Obsah

Úvod 1

Několik slov autora 2

Upozornění

Úvod 3

Co je to cracking 4

Obecná pravidla pro ochranu před crackingem 5

Markova pravidla 5

Další pravidla 6

Základní programy užívané při crackingu 7

Má vůbec cenu chránit software aneb stejně to někdo crackne 7

Co najdete na přiloženém CD 8

KAPITOLA 1

Stávající způsoby ochrany a jejich zranitelnost 9

1. Zašifrování dat 10

2. Neúplné programy 10

Základní rozdělení dnešních typů ochran 10

Časová omezení 11

Další počtová omezení 14

Registrační číslo 15

Klíčový soubor 20

Funkčně omezené programy 25

Hardwarový klíč 27

Kontrola přítomnosti CD 29

Protikopírovací ochrany datových CD 32

Fyzické chyby na CD 32

Nekorektní soubory (Dummy files) 32

CD delší než 74 minut (Oversized CD) 33

Nekorektní TOC (Illegal Table Of Contents) 33

Velké soubory 33

Softwarové (fiktivní) chyby a jiné zásahy do procesu výroby CD 34

Komerční ochrany 34

SafeDisc 35
SecuROM 36
ProtectCD 36
Armadillo (The Armadillo Software Protection System) 37
ASProtect 37
SalesAgent 38
VBox 39
Programy naprogramované ve Visual Basicu 39
Porovnání řetězců 40
Porovnání proměnných (Variant data type) 40
Porovnání proměnných (Long data type) 41
Konverze datových typů 41
Přemisťování dat 41
Matematika 41
Různé 42
Další velké chyby dnešních ochran 42

KAPITOLA 2
Ochrana před debuggingem 47
Užívané debuggery 48
Základy užívání programu SoftICE 48
Konfigurace programu 49
Základní příkazy, funkce a ovládání 50
Okna 50
Breakpointy 52
Práce s breakpointy 55
SEH – Strukturované ovládání chyb 56
Co je to SEH a jaké je jeho využití 56
Konstrukce s využitím SEHu 57
Užívané algoritmy 58
Algoritmy využívající funkci API CreateFileA 58
BoundsChecker interface a využití přerušení INT 3 59
Využití přerušení INT 1 62
Využití přerušení INT 68h 64
Hledání hodnot v registrech 64
Hledání hodnot v souboru autoexec.bat 65
Breakpointy 66
Softwarové breakpointy 67
Breakpoint na přerušení (BPINT) 67
Breakpoint na spuštění (BPX) 67
Breakpoint na přístup do oblasti paměti (BPR) 68
Hardwarové breakpointy 69
Popis ukázkového programu pro detekci hardwarových breakpointů 70

Pokročilé metody 73
Ring módy 73
Způsoby přechodu mezi Ring3 a Ring0 74
Detekce programu SoftICE pomocí VxDCall 79
Deaktivace klávesové zkratky programu SoftICE 81
Další jednoduché možnosti a využití SEHu 84

KAPITOLA 3
Ochrana před disassemblingem 87
Užívané disassemblery 88
Základy užívání programu W32Dasm 88
Užívané algoritmy 90
Základní algoritmy 91
Ochrana řetězců 91
Ochrana importovaných funkcí 91
SMC – Sebemodifikující kód 92
Pasivní SMC 93
Aktivní SMC 95
Editace programového kódu za běhu programu 97

KAPITOLA 4
Program FrogsICE a obrana před ním 99
Základy užívání programu FrogsICE 100
Basic options 100
Advanced options 101
Užívané algoritmy 101
VxDCall funkce VMM_GetDDBList 101
Využití funkce CreateFileA 104

KAPITOLA 5
Program ProcDump a obrana před ním 107
Základy užívání programu ProcDump 108
Co je to dumping a k čemu je dobrý 111
Užívané algoritmy 111

KAPITOLA 6
Editace programového kódu 113
Postupy užívané při editaci programového kódu 114
Základy užívání programu Hiew 114
Editace programu pro detekci programu SoftICE 115

Užívané algoritmy 118
Kontrola integrity dat 118
Kontrola integrity dat v souboru 118
Kontrola integrity dat v paměti 121
Další způsoby 125

KAPITOLA 7
PE-šifréry/kompresory a PE-formát 127
Co je to PE-file format 128
Co je to PE-šifrér/kompresor a jak pracuje 129
Jak vytvořit PE-šifrér/kompresor 130
Nevýhody PE-šifrérů/kompresorů 130
Užívané PE-šifréry/kompresory 130
ASPack 130
CodeSafe 131
NeoLite 132
NFO 132
PE-Compact 132
PE-Crypt 133
PE-Shield 133
Petite 134
Shrinker 134
UPX 135
WWPack32 135
PE-souborový formát 136
Ověřování PE-formátu 136
PE-hlavička 139
Tabulka sekcí 141
Nevíte, co znamenají slova Virtual, Raw a RVA? 142
Tabulka importů 143
Tabulka exportů 146
Vytváříme PE-šifrér 147
Přidání nové sekce do souboru 147
Přesměrování toku dat 151
Přidání kódu do nové sekce 152
Skok zpět a proměnné 153
Importované funkce 158
Vytvoření tabulky importů 159
Zpracování původní tabulky importů 162
Použití importované funkce 166
Zpracování TLS 167
Když se řekne šifrování 169
Jaký zvolit šifrovací algoritmus 169
Známé šifrovací algoritmy 169

Co když někdo šifrování prolomí 171
Co šifrovat a co ne 172
Ukázka jednoduchého šifrování v PE-šifréru 173
Finální podoba vytvořeného PE-šifréru 178
Další možnosti ochrany 197
Anti-SoftICE Symbol Loader 197
Kontrola Program Entry Pointu 197
RSA 198
Ukázka použití RSA 201
Závěr k PE-šifrérům a PE-formátu 202

KAPITOLA 8
Další programy používané crackery 203
Registry Monitor 204
File Monitor 206
R!SC's Process Patcher 207
Příkazy ve skriptech 208
The Customiser 209

KAPITOLA 9
Crackujeme 213
Cruehead – CrackMe v1.0 214
Cruehead – CrackMe v2.0 217
Cruehead – CrackMe v3.0 218
CoSH – Crackme1 220
Mexelite – CrackMe 4.0 222
Immortal Descendants – Crackme 8 223
Easy Serial 224
Harder Serial 225
Name/Serial 225
Matrix 226
KeyFile 226
NAG 227
Cripple 227
Duelist – Crackme #5 227
Manuální dešifrování souboru 227
Změny přímo v paměti 231
tC – CrackMe 9 <ID: 6> 232
Manuální získání správného sériového čísla 232
Přestavba programu na key-generator 234
tC – CrackMe 10 <ID: 7> 235
tC – CrackMe 13 <ID: 10> 236

tC – CrackMe 20 <ID: 17> 239
ZemoZ – Matrix CrackMe 242
ZemoZ – CRCMe 245
Editace programu hexadecimálním editorem 247
Použití loaderu 250

KAPITOLA 10
Další informace o crackingu 255
Velký třesk... jak to všechno začalo 256
Kdo se věnuje crackingu 257
Známí crackeři a crackerské skupiny 257
+HCU 257
Immortal Descendants 258
Messing in Bytes – MiB 258
Crackers in Action – CiA 259
Phrozen Crew 259
United Cracking Force – UCF 259
Ebola Virus Crew 259
TNT 260
Evidence 260
Da Breaker Crew 260
Důležitá místa a zdroje na Internetu 260
Několik všeobecných rad od crackerů 263
Cracking (Lucifer48) 263
NOP Patching (+ORC) 263
Patching (MisterE) 263
Myslet jako cracker (rudeboy) 264
Tools (rudeboy) 264

KAPITOLA 11
Referenční část 265
Základní instrukce Assembleru 266
Zprávy Windows 271
Přístupy do registrů 275
Přehled funkcí programu SoftICe 278
Nastavování breakpointů 278
Manipulace s breakpointy 278
Zobrazení/Změny paměti 279
Zobrazení systémových informací 279
Příkazy pro I/O porty 281
Příkazy pro řízení toku dat 281
Řízení módů 281
Uživatelské příkazy 281
Užitečné příkazy 282

Klávesy pro řádkový editor 282
Rolování 282
Příkazy pro manipulaci s okny 283
Ovládání oken 283
Příkazy pro symboly/zdroje 283
Speciální operátory 284

Podmíněné, nepodmíněné skoky a instrukce SET 284
Podmíněné skoky (převzato z CRC32 Tutorial #7) 284
Nepodmíněné skoky (převzato z CRC32 Tutorial #7) 286
Instrukce SET (AntiMaterie) 286

Algoritmus CRC-32 287
Další algoritmy pro použití s PE-šifréry/kompresory 290
Ukázka šifrovacího algoritmu 292
Drobná vylepšení ProcDumpu 296
BoundsChecker interface 302
Get ID 302
Set Breakpoint 302
Activate breakpoint 302
Deactivate Lowest Breakpoint 303
Get Breakpoint Status 303
Clear Breakpoint 303

KAPITOLA 12
Závěr 305

Rejstřík 309