



David Harley, Robert Slade & Urs E. Gattiker

VIRUS

Définitions, mécanismes et antidotes

Collection

Référence


CampusPress

www.campuspress.net



005-444-1

2-005-444-1

Table des matières

Virus

Définitions, mécanismes et antidotes

David Harley, Robert Slade
et Urs E. Gattiker




CAMPUSPRESS

Retrouvez
tous nos livres sur
www.campuspress.net

Table des matières

Introduction	1
Pourquoi cet ouvrage ?	1
En quoi cet ouvrage est-il différent ?	1
A qui s'adresse cet ouvrage ?	3
Structure de cet ouvrage	5
A quoi devez-vous vous attendre ?	6

Partie I

Le problème

Chapitre 1. Définitions fondamentales	9
Virus informatiques : réalité et imaginaire	10
Définitions	11
Virus et mécanismes de virus	12
Structure des virus	12
Dégâts	13
Dégâts et infection	14
Mécanismes furtifs	14
Polymorphisme	15
Est-ce un livre sur UNIX ?	16
Régime aux vers	17
Chevaux de Troie	17
Dans la nature	18
Guide express des logiciels antivirus	20
En résumé	21

Chapitre 2. Rappel historique	23
La préhistoire des virus : de Jurassic Park à Xerox PARC	24
Trous de vers	24
Core Wars	25
Le ver Xerox (ver segmenté Shoch/Hupp)	26

Les débuts des vrais virus	27
1981 : un virus Apple II	27
1983 : Elk Cloner	28
1986 : © BRAIN	30
1987 : bonsoir Vienna, bonjour Lehigh	31
1988 : la période des vers	33
L'âge d'Internet	36
1989 : les vers, Dark Avenger et AIDS	36
1990 : virus polymorphes et à cibles multiples	38
1991 : virus de la Renaissance et Tequila Sunrise	39
1992 : la revanche de la tortue (Turtle)	40
1993 : le polymorphisme règne en maître	42
1994 : Smoke Me a Kipper	43
1995 : virus de macros pour Microsoft Office	44
1996 : Mac, macros, l'univers et tout le reste	45
1997 : canulars et pyramides	46
1998 : ce n'est pas un canular	46
1999 : et voici le 19 ^e crash de votre serveur	47
2000 : l'année du virus/ver VBScript	50
Et ça continue... ..	55
En résumé	55
Chapitre 3. Définition des logiciels malveillants	57
Que font les ordinateurs ?	58
Fonctions des virus	58
Fonctionnalités des applications et sécurité	59
Virus dans la nature et grands nombres absolus	59
Que détectent les programmes antivirus ?	62
Les virus	64
Les vers	66
Les intendeds : virus intentionnels	67
Altérations	69
Germe	69
Injecteurs	69
Virus de test	70
Générateurs	71
Chevaux de Troie	71
Voleurs de mots de passe et backdoors	75
Blagues	76

Outils d'accès à distance	79
Agents DDoS	80
Rootkits	82
Fausses alarmes	82
En résumé	84
Chapitre 4. Activité et fonctionnement des virus	87
Comment écrire un virus ?	89
Structure tripartite	92
Mécanisme d'infection	92
Déclencheur	93
Charge	94
Reproduction	95
Virus non résidants	96
Virus résidants en mémoire	96
Virus hybrides	98
Généralité, étendue, persistance	98
Charge et reproduction	100
Dégâts	101
Impact de l'infection virale sur l'environnement informatique	102
Dégâts directs des charges de virus et de chevaux de Troie	103
Dégâts psychologiques et sociaux	103
Dégâts secondaires	104
Dégâts matériels	104
Interdire la bombe	105
Bombes logiques	106
Bombes à retardement	106
Bombes ANSI	106
Bombes de courrier et d'abonnement	107
En résumé	107
Chapitre 5. Mécanismes des virus	109
Les virus spécifiques du matériel	110
Agents infectieux de secteur de démarrage	110
La zone de démarrage	115
Les agents infectieux de fichiers	117
Ajouter avant ou après	120
Virus écraseurs	121
Fausse direction	123

Virus compagnons	123
Les virus à cibles multiples (multipartite)	125
Les virus interprétés	126
Virus de macros	127
Virus de scripts	128
Les mécanismes de dissimulation	129
Furtivité	132
Polymorphisme	135
Ingénierie sociale et logiciels malveillants	137
En résumé	140

Partie II

Solutions système

Chapitre 6. Vue d'ensemble des technologies contre les logiciels malveillants	143
Les grandes attentes	143
Comment gérer les virus et leurs menaces ?	146
Mesures préventives	147
Que font les logiciels antivirus ?	155
Au-delà du bureau	166
Sous-traitance	173
En résumé	174
Chapitre 7. Gestion des logiciels malveillants	175
Définition de la gestion des logiciels malveillants	176
La gestion anticipative	177
Gestion réactive	189
Comparaison entre le coût de propriété et les coûts de gestion	191
En résumé	195
Chapitre 8. Collecte des informations	197
Comment savoir si un conseil est fiable ou utile ?	198
Livres	200
Ouvrages de référence	200
Ouvrages utiles	201
Ouvrages déconseillés	202
Sujets annexes	203

Sécurité générale	204
Aspects éthiques	207
Fiction	207
Ressources en ligne	209
Listes de diffusion et newsgroups	210
Scanners gratuits	211
Scanners en ligne	212
Encyclopédies	212
Canulars de virus et fausses alertes	213
Evaluation et critiques	214
Vendeurs d'antivirus	214
Ressources générales	215
Articles divers	216
Conseils d'ordre général	216
Vulnérabilité et virus particuliers	217
Références générales sur la sécurité	220
Chapitre 9. Evaluation et test des produits	223
Principaux problèmes	224
Prix	224
Performances	230
Ce n'est pas mon réglage par défaut	237
Test Match	255
Virus en circuit fermé	260
Nous avons apprécié EICAR	264
Informations complémentaires	267
En résumé	268
Chapitre 10. Gestion des risques et des incidents	269
Gestion des risques	270
La meilleure méthode de défense : la préparation	272
L'ordinateur	272
Le bureau	273
La maintenance préventive	276
En toute sécurité, la première fois	278
Incidents de virus signalés	280
Enquêtes du service d'assistance	280
Gérer les incidents de virus	281
Identification des virus	284

Politiques de protection générale	284
En résumé	285
Chapitre 11. Administration des utilisateurs	287
Administration de la direction	288
Les politiques comptent	289
Sécurité et assurance	289
Virus et assurances	290
Analyse des risques et des impacts	290
Perte de productivité, déni des coûts du service	291
Effets non observés	291
Effets observés	291
Dommages psychologiques suite à l'incident	292
Prix de la gestion	292
Coûts préalables à la mise en place	293
Analyse des coûts	293
Boucle des commentaires de la direction	294
Formation et éducation	294
Problèmes de politiques	294
Service d'assistance	296
Autres personnels de support informatique	299
Sécurité informatique et autres services	300
Formation et éducation	300
Renforcement positif	304
Gestion anticipative des logiciels malveillants	305
Instructions pour des pratiques sécurisées	305
Vérifier toutes les alertes et avertissements auprès du service informatique	305
Ne jamais faire confiance aux pièces jointes	305
Faire attention aux newsgroups et sur le Web	306
Ne pas installer de programmes non autorisés	307
Prendre garde aux documents Microsoft Office	307
Utiliser et demander des formats de fichiers plus sûrs	308
Continuer à utiliser les logiciels antivirus	308
Assurer la mise à jour de votre antivirus	309
"A jour" n'est pas synonyme "d'invulnérable"	309
Les superutilisateurs ne sont pas surhumains	309
Désactiver l'amorçage des disquettes	309
Disquettes protégées en écriture	310
Eviter le bureau	310

Réfléchir à son logiciel de messagerie et de news	310
Afficher toutes les extensions dans l'Explorateur de Windows	311
Désactiver Windows Script Host	311
Introduire l'analyse générique des courriers	311
Utiliser les ressources de sécurité de Microsoft	311
S'abonner aux listes de fournisseurs d'antivirus	312
Tout analyser	312
Ne pas se fier aux logiciels antivirus	312
Sauvegarder, sauvegarder, sauvegarder	313
Gestion des rumeurs	314
Formulaire de réponse	314
Guide rapide des rumeurs	315
En résumé	316

Partie III

Cas d'étude : que s'est-il passé, quelles leçons en tirer ?

Chapitre 12. Cas d'étude : la première vague	319
Le virus Brain	320
Qui a écrit le virus Brain ?	320
Les variantes Ohio et Den Zuk	322
Le virus MacMag	323
Que la paix soit avec vous	324
Le virus publicitaire	326
Des macros par milliers	327
Le virus Scores	328
Le virus Lehigh	330
CHRISTMA EXEC	331
Le ver Morris Worm (Internet Worm)	332
Le ver WANK	336
Jerusalem	337
Le cheval de Troie AIDS	339
Stoned, le monde est stone	340
Michelangelo, Monkey et autres variantes de Stoned	341
Le virus Monkey	346
Le virus Form	348
Le virus Modem	349

Le virus de l'imprimante iraquienne	350
En résumé	354
Chapitre 13. Cas d'étude : la deuxième vague	355
Black Baron	357
Good Times	358
Les messages et le texte	359
Le "vrai" Good Times	359
Qu'est devenu le virus Good Times ?	359
Good Times ou le big-bang électronique	360
Prototypes de virus	361
Différence entre un programme et des données	362
Entrée de Concept dans l'histoire des virus	363
Quand est-ce qu'une charge n'en est pas une ?	364
Macros automatiques	366
L'empire contre-attaque... oui mais à son rythme !	367
WM/Nuclear	368
Colors	371
DMV	372
Wiederoffnen et FormatC	372
Green Stripe et Wazzu	373
WM/Atom	374
WM/Cap	374
Les virus d'Excel	375
Variations sur le même thème	377
Word 97	378
ShareFun	379
Nomenclature des virus de macros	379
Techniques contre les virus de macros	380
Hare	383
Chernobyl (CIH/Spacefiller)	383
Esperanto	385
En résumé	386
Chapitre 14. Cas d'étude : la troisième vague	387
Le ver AutoStart	388
W97M/Melissa (Mailissa)	390
Conditions à la propagation de Melissa	390
Mode de propagation de Melissa	391

Divulgation du code source	392
Melissa : le virus force de vente	393
Une propagation foudroyante	393
W32/Happy99 (Ska) : le virus à valeur ajoutée	394
PrettyPark	395
L'apparition des virus de scripts	396
VBS/Freelink	397
VBS/LoveLetter	398
VBS/NewLove-A	401
Le ver 911	402
VBS/Stages	403
BubbleBoy et KAKworm	404
MTX	405
Naked Wife	408
W32/Navidad	408
W32/Hybris	410
VBS/VBSWG.J@mm (Anna Kournikova)	411
VBS/Staple.a@mm	412
Les vers Linux	413
Ramen	413
Linux/Lion	413
Linux/Adore (Linux/Red)	414
Lindose (Winux)	414
W32/Magistr@mm	415
BadTrans	416
En résumé	417

Partie IV

Aspects sociaux

Chapitre 15. Origines et propagation des virus	421
Qui peut bien écrire tout ça ?	423
Ingénierie sociale	424
Définitions de l'ingénierie sociale	426
Les voleurs de mots de passe	429
C'est personnel	430
Pourquoi écrivent-ils tout ça ?	431
Diffusion	436

Un minimum d'éducation peut-il résoudre le problème ?	437
L'éducation pour tous	439
En résumé	440
Chapitre 16. Métavirus, rumeurs et fléaux associés	441
Chaînes de lettres	443
Rumeurs	444
Légendes urbaines	444
Chaînes de lettres et rumeurs	445
Rumeurs et alertes au virus	446
Mauvaises informations et confusions	447
BIOS, CMOS et Battery	447
La rumeur JPEG	448
Le virus Budget	449
Amère désillusion	450
Nous n'avons pas les mêmes valeurs	450
Méthodes d'identification d'une rumeur	451
Spam, spam, spam	460
Motivations	461
Types de spamming	463
Etude du spamming et des virus	463
Métavirus et gestion de l'utilisateur	465
Que dois-je dire à mes clients ?	466
Traiter le spamming, les chaînes de lettres et les fausses alertes	467
En résumé	469
Chapitre 17. Responsabilité, morale et éthique	471
Petit guide d'éthique	472
Statistiques démographiques	475
Age	475
Sexe	477
Normes culturelles et nationales	478
Identités nationales	478
Motivations	482
Différences entre nations	482
Connaissances et éthique	483
Utilisateurs finaux et responsabilité	484
La recherche antivirus est-elle une profession ?	486
Vendeurs et éthique	487

Ethique commerciale	489
A tort et à travers	491
Développement de codes de conduite	491
Code de conduite minimal	491
EICAR	492
Article 1 : Intérêt public	493
Article 2 : Soumission aux lois	494
Article 3 : Devoirs envers les employeurs, les clients et les collègues	494
Article 4 : Devoirs envers la profession	494
Article 5 : Compétences des spécialistes	494
Les codes de conduite font-ils la différence ?	495
En résumé	498
Chapitre 18. Conclusion	501
Prédictions	501
Conclusion	503
Mauvaises nouvelles : les spécialistes de la sécurité ne connaissent pas vraiment les virus	503
Bonne nouvelle : quelques connaissances et des stratégies de base sont une aide	503
Mauvaise nouvelle : la convergence va empirer	505
Bonne nouvelle : les mêmes en plus nombreux	505
Mauvaise nouvelle : les multiples points d'attaque peuvent aggraver le problème	506
Bonne nouvelle : les outils existants et un peu d'attention sont une aide	507
Dernière minute	507
Le RTF n'est pas la panacée	507
Poly/Noped	509
Mandragore	509
Rumeur SULFNBK	510
Sadmind	510
Cheese	511
Lindose/Winux	511
MacSimpsons	512
Outlook View Control	512
Code Red/Bady	512
Sircam	513
En résumé	514
Glossaire	515
Index	535