

## BRIEF CONTENTS

|   |  |
|---|--|
| <b>Introduction</b>   |  |
| 1   |  |
| <b>Chapter 1</b>  |  |
| Basics  |  |
| 5   |  |
| <b>Chapter 2</b>  |  |
| Cracking Tools  |  |
| 9   |  |
| <b>Chapter 3</b>  |  |
| The Basic Types of<br>Software Protection   |  |
| 15  |  |
| <b>Chapter 4</b>  |  |
| CD Protection Tricks  |  |
| 41  |  |
| <b>Chapter 5</b>  |  |
| Program Compression and<br>Encoding: Freeware and Shareware                               |  |
| 53  |  |
| <b>Chapter 6</b>  |  |
| Commercial Software<br>Protection Programs  |  |
| 75  |  |
| <b>Chapter 7</b>  |  |
| Anti-Debugging, Anti-Disassembling,<br>and Other Tricks for Protecting<br>Against SoftICE |  |
| 95  |  |
| <b>Chapter 8</b>  |  |
| Protecting Against Breakpoints,<br>Tracers, and User Debuggers                            |  |
| 167   |  |
| <b>Chapter 9</b>  |  |
| Other Protection Tricks   |  |
| 185   |  |
| <b>Chapter 10</b>   |  |
| Important Structures in Windows   |  |
| 207   |  |

**Chapter 11**  
Suggestions for Better  
Software Protection  
225

**Glossary**  
231

**About the CD**  
232

**Index**  
233

## CONTENTS IN DETAIL

### INTRODUCTION

|                           |   |
|---------------------------|---|
| Protection as a Deterrent | 2 |
| Working with Assembler    | 2 |
| Publishing Cracker Tricks | 2 |

## 1

### BASICS

|   |   |
|---|---|
| Why Crackers Crack                              | 5 |
| How Crackers Crack: Debuggers and Disassemblers | 6 |
| <i>Debuggers</i>                                | 6 |
| <i>Disassemblers</i>                            | 6 |
| <i>Decompilers</i>                              | 6 |
| The Most Frequent Protection Failures           | 7 |

## 2

### CRACKING TOOLS

|                         |    |
|-------------------------|----|
| SoftICE Basics          | 10 |
| <i>Key Commands</i>     | 12 |
| <i>The BPX Command</i>  | 13 |
| <i>The BPR Switch</i>   | 13 |
| <i>The BPM Switch</i>   | 13 |
| <i>Display Commands</i> | 13 |

## 3

### THE BASIC TYPES OF SOFTWARE PROTECTION

|   |    |
|---|----|
| Registration-Number (Serial-Number) Protection                            | 15 |
| <i>Registration Number Is Always the Same</i>                             | 16 |
| <i>Registration Number Changes in Accordance with Entered Information</i> | 17 |
| <i>Registration Number Changes in Accordance with the User's Computer</i> | 19 |
| <i>Registration-Number Protection in Visual Basic Programs</i>            | 19 |
| <i>Registration Number Is Checked Online</i>                              | 23 |

|   |    |
|---|----|
| Time-Limited Programs   | 25 |
| <i>Time Limit Is Removed Once the Correct Registration Number Is Entered</i>    | 26 |
| <i>Time Limit Is Removed Once a Registration Key File (.REG) Is Entered</i>     | 26 |
| <i>Time Limit Cannot Be Removed; the User Must Buy the Full Program</i>         | 27 |
| <i>Time Limit Is Contained in a Visual Basic Program</i>                        | 28 |
| <i>Time Limit Applies to a Certain Number of Starts</i>                         | 28 |
| Registration-File (KEY File) Protection   | 29 |
| <i>Some Program Functions Are Blocked Without the Correct Registration File</i> | 29 |
| <i>Program Is Time-Limited Without the Correct Registration File</i>            | 30 |
| Hardware-Key (Dongle) Protection  | 30 |
| <i>Program Cannot Be Started Without the Hardware Key</i>                       | 30 |
| <i>Some Functions Are Limited Without the Hardware Key</i>                      | 32 |
| <i>HASP Hardware Keys</i>   | 32 |
| <i>Sentinel Hardware Keys</i>   | 38 |

## 4

### CD PROTECTION TRICKS

|   |    |
|---|----|
| How CD-Checkers Work                                | 42 |
| CD Protection Software                              | 42 |
| <i>CD-Cops</i>                                      | 42 |
| <i>DiscGuard</i>                                    | 43 |
| <i>LaserLock</i>                                    | 44 |
| <i>SafeCast</i>                                     | 44 |
| <i>SafeDisc</i>                                     | 44 |
| <i>SecuROM</i>                                      | 47 |
| <i>VOB</i>  | 48 |
| Other CD Protection Tricks                          | 48 |
| <i>CD Contains More Than 74 Minutes of Data</i>     | 49 |
| <i>Damaged TOC (Table of Contents)</i>              | 49 |
| <i>Huge Files</i>                                   | 50 |
| <i>Physical Errors</i>                              | 50 |
| <i>One or More Huge Files</i>                       | 50 |
| <i>Demo with Selected Program Functions Limited</i> | 50 |

## 5

### PROGRAM COMPRESSION AND ENCODING: FREWARE AND SHAREWARE

|                                     |    |
|-------------------------------------|----|
| aPLib                               | 54 |
| ASPack                              | 54 |
| Ding Boys PE-Crypt                  | 56 |
| Neolite v2.0                        | 58 |
| <i>Advanced Compression Options</i> | 59 |
| <i>Icons</i>                        | 59 |
| <i>Preserve Data</i>                | 59 |
| <i>Other Resources</i>              | 60 |
| <i>Miscellaneous</i>                | 60 |
| NFO                                 | 61 |
| PE Compact                          | 61 |
| PELOCKnt                            | 62 |
| PE-Crypt                            | 63 |
| <i>Manual Removal</i>               | 66 |
| <i>Creating a Loader</i>            | 66 |
| <i>PE-Crypt Options</i>             | 67 |
| <i>PE-Crypt Summary</i>             | 68 |
| PE Shield                           | 68 |
| Pefite                              | 70 |
| Shrinker                            | 71 |
| UPX                                 | 72 |
| WWPACK32                            | 73 |

## 6

### COMMERCIAL SOFTWARE PROTECTION PROGRAMS

|  |    |
|--|----|
| ASProtect                                | 76 |
| FLEXIm                                   | 80 |
| InstallShield                            | 82 |
| ShareLock                                | 84 |
| The Armadillo Software Protection System | 84 |
| Vbox                                     | 86 |
| <i>Timelock 3.03 Through 3.10</i>        | 87 |
| <i>TimeLock 3.13 Through 3.15</i>        | 87 |
| <i>Vbox 4.0 Through 4.03</i>             | 87 |
| <i>Vbox 4.10</i>                         | 88 |
| <i>Vbox 4.3</i>                          | 88 |
| <i>The Slovak Protector (SVKP)</i>       | 89 |

# 7

## ANTI-DEBUGGING, ANTI-DISASSEMBLING, AND OTHER TRICKS FOR PROTECTING AGAINST SOFTICE AND TRW

|  |     |
|--|-----|
| Detecting SoftICE by Calling INT 68h   | 97  |
| Detecting SoftICE by Calling INT 3h  | 99  |
| Detecting SoftICE by Searching Memory  | 101 |
| Detecting SoftICE by Opening Its Drivers and Calling the CreateFileA API Function (SICE, NTICE)                                  | 103 |
| Detecting SoftICE by Measuring the Distance Between INT 1h and INT 3h Services   | 107 |
| Detecting SoftICE by Opening Its Drivers and Calling the API Function CreateFileA (SIWVID)                                       | 109 |
| Detecting SoftICE by Calling the NmSymlsSoftICELoaded DLL Function from the nmtrans.dll Library                                  | 110 |
| Detecting SoftICE by Identifying Its INT 68h Service   | 113 |
| Detecting SoftICE by Detecting a Change in the INT 41h Service   | 114 |
| Detecting SoftICE by Opening Its Driver and Calling the API Function CreateFileA (SIWDEBUG)                                      | 115 |
| Detecting SoftICE by Calling Int 2Fh and Its Function GET DEVICE API ENTRY POINT for VxD SICE                                    | 117 |
| Detecting SoftICE by Calling Int 2Fh and Its Function GET DEVICE API ENTRY POINT for VxD SIWVID                                  | 122 |
| Usage of the CMPXCHG8B Instruction with the LOCK Prefix  | 127 |
| Detecting SoftICE with the VxDCall   | 129 |
| Finding an Active Debugger Through the DR7 Debug Register  | 132 |
| Detecting SoftICE by Calling VxDCall Through Kernel32!ORD_0001   | 135 |
| Using the Windows Registry to Find the Directory Where SoftICE Is Installed  | 139 |
| TRW Detection Using the Distance Between the Int 1h and the Int 3h Services  | 142 |
| Detecting TRW by Opening Its Driver Through Calling the API of the CreateFileA (TRW)   | 144 |
| Launching the BCHK Command of the SoftICE Interface  | 145 |
| Detecting TRW by Calling Int 3h  | 149 |
| Detecting SoftICE by Opening Its Driver with an API Call to the CreateFileA (SIWVIDSTART) Function                               | 152 |
| Detecting SoftICE by Opening Its Driver with an API Call to the<br>CreateFileW (NTICE, SIWVIDSTART) Function                     | 154 |
| Detecting SoftICE by Opening Its Driver with an API Call to the<br>Function _lcreat (SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART) | 156 |
| Detecting SoftICE by Opening Its Driver with an API Call to the<br>Function _lopen (SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART)  | 158 |
| Anti-FrogsICE Trick  | 160 |
| Detecting SoftICE by Searching for the Int 3h Instruction in the UnhandledExceptionFilter  | 163 |
| Detecting SoftICE Through Int 1h   | 164 |

## 8

### DETECTING BREAKPOINTS, TRACERS, AND DEBUGGERS

|   |     |
|---|-----|
| Detecting Tracers Using the Trap Flag                             | 167 |
| Detecting Breakpoints by Searching for Int 3h                     | 169 |
| Detecting Breakpoints by CRC                                      | 173 |
| Detecting Debug Breakpoints                                       | 177 |
| Detecting User Debuggers  | 180 |
| Detecting User Debuggers Using the API Function IsDebuggerPresent | 182 |

## 9

### OTHER PROTECTION TRICKS

|   |     |
|---|-----|
| API Hook Detection  | 185 |
| Anti-ProcDump Trick   | 188 |
| Switching a Running Program from RING3 to RING0   | 191 |
| <i>Switching into Ring0 Using the LDT (Locale Descriptor Table)</i>                     | 191 |
| <i>Switching into Ring0 Using the IDT (EliCZ's Method)</i>                              | 193 |
| <i>Switching into Ring0 Using the SEH (The Owl's Method)</i>                            | 196 |
| Anti-Disassembling Macros   | 199 |
| <i>The Simplest Method</i>  | 199 |
| <i>A Similar Method</i>   | 200 |
| <i>Making It Even Better</i>  | 200 |
| <i>Fantasy is Unlimited</i>   | 200 |
| <i>Jumping into the Middle of Instructions and Making the Code Harder to Understand</i> | 201 |
| Detecting Attempts to Decompress Programs Prior to Decoding                             | 202 |
| Testing a File's Checksum with the API Function MapFileAndChecksumA                     | 202 |
| Changes in Characteristics for the .code Section of the PE File                         | 203 |
| Finding Monitoring Programs   | 203 |
| A trick for Punishing a Cracker   | 205 |

## 10

### IMPORTANT STRUCTURES IN WINDOWS

|  |     |
|--|-----|
| Context Structure                      | 207 |
| Windows NT Executable Files (PE Files) | 211 |
| Object Table                           | 217 |
| Section Types                          | 219 |
| <i>Code Section</i>                    | 219 |
| <i>Data Section</i>                    | 219 |
| <i>BSS Section</i>                     | 219 |
| <i>Exported Symbols</i>                | 220 |
| <i>Imported Symbols</i>                | 221 |
| <i>Resources</i>                       | 222 |

## 11

### SUGGESTIONS FOR BETTER SOFTWARE PROTECTION

|  |     |
|--|-----|
| Rules for Writing Good Software Protection | 226 |
| Keep Current                               | 229 |

## Glossary

231

## About the CD

232

## Index

233