

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