



Éric Filiol

Collection IRIS
dirigée par Nicolas Puech



Les virus informatiques : théorie, pratique et applications



Springer



INRIA

2-004-266-1.

2-004-266-1

Éric Filiol



Les virus informatiques : théorie, pratique et applications



Springer

Table des matières

Avant-propos	VII
Préface	IX
Première partie - Les virus : genèse et théorie	
1 Introduction	3
2 Les bases de la formalisation	7
2.1 Introduction	7
2.2 Les machines de Turing	8
2.2.1 Machines de Turing et fonctions récursives	8
2.2.2 Machine de Turing universelle	13
2.2.3 Problème d'arrêt et décidabilité	15
2.2.4 Fonctions récursives et virus	16
2.3 Les automates auto-reproducteurs	18
2.3.1 Modèle mathématique du modèle de von Neumann	19
2.3.2 L'automate auto-reproducteur de von Neumann	27
2.3.3 L'automate de Langton	30
Exercices	33
Projets d'études	34
Étude du théorème de Herman	34
Programmation de l'automate de Codd	36
3 La formalisation : F. Cohen et L. Adleman (1984 - 1989) ..	37
3.1 Introduction	37
3.2 La formalisation de Fred Cohen	39

3.2.1	Concepts de base et notations	39
3.2.2	Définitions formelles des virus	41
3.2.3	Étude et propriétés des ensembles viraux	44
3.2.4	Formalisation de la lutte antivirale	49
3.2.5	Modèles de prévention et de protection	53
3.2.6	Résultats expérimentaux	58
3.3	La formalisation de Leonard Adleman	62
3.3.1	Notations et concepts de base	63
3.3.2	Virus et infections informatiques	66
3.3.3	Complexité de la détection	69
3.3.4	Étude du modèle isolationniste	72
3.4	Conclusion	73
	Exercices	74
	Projets d'études	75
	Programmation de la machine du théorème 8	75
	Programmation de la machine du théorème 11	76
4	Taxonomie, techniques et outils	77
4.1	Introduction	77
4.2	Aspects généraux des infections informatiques	79
4.2.1	Définitions et concepts de base	79
4.2.2	Diagramme fonctionnel d'un virus ou d'un ver	81
4.2.3	Les cycles de vie d'un virus ou d'un ver	82
4.2.4	Comparaison biologique/informatique	86
4.2.5	Données et indices numériques	88
4.2.6	La conception d'une infection informatique	91
4.3	Les infections simples	93
4.3.1	Les bombes logiques	94
4.3.2	Les chevaux de Troie et leurres	94
4.4	Les modes d'action des virus	97
4.4.1	Virus par écrasement de code	97
4.4.2	Virus par recouvrement de code	98
4.4.3	Virus par entrelacement de code	100
4.4.4	Virus par accompagnement de code	103
4.4.5	Virus de code source	107
4.4.6	Les techniques anti-antivirales	111
4.5	Classification des virus et des vers	115
4.5.1	Nomenclature des virus	116
4.5.2	Nomenclature des vers	133
4.6	Outils et viralogie informatique	139

Exercices	141
5 La lutte antivirale	143
5.1 Introduction	143
5.2 La lutte contre les infections informatiques	145
5.2.1 Les techniques antivirales	147
5.2.2 Le coût d'une attaque virale	154
5.2.3 Les règles d'hygiène informatique	155
5.2.4 Conduite à tenir en cas d'infection	157
5.2.5 Conclusion	161
5.3 Aspects juridiques de la virologie informatique	161
5.3.1 La situation actuelle	162
5.3.2 Évolution du cadre législatif : la loi pour l'économie numérique	164

Deuxième partie - Les virus : pratique

6 Introduction	171
7 Les virus interprétés	175
7.1 Introduction	175
7.2 Création d'un virus en Bash sous Linux	176
7.2.1 La lutte contre la surinfection	178
7.2.2 La lutte anti-antivirale : le polymorphisme	180
7.2.3 Accroissement de la virulence de <i>vbash</i>	184
7.2.4 Placement d'une charge finale	186
7.3 Quelques exemples réels	187
7.3.1 Le virus UNIX_OWR	187
7.3.2 Le virus UNIX_HEAD	188
7.3.3 Le virus UNIX_COCO	189
7.3.4 Le virus UNIX_BASH	189
7.4 Conclusion	193
Exercices	193
Projets d'études	194
Virus chiffré en PERL	194
Scripts de désinfection	195

8	Les virus compagnons	197
8.1	Introduction	197
8.2	Le virus compagnon <code>vcomp_ex</code>	200
8.2.1	Étude détaillée du code de <code>vcomp_ex</code>	201
8.2.2	Les faiblesses du virus <code>vcomp_ex</code>	209
8.3	Variantes optimisées et furtives de <code>vcomp_ex</code>	211
8.3.1	Variante <code>vcomp_ex_v1</code>	211
8.3.2	Variante <code>vcomp_ex_v2</code>	219
8.3.3	Conclusion	227
8.4	Le virus compagnon <code>vcomp_ex_v3</code>	228
8.5	Un virus compagnon hybride : <code>Unix.satyr</code>	231
8.5.1	Description du virus <code>Unix.satyr</code>	231
8.5.2	Étude détaillée du code d' <code>Unix.satyr</code>	232
8.6	Conclusion	238
	Exercices	239
	Projets d'études	243
	Contournement d'un contrôle d'intégrité	243
	Contournement du contrôle de signature de RPM	243
	Récupération de mot de passe	244
9	Les vers	245
9.1	Introduction	245
9.2	Le ver Internet	247
9.2.1	L'action du ver Internet	248
9.2.2	Les mécanismes d'action du ver Internet	249
9.2.3	La gestion de la crise	253
9.3	Analyse du code d' <code>IIS_Worm</code>	253
9.3.1	Débordement de tampon	254
9.3.2	Faible <code>IIS</code> et débordement de tampon	260
9.3.3	Étude détaillée du code	261
9.3.4	Conclusion	273
9.4	Analyse du code du ver <code>Xanax</code>	273
9.4.1	Action principale : infection des <i>emails</i>	274
9.4.2	Infection des fichiers exécutables	280
9.4.3	Infection via les canaux IRC	283
9.4.4	Action finale du ver	286
9.4.5	Procédures diverses	288
9.4.6	Conclusion	294
9.5	Analyse du code du ver <code>UNIX.LoveLetter</code>	294
9.5.1	Variables et procédures	295

9.5.2	L'action du ver	302
9.6	Conclusion	303
	Exercices	304
	Projets d'études	305
	Analyse du code du ver Apache	305
	Analyse du code du ver Ramen	306

Troisième partie - Les virus : applications

10	Introduction	309
11	Virus et applications	313
11.1	Introduction	313
11.2	État de l'art	317
11.2.1	Le ver Xerox	320
11.2.2	Le virus KOH	321
11.2.3	Les applications militaires	325
11.3	La lutte contre le crime	327
11.4	Génération environnementale de clefs cryptographiques	329
11.5	Conclusion	334
	Exercices	334
12	Les virus de BIOS	337
12.1	Introduction	337
12.2	Structure et fonctionnement du BIOS	340
12.2.1	Récupération et étude du code BIOS	341
12.2.2	Étude détaillée du code BIOS	342
12.3	Description du virus VBIOS	346
12.3.1	Concept de secteur de démarrage viral	346
12.4	Implémentation de VBIOS	350
12.5	Perspectives et conclusion	352
13	Cryptanalyse appliquée de systèmes de chiffrement	355
13.1	Introduction	355
13.2	Description générale du virus et de l'attaque	357
13.2.1	Le virus V_1 : première étape de l'infection	358
13.2.2	Le virus V_2 : seconde étape de l'infection	358
13.2.3	Le virus V_2 : la cryptanalyse appliquée	360
13.3	Description détaillée du virus YMUN20	361

13.3.1 Le contexte	361
13.3.2 Le virus YMUN20- V_1	362
13.3.3 Le virus YMUN20- V_2	365
13.4 Conclusion	368
Projet d'études : programmation du virus YMUN20	368

Conclusion

14 Conclusion	371
Avertissement sur le CDROM	375
Références	377
Index	385