

<<Cracker终结者>>

图书基本信息

书名：<<Cracker终结者>>

13位ISBN编号：9787302079941

10位ISBN编号：7302079943

出版时间：2004-2

出版时间：清华大学出版社

作者：韩宏莲

页数：216

字数：295000

译者：科尔文

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<Cracker终结者>>

内容概要

本书全面分析软件防护技术，系统阐述防范非法复制的解决方案。

首先介绍解密工具、软件保护的基本类型、光盘保护策略、免费软件和共享件以及商业软件保护程序

。然后论述防范SoftICE和TRW的反调试、反-反汇编策略；分析断点、跟踪程序和调试程序的检测方法

。最后介绍Windows的重要结构和一些软件保护编写规则。

本书是最新软件防护技术的结晶，适合那些从事软件保护工作和商业软件开发的技术人员，也适合从事软件保护研究的相关人员。

作者简介

Pavol Cerven : Alcatel公司的编程专家，原从事PC病毒防护，后主要研究软件防护，曾开发著名的SVKP安全软件。

书籍目录

第1章 开篇 1 1.1 解密者的动机 1 1.2 解密方法：调试程序和反汇编程序 1 1.3 常见的保护故障 2第2章 解密工具 3 2.1 认识SoftICE 4第3章 软件保护的基本类型 8 3.1 注册号保护 8 3.2 限期程序 16 3.3 注册文件保护 19 3.4 硬件密钥保护 20第4章 光盘保护策略 30 4.1 光盘保护软件 31 4.2 其他光盘保护策略 36第5章 程序压缩和编码：免费软件和共享件 40 5.1 aPLib 40 5.2 ASPack 40 5.3 Ding Boy ' s PE-Crypt 42 5.4 NeoLite 44 5.5 NFO 46 5.6 PECompact 47 5.7 PELOCKnt 48 5.8 PE-Crypt 49 5.9 PE-SHiELD 54 5.10 Petite 55 5.11 Shrinker 56 5.12 UPX 56 5.13 WWPack32 57第6章 商业软件保护程序 59 6.1 ASProtect 59 6.2 FLEXIm 63 6.3 InstallShield 64 6.4 ShareLock 66 6.5 Armadillo软件保护系统 66 6.6 VBox 68第7章 用于防范SoftICE和TRW的反调试、反-反汇编及其他策略 75 7.1 通过调用INT 68h检测SoftICE 76 7.2 通过调用INT 3h检测SoftICE 78 7.3 通过搜索内存检测SoftICE 81 7.4 通过打开SoftICE驱动程序并调用API函数CreateFileA(SICE, NTICE) 来检测SoftICE 83 7.5 通过测量INT 1h和INT 3h服务之间的距离检测SoftICE 87 7.6 通过打开SoftICE驱动程序并调用API函数CreateFileA(SIWVID) 来检测SoftICE 89 7.7 通过调用nmtrans.dll库的NmSymlsSoftICELoaded DLL函数检测 SoftICE 90 7.8 通过识别SoftICE的INT 68h服务来检测SoftICE 93 7.9 通过检测INT 41h服务的更改来检测SoftICE 94 7.10 通过打开SoftICE驱动程序并调用API函数CreateFileA(SIWDEBUG) 来检测SoftICE 96 7.11 通过调用INT 2Fh及其函数GET DEVICE API ENTRY POINT检测 SoftICE (查找VxD ICE) 98 7.12 通过调用INT 2Fh及其函数GET DEVICE API ENTRY POINT检测 SoftICE (查找VxD SIWVID) 103 7.13 使用前缀为LOCK的CMPXCHG8B指令 108 7.14 通过VxDCall检测SoftICE 111 7.15 通过DR7调试寄存器查找活动的调试程序 114 7.16 通过Kernel32!ORD_0001并调用VxDCalls检测SoftICE 116 7.17 通过Windows注册表找出SoftICE的安装目录 121 7.18 通过Int 1h和Int 3h服务之间的距离检测TRW 124 7.19 通过调用API函数CreateFileA(TRW)打开TRW驱动程序来检测 TRW 126 7.20 启动SoftICE接口的BCHK命令 127 7.21 通过调用Int 3h检测TRW 132 7.22 通过调用API函数CreateFileA(SIWVIDSTART)打开SoftICE驱动 程序来检测 SoftICE 135 7.23 通过调用API函数CreateFileW(NTICE, SIWVIDSTART)打开SoftICE 驱动程序来检测SoftICE 137 7.24 通过调用API函数Function_lcreat(SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART)打开SoftICE驱动程序来检测SoftICE 140 7.25 通过调用API函数Function_lopen(SICE, NTICE, SIWVID, SIWDEBUG, SIWVIDSTART)打开SoftICE驱动程序来检测SoftICE 142 7.26 反FrogsICE策略 143 7.27 通过在UnhandledExceptionFilter查找指令Int 3h来检测SoftICE 147 7.28 通过Int 1h检测SoftICE 149第8章 防止断点、跟踪程序和调试程序 152 8.1 通过Trap标志检测跟踪程序 152 8.2 通过查找Int 3h检测断点 154 8.3 通过CRC测试断点 157 8.4 检测调试断点 163 8.5 检测用户调试程序 165 8.6 通过API函数IsDebuggerPresent检测用户调试程序 167第9章 其他保护策略 170 9.1 API挂钩检测 170 9.2 反ProcDump策略 173 9.3 将运行程序从ring3切换到ring0 176 9.4 反-反汇编宏 184 9.5 在解码前测试解压缩试图 188 9.6 用API函数MapFileAndCheckSumA测试文件校验和 188 9.7 PE文件.code节的特性更改 188 9.8 查找监视程序 189 9.9 惩罚解密者之策 191第10章 Windows中的重要结构 193 10.1 上下文结构 193 10.2 Windows NT可执行文件 196 10.3 对象表 202 10.4 节类型 204第11章 软件防护建议 210 11.1 编写软件保护的原则 210 11.2 最新信息 213术语表 214

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>