

Index

Nombres

097M/TRISTATE 72

1260 54

20/20 22

29A 73, 104, 130, 179, 283,
284

3APA3A 62

40Hex 60, 61

A

A2KM/Sadip@MM 217

A97M/Accessiv 217

A97M/Cross 218

A97M/Tox 218

Adam Levitt 38

Adware 22

AIDS-II.8064 57

ajout 159

Alameda 51

Alan Solomon 49, 54, 58

Anticmos 69 154

Anti-Congo 41

anti-debugging 101

Antiexe 69, 89

anti-virus 221, 231

Anti-Virus Toolkit from S&S
49

appender 160

Applets Java hostiles 28

APStrojan@MM 209

ARCV 63

Arj-virus 62

Arthur Burks 36

AVERT 64, 83

AVP 50

B

Baby 109

Back Orifice 31

backdoor 26

BackDoor-JW 29

BadGuy 158

BatMan 62, 220

BBS 53

Beast 58

Benny 104, 283

BHO 23

BIOS 133, 136

Bit Addict 60

Bizatch 66

Black Baron 60, 63

Black Wolf 60

blended threat 107

bombe logique 25

BOOT 88

Boot Sector 88, 132

botnet 292

Brain 45, 46, 51

buffer overflow 209

C

C-4 48

canulars 18

CARO 58, 107, 111, 125

Cascade 47, 49, 51, 109, 161

cavité 162, 187

Chameleon 54

checksum 48

Chen Ing-hau 70

Cheval de Troie 26, 112

Chile Mediera 104

Chk4Bomb 48

Christoph Fischer 58

Civil_War 110

CLUSIF 2, 49, 76, 254, 263,
293

cluster 139, 164

CNIL 11

cocktail 107

code checksum 228

code complémentaire 136,
142, 148, 152, 153

CodeBlue.worm 287

CodeRed 268

Columbus Day 49

Commander Bomber 54, 62

compagnons 164

contrôle d'intégrité 48, 228

Core War 37

CPW 104

Craig Sch mugar 83

CreateObject 196

CREEPER 37

Cruncher 61

cryptage 47, 102, 215

D

DAME 60

Dark Angel 60

Dark Avenger 53
Dark Slayer 60
Datacrime 48, 51
 David Gerrold 39
 David L. Smith 75
 DDM 13
 débordement de tampon 209
 délimiteurs 111
 délocalisé 57, 164
Den Zuko 47, 51, 153
 deni de service (DoS) 32
 déni de service distribué (DDoS) 33
 dévolution 111, 122
 DGME 60
 dialers 30
DIR-II 57
Dmsetup.worm 203
 DMU 60
 DMV 64
 Dr Solomon 70, 74
 dropper 79, 89, 112
 DSME 60
 dump mémoire 113
 duplication 94

E

Eddy Willems 59
EDV 151
 EICAR 58
 eicar.com 251
Elk Cloner 40
 en-tête des sections 170
 en-tête MS-DOS 167
 en-tête optionnelle 168
 en-tête PE 167
 entrelacement 162
 EntryPoint RVA 169
 Eudora 210
 Eugène Kaspersky 50, 62, 287
EXEBug 62, 150
 Executable Linkable Format 94
 exploit 271

F

farces 18
 fast infector 53
Father Christmas Worm 44
Flip 55, 154
 flooding 32
 Flu_shot 48
Form 69, 89, 142, 153
 F-Prot 50
 F-PROT Development 64
 fractionnement 163
 fraude 419 14
 Fred Cohen 34, 41
 Fridrik Skulason 47, 50, 58, 107
FriendGreetings 289
Frodo 57, 107
Frogbender 18
 FSMN 111
Fu Manchu 51
 furtivité 45, 55, 57, 61, 106, 151, 215, 218

G

Gaobot 267, 291
 garbage 113, 181
 GenB 109
 générateurs de virus 59
 GenP 109
Genvirus 59
Good Times 64
Gotcha 54, 110
 GP1 57
Grammersoft 78
GriYo 104
GT-Spoof 64
 Gunther Musstopf 58
 Gunther von Gravenreuth 58

H

Hackers 47
Happy-99 72
HLL.C 109
HLL.ow 109

HLLC 109
HLLLO 109
HLLP.Toadie@MM 199
HLLT/Toadie@MM 98
HLLW.Idomoshe 96
 hoax 6, 64
Homepage 80, 91
Horse Boot 89
 Hijackers 23

I

IBM Christmas Tree 43
IBM V SCAN 49, 50
 Image Base 169
 implanteurs 89, 112
 infecteur rapide 53, 55, 107
 injecteurs 89, 112
 Instant Messenger 209
 intended 112, 125
 interruptions 134
Intruder 56
 IRC 203
IRC/Acoragil 203
IRC/Theme.worm 203

J

Jan Hruska 54
 JavaScript 91
Jérusalem 46, 48, 49, 51, 109, 160
 Jimmy Kuo 65
 Joe Wells 56, 63
 John Brunner 39
 John Louis von Neumann 35
 John McAfee 48, 50
 John Shoch 34, 38, 40
 jokes 18
 Jon Hupp 34, 38, 40
JS/Kak@M 72, 78, 80, 91, 98, 194
JS/TheFly@MM 91, 98
 JUMPER 69
Jumper.B 69, 89, 148, 153
 JUNKIE 69

K

keylogger 27
 KeyLog-SSKC 27
Kilroy 56
 kit 112
 Klaus Brunnstein 58

L

Lehigh 46, 51, 162
 lettres chaînes 8
 Linear Executable 94, 127
 Linux 129
Linux/Bliss 130
Linux/Etap 130
Linux/Radix.ow 158
Linux/Simile 130
 Lowsan 81

M

MAC/Simpsons@MM 98
 Macintosh 128
MacOS/Autostart 128
MacOS/Simpsons@MM 128
 macro-virus 51, 65, 67, 72, 90,
 194, 211, 261
Mafia.a 27
Maltese Amoeba 55
Manta 60
 MAPI 206
 Marc Blanchard 283
Marijuana 47
 Marius Van Oers 65
 Mark Ludwig 56, 60
 mass-mailer 72, 80, 94, 97,
 112, 124, 128, 196, 261
Mass-Produced Code Generator
 60
 Master Boot Record (MBR)
 88, 132
Masud Khafir 54, 60, 61
 MBR 88
 McAfee 64
 McAfee Associates 69
Mental Driller 130
 MessageLabs 83
 métamorphisme 103
 Michael Weiner 58
Michelangelo 59

micro-programme mode réel
 167
 Mikko Hypponen 104
Mini 109
Minimal 109
 minus-virus 50
Moloch 154
 moniteur de virus 225
 monitoring de programme 48,
 231
Monkey 63, 69, 152
 Morton Swimmer 58
 Mozilla 248
 MtE 110
MtE.Pogue 54
 MTX_II 79
 multi-application 213
 multipartite 54, 57, 61, 89,
 154, 213, 218
Murphy 58
Mutation Engine 53

N

Natas 61
NetBus Pro 32
 Network Associates Inc. 69
Neurobasher 62, 105
 New Executable 92
 Nick FitzGerald 111, 196
 NNTP 210
 nom de famille 108, 120
 nom de groupe 109, 121
Nomenclatura 58
 Norton Antivirus 56
Nowhere Man 60
NuKE 60
 nuker 33

O

O97M/Cybernet@MM 98
O97M/Shiver 196
O97M/Tristate 114, 196
 Objets Active-X hostiles 29
 offset 146
 oligomorphiques 102
Omicron 55
One_Half 61, 89, 154, 162
 Onel de Guzman 76

opcodes 102, 181
 OS/2 127
OS2.AEP 67
OS2/AEP 127
OS2/DA 67
OS2/Jiskefet 127
OS2/Myname 127
OS2first 67

P

P97M/Phlaco 216
P97M/Yesi 216
PalmOS/Phage 79
 pare-feu 236
Parity Boot 69, 89
 partition récursive 153
 PassWord Stealer (PWS) 27,
 280
 Paul Ducklin 58
 Paul Langemeyer 58
 payload 33, 104
 PDF 199
Peach 106
 Pegasus 199, 210
 Peter Denning 34
 Peter Haag 293
 Peter Troxler 293
Phalcon/Skism 60
 phishing 15, 293
 PIF 246
PIF/Fable@MM 98
Ping-Pong 46, 51
 plate-forme 113
 plug-ins 284, 285
 Ply 102
Pogue 110
 point d'entrée obscur 159, 184
 polymorphie 53, 54, 55, 61, 62,
 63, 103, 154, 180, 216
Porn-Dialer 30
 Portable Executable 93, 165
 porte dérobée 26, 277
 poste à poste 81, 99, 201, 208
Prank 65
 prepender 160
 prévisualisation 194
Priest 61
 programmes simples 19
 propagation 94

Proxy-Guzu 30
 PS-MPC 60
 PWS-Hooker.dll 27, 281

Q

Qark 64
 Quantum 66

R

Rabbit 71
 Rainbow 63, 152
 Randex 291
 rang de variante 109, 110, 111, 122
 Real-Mode Stub Program 167
 REAPER 37
 recherche générique 225
 recherche heuristique 229
 recherche par signature 222
 recouvrement 158
 récursivité 112, 125
 renifleur de clavier 27, 281
 renifleurs de mot de passe 27, 280
 renifleurs de trafic 32
 rétro-virus 62, 104
 RHINCE 64
 robots 267, 291
 Roger Riordan 59
 Roger Riordan 50
 RTF 287
 RTM Worm 43
 rumeurs 6
 Rush Hour 46
 RVA 169

S

Sarah Gordon 65, 67
 Satanbug 106
 scam africain 14
 ScanProt 65
 Sdbot 267
 secteur de démarrage 88, 109, 132
 secteur de partition 88, 109, 132
 secteur logique 137, 139, 146
 secteur physique 137, 146

Sendkeys 195
 Sentry 48
 ShellScrap 246
 Shifting Objectives 62
 SHS 246
 signature du virus 160
 Silly 109
 singularité 108, 110, 112, 123
 Slider joke 18
 Small 109
 SMEG 60
 SMEG-Pathogen 63
 SMTP 204
 smurfing 32
 Sniff-ICQ.WPD 32
 socket 205
 Socket de Troie 31
 Socket23 278
 Sophos 54
 spam 293
 spamming 11
 Spanska 72
 spoofing 32, 205
 Spybot 267, 291
 Spyware 23
 Staog 67
 Starship 57
 Stealth 56
 Stoned 46, 51, 59, 69
 Stoned-Spirit 153
 Stream NTFS 191
 SubSeven 285
 Symantec 56

T

table d'allocation des fichiers (FAT) 140
 taille 121
 TbScan 229
 Tchernobyl 70
 Tequila 55, 89, 106, 154
 Thomas Ryan 40
 Thread Local Storage 189
 Timid 56
 Tiny 58, 109
 TLS 189
 TPE 60
 TPE.1_0.Girafe 60
 trashbin 113

Tremor 62, 105
 TridentT 54, 60
 trigger 33
 Trivial 108
 trojan 20, 26, 112

U

Ultimate Mutation Engine 60
 Univ 109
 Unix 129

V

V2P1 54
 Vaccine 54
 VBS/BubbleBoy@MM 78, 195
 VBS/Davina@MM 30
 VBS/Entice.ow 158
 VBS/FreeLink@MM 91, 98
 VBS/GWV 99, 201
 VBS/LifeStages@MM 246
 VBS/Loding 198
 VBS/LoveLetter@MM 6, 72, 75, 91, 197
 VBS/Monopoly@MM 91
 VBS/Netlog 96, 201
 VBS/Peachy@MM 197, 199
 VBS/Sludge.worm 201
 VBS/Stages@MM 72
 VBS/Tam@MM 80
 VBS/Timofonica@MM 79
 VBS/TripleSix@MM 91
 VBS/VBS@MM 80
 VBS/VBSWG@MM 91
 VBS/Vierika 198
 VBS/Wobble@MM 6
 VBS/XPMsg@MM 29
 VBSV 71
 VCL 60
 VCS V1.0 60
 Vecna 284
 ver 34, 39, 94, 193
 vers automatiques 100, 209
 Vesselin Bontchev 50, 53, 57, 58, 64, 107, 125
 Vet (Cybec) 50
 VGREP 120
 VicodinES 75, 218
 Vienna 46

- VIRDEM 46
 Virtran 54
 virus 34, 39, 94, 112
 virus Batch 92
 Virus Bulletin 52
 Virus Communication Interfa-
 ce (VCI) 283
 virus compagnon 57
 virus de script 71, 72, 90, 91,
 158, 194, 211, 219, 261
 virus défensif 104
 virus interprètes 89
 virus multipartite 87
 Virus Patrol 74
 virus programme 70, 80, 92,
 157
 virus système 45, 69, 88, 131
 VIRUS-L 53
 VirusScan 50, 69
 VLAD 67
 VLAD#4 64
 VME 60
 vulnérabilité 209, 271
- W**
- W16/RedTeam@MM 98
 W16/Tentacle.1966 61
 W2K/Stream 191
 W32/Android@MM 206
 W32/Anvil 225
 W32/Apparition 103
 W32/Auric@MM 100
 W32/Babylonia@MM 206
 W32/Badtrans@MM 194, 281
 W32/Bagle@MM 94, 288
 W32/Benjamin.worm 81, 99
 W32/BlackBat 102
 W32/Blaster.worm 81, 208
 W32/Blebla@MM 204
 W32/Bolzano 183
 W32/Bugbear@MM 80, 81,
 278, 281
 W32/Bymer.worm 204
 W32/Cabanas 177
 W32/Caw 163
 W32/Chiton 161, 189
 W32/Choke.worm 204, 209
 W32/CodeRed.worm 81, 101,
 208, 268, 277, 287
 W32/Crypto 225
 W32/Dengue 104
 W32/Duksten@MM 210
 W32/Dumaru@MM 82, 98,
 191
 W32/Etap 130
 W32/EXPLOREZIP.worm@M
 72
 W32/ExploreZIP@MM 204
 W32/Fix@MM 204
 W32/Fizzer@MM 80
 W32/Floodnet@MM 209
 W32/Forforo 185
 W32/Fourseman@MM 99
 W32/Frethem@MM 80
 W32/Gnuman.worm 99, 208
 W32/Grand!p2p 223
 W32/Haless 182
 W32/Hayque.worm 96, 208
 W32/HLL.ow.ANT 158
 W32/HLL.ow.Jetto 158
 W32/HLLP.DE TROIE 69
 W32/Hybris@MM 72, 80, 204,
 285
 W32/Kazmor.worm 99
 W32/Kelino 101
 W32/Klez@MM 80, 84, 105,
 280
 W32/Kriz 189
 W32/Lirva@MM 80, 105
 W32/Lovsan.worm 272
 W32/Maddis.worm 107
 W32/Magistr@MM 80, 204,
 206, 280
 W32/Marburg 70
 W32/Mimail@MM 80, 282
 W32/MTX@MM 72, 204, 206
 W32/Mydoom@MM 83, 94,
 255
 W32/Mylife@MM 204, 207
 W32/MyParty@MM 80
 W32/Nachi.worm 81, 208
 W32/Navidad@MM 72, 80, 207
 W32/Netsky@MM 94
 W32/Newpic.worm 204
 W32/Nimda@MM 81, 205,
 208, 286
 W32/Orez 187
 W32/Parvo@MM 206
 W32/PrettyPack@MM 72, 206
 W32/Sabia.prc 79
 W32/Sasser.worm 208
 W32/Simile 130
 W32/Sircam@MM 80, 81, 205,
 206, 280
 W32/Ska@MM 72, 204, 206
 W32/Smibag.worm 209
 W32/Sobig@MM 14, 80, 81,
 283
 W32/SQLSlammer 81
 W32/SQLSlammer.worm 101,
 208, 269
 W32/SUK 225
 W32/Suppl@MM 206
 W32/Swen@MM 80, 82
 W32/Torvil@MM 210
 W32/Ultimax.worm 30
 W32/Urbe@MM 207
 W32/Yaha@MM 80, 105
 W32/Yarner@MM 224
 W32/Zmist 225
 W95/Anxiety 161, 175
 W95/Babylonia@MM 284
 W95/Boza 66, 173
 W95/CIH 70, 72, 107, 223
 W95/Fono 207
 W95/Kuang 278
 W95/Marburg 180
 W95/MTX 106
 W95/Padania 179
 W95/Parvo@MM 98
 W95/Weird 278
 W97M/AntiMarc@MM 98,
 195
 W97M/Class 68, 72, 75
 W97M/Coldape 71, 196
 W97M/Cross 218
 W97M/Eight941 123
 W97M/Ethan 72
 W97M/Groov 68, 71
 W97M/Jim@MM 199
 W97M/Lucia 198
 W97M/MARKER 72
 W97M/Melissa@MM 72, 74,
 197
 W97M/Mimir@MM 197, 198
 W97M/Moridin@MM 199
 W97M/Nail@MM 197

W97M/NightShade 67
W97M/PolyPoster@MM 195
W97M/Wazzu 67
Welchia 81
Whale 57
WildList 63, 93
Win32/HLLP.DeTroie 278
Winvir_1_4 61
WM/CAP 69, 72, 216
WM/Colors 215
WM/Concept 65, 69, 215
WM/Futurenot 216

WM/Hassle 216
WM/Inexist 69
WM/Johnny 123
WM/MDMA 69, 215
WM/NPAD 69
WM/Rapi 123
WM/Sharefun@MM 98, 195
WM/Wazzu 69, 215
WormNET 283
Worms Against Nuclear Killers
44

X

X97M/Laroux 216
X97M/Papa@MM 98, 197
XF/Paix 68, 69, 217
XM/Laroux 67, 216

Z

zombie 33
Zulu 78