

Obsah

Úvod	1
Kapitola 1	
Úvod do problematiky	3
Kapitola 2	
Programy nejčastěji používané crackery	5
2.1 Základy práce ze Soft-Ice	6
Kapitola 3	
Nejčastější chyby ochrany	11
Kapitola 4	
Základní typy ochrany	13
4.1 Registrační číslo (serial number)	13
4.2 Časové omezení (time limit)	19
4.3 Registrační soubor (KEY file)	23
4.4 Hardwarový klíč (Dongle)	24
4.5 Kontrola originálního CD (CD-Check)	32
4.6 Další ochrany používané pro CD	38
4.7 Demo, ve kterém jsou omezeny některé funkce programu	40
4.8 Další typy ochrany programů	40
Kapitola 5	
Anti-debugovací, anti-disassemblovací a další triky na zlepšení ochrany	71
5.1 Detekování Soft-Ice voláním INT 68h	73
5.2 Detekování Soft-Ice voláním INT 3h	74
5.3 Detekce Soft-Ice hledáním v paměti	76
5.4 Detekování Soft-Ice pomocí otevření jeho ovladačů, voláním API funkce CreateFileA (SICE, NTICE)	78
5.5 Detekování Soft-Ice pomocí vzdálenosti mezi obsluhami Int 1h a Int 3h	81
5.6 Detekování Soft-Ice pomocí otevření jeho ovladačů voláním API funkce CreateFileA (SIWVID)	83

5.7 Detekování Soft-Ice voláním funkce NmSymIsSoftICELoaded DLL z knihovny nmtrans.dll	84
5.8 Detekce Soft-Ice pomocí identifikování jeho obsluhy Int 68h	87
5.9 Detekce Soft-Ice změnou obsluhy Int 41h	88
5.10 Detekování Soft-Ice pomocí otevření jeho ovladače voláním API funkce CreateFileA (SIWDEBUG)	90
5.11 Detekce Soft-Ice voláním Int 2Fh a jeho funkce GET_DEVICE_API_ENTRY_POINT pro VXD SICE	92
5.12 Detekce Soft-Ice voláním Int 2Fh a jeho funkce GET_DEVICE_API_ENTRY_POINT pro VXD SIWVID	97
5.13 Použití instrukce CMPXCHG8B s prefixem LOCK	101
5.14 Detekce Soft-Ice pomocí VxDCall	103
5.15 Zjištění aktivního debuggeru pomocí debug registru DR7	106
5.16 Detekce Soft-Ice pomocí VxDCall volaného přes Kernel32!ORD_0001	109
5.17 Nalezení adresáře, kde je nainstalován Soft-Ice pomocí registrů Windows	113
5.18 Detekování TRW pomocí vzdálenosti mezi obsluhami Int 1h a Int 3h	116
5.19 Detekování TRW pomocí otevření jeho ovladače voláním API funkce CreateFileA (TRW)	118
5.20 Spouštění příkazů BCHK rozhraní Soft-Ice	119
5.21 Detekce TRW voláním Int 3h	124
5.22 Detekování Soft-Ice pomocí otevření jeho ovladače voláním API funkce CreateFileA (SIWVIDSTART)	126
5.23 Detekování Soft-Ice pomocí otevření jeho ovladače voláním API funkce CreateFileW (NTICE, SIWVIDSTART)	128
5.24 Detekování Soft-Ice pomocí otevření jeho ovladače voláním API funkce _lcreat (SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART)	130
5.25 Detekování Soft-Ice pomocí otevření jeho ovladače voláním API funkce _lopen (SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART)	131
5.26 Anti-FrogsICE trik	133
5.27 Detekování trcera pomocí Trap flag	136
5.28 Detekce breakpointů hledáním Int 3h	138
5.29 Detekce breakpointu pomocí CRC	141
5.30 Detekce debug breakpointů	145
5.31 Detekce user debuggeru	148
5.32 Detekce user debuggeru pomocí API funkce IsDebuggerPresent	149
5.33 Detekce Soft-Ice hledáním instrukce Int 3h v UnhandledExceptionFilter	151
5.34 Detekce Soft-Ice hledáním instrukce Int 3h v UnhandledExceptionFilter	152
5.35 Detekce Soft-Ice pomocí Int 1h	154

5.36	Detekce API hook	156
5.37	Anti-ProcDump trik	159
5.38	Přepnutí běhu programu z RING3 do RING0	161
5.39	Anti-disassemblovací makra	169
5.40	Detekce pokusu o dekomprimování, anebo dekodování programu	172
5.41	Výpočet kontrolního součtu programu pomocí API funkce MapFileAndCheckSumA	172
5.42	Změna charakteristik pro .code sekci PE souboru	172
5.43	Zjištění monitorovacích programů	173
5.44	Trik na potrestání crackera	175
Kapitola 6		
	Rady, jak lépe chránit své programy	177
Kapitola 7		
	Důležité struktury ve Windows	181
7.1	Struktura Context	181
7.2	Spustitelný soubor Windows NT (PE soubory)	184
Kapitola 8		
	Důsledky ochrany programů	197
Kapitola 9		
	Zajímavé stránky na Internetu	199
	Závěr	200
	Pár slov o autorovi	200
	Glosář	201
	Rejstřík	203