1.2	Mode de fonctionnement sous Excel et PowerPoint	216
7.1.3	Un cas particulier : XF/PAIX	217
7.1.4	Virus sous Access	217
7.2	Virus de script	219
7.2.1	VBScript	219
7.2.2	Java et JavaScript	220
7.2.3	Traitement par lot	220
Chapitre 8 – Les logiciels anti-virus		221
8.1	Les méthodes de détection	221
8.1.1	La recherche par signature	222
8.1.2	La recherche générique	225
8.1.3	Le contrôle d'intégrité	228
8.1.4	La recherche heuristique	229
8.1.5	Le monitoring de programmes	231
8.2	Les principaux concepteurs de produits anti-virus	231
Chapitre 9 – Organiser la lutte anti-virale		235
9.1	Les grandes règles à respecter	235
9.1.1	Les ressources propres à l'utilisateur	236
9.1.2	Les ressources partagées	237
9.1.3	Les passerelles	237
9.1.4	Le monde extérieur	238
9.1.5	La dimension humaine	238
9.1.6	La politique des mises à jour	239

9.2	Techniques de protection	239
9.2.1	Les anciennes méthodes	240
9.2.2	Les suites office	240
9.2.3	Internet explorer	241
9.2.4	Outlook et Outlook Express	242
9.2.5	Windows Scripting Host	244
9.2.6	Simple et doubles extensions	244
9.2.7	L'extension SHS	246
9.2.8	Paramètres réseau	247
9.3	Choisir son anti-virus	249
9.3.1	Les benchmarks	249
9.3.2	Se faire sa propre opinion	250
9.3.3	Testez votre anti-virus	251
9.4	Le poids d'une infection virale pour l'entreprise	253
	Chapitre 10 – Dernières évolutions et perspectives	259
10.1	Les buts recherchés	260
10.2	Envahir nos machines	261
10.3	S'affranchir de l'utilisateur, gagner en vitesse, diminuer en taille	267
10.3.1	CODERED	267
10.3.2	SLAMMER	269
10.4	Utiliser des failles	271
10.5	Distribuer une porte dérobée	277
10.6	Porter atteinte à la confidentialité	280
10.7	Faire la collecte de mots de passe	280
10.8	Savoir se mettre à jour	283
10.9	Intégrer de multiples techniques de propagation	286
10.10	Investir les modes poste à poste	287
10.11	Usurper intelligemment les adresses	288
10.12	Rechercher l'aval de l'utilisateur	288
10.13	L'invasion des robots	291
10.14	Conclusion : la fin de l'enfantillage – L'appât du gain	295
	Abréviations et glossaire	297
	Index	305

Avant propos

L'idée d'écrire ce livre m'est venue après avoir écouté les interrogations et les commentaires de nombreux curieux. Parfois disponibles au sein d'actes de conférences quasi privés ou à l'intérieur de revues à la diffusion limitée, il m'est très vite apparu que beaucoup d'informations étaient introuvables. Cette constatation m'a encouragé à poursuivre ma démarche.

Même si mon but initial fut d'intéresser le plus grand nombre, ce livre cible un public d'informaticiens et de spécialistes. Je souhaite leur montrer une autre vision du phénomène virus : celle du *chasseur* et non pas celle du créateur. Vous n'apprendrez pas à écrire des virus mais, au fil des chapitres, vous comprendrez mieux comment on les combat.

Pour débiter notre voyage, nous positionnerons les infections informatiques dans la pyramide sécuritaire. Nous en déroulerons ses diverses facettes pour comprendre *qui est qui* et *qui fait quoi* dans cette nébuleuse malveillante.

Afin de comprendre les enjeux actuels, il est indispensable de connaître l'histoire du phénomène virus. Il s'agit d'une histoire passionnante avec une étonnante galerie de personnages. Elle est pleine de rebondissements et se rapproche parfois du triller et de la science-fiction. Par cette découverte nous entrerons dans le cœur du sujet.

Sachant où se situe notre ennemi et quelle est son histoire, nous le décrirons dans ses multiples formes. Les divers types de virus et de vers seront déclinés selon leurs cibles et leurs attributs. Avec les virus programmes, nous rentrerons dans le cœur du métier. Ce chapitre, ainsi que celui dédié aux vers, risque d'effrayer certains lecteurs. Il me fallait trouver une méthode pour vous amener à *voir avec l'œil du chercheur*. J'ai donc manié l'hexadécimal et la visualisation des fichiers qu'il nous propose. En vous faisant appréhender la structure interne des fichiers modernes j'ai voulu donner une forte plus-value à ce livre.

Nous aborderons ensuite la protection anti-virale dans ses aspects théoriques, pratiques autant que méthodologiques. Ayant expliqué les méthodes, des pistes seront ouvertes pour aider le professionnel dans sa quête d'un bon anti-virus.

Les produits du marché sont souvent performants, ils n'excluent pas la mise en pratique de quelques conseils de configuration qui se doivent de les compléter.

Pour conclure, partant des faits marquants depuis l'an 2000, ce livre démontrera que les auteurs de virus d'aujourd'hui ne cherchent plus, ni à détruire, ni à détériorer des informations. Il mettra à jour leurs buts actuels qui, plus discrets, sont souvent bien plus préjudiciables.

Voilà donc l'itinéraire de ce livre. Pour prolonger le parcours, de nombreux liens bibliographiques vous seront offerts tout au long de votre lecture. Si le jargon technique vous laissait un temps désorienté, un glossaire que j'ai souhaité important et un index devraient vous aider à retrouver votre chemin.