

黑客防线 4

书

の书

——凝结无数破解高手经验与技巧

盘

の盘

——尽数收录黑客给予成名的工具



内容提要

很多人都想学学做 Cracker，好象破了一个程序很风光，人人都很佩服。可是做一个 Cracker 其实很累，需花费大量的时间，而且经常会碰壁，三五天毫无进展是极为平常的事情。而且 crack 是违法的，这点要牢记。长久以来破解技术受到世人的鄙视，绝大多数人甚至根本不认为它是一项技术，而只把它看作是一些小伎俩罢了。其实，破解技术的应用范围十分广泛，而 Cracker 们也就在我们身边，如何正确运用破解技术才是关键，当 Cracker 目的不是破解软件，而是通过跟踪软件，了解程序思路，学习别人的编程技巧，这样提高自己，使自己能写出更好的程序。破解不在多，而在于你要掌握它，尽量了解注册码计算原理，写出注册机等等。

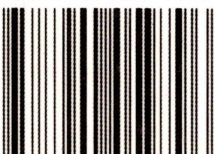
很多初学者都希望找一部完整破解技术教程，由浅到深，系统学习破解知识，但很难如愿以偿，毕竟这方面技术太多太杂，设计的领域也很广，所以很难系统化，为了尽可能多的帮助新手，我们从网上搜集了大量相关资料，按类别分开章节，制作出这部《黑客防线4》——“破解大师速成宝典”，这份资料主要是和大家探讨一些加密解密的问题，之所以敢称“宝典”，不是说编书的人水平如何的高深，而是在于文中引用的大量文献资料绝对都是此道高手所著，尽管很多没有署名，但文章基本保持原样。

要想成为一名出色的 Cracker，除了精通各种破解技术外，得心应手的工具也是必不可少的，这些工具多数是个人开发的，散布在网上，我们将它们尽数收录进《黑客防线4》光盘中，选择称手的工具，可以使你的破解事半功倍。

这里还要多说几句，望大家别嫌我罗嗦，从这本书中学到的破解技能去破解软件是可以的，但千万不要把破解后的东东发布或用于商业用途，那是非法的，切记，切记……

ISBN 7-900059-79-2/G. 17

ISBN 7-900059-79-2



9 787900 059796 >

金版电子出版公司出版
软件渠道总经销:北京正普公司
电话:010-82671133

定价: 19.8 元 (CD+书)



引言

很多人都想学学做 Cracker, 好像破了一个程序很风光的, 人人都很佩服。可是做一个 Cracker 其实很累, 需花费大量的时间, 而且经常会碰壁, 三五天毫无进展是极为平常的事情。而且 Crack 是违法的, 这点要牢记。长久以来破解技术受到世人的鄙视, 绝大多数人甚至根本不认为它是一项技术, 而只把它看作是一些小伎俩罢了。其实, 破解技术的应用范围十分广泛, 而 Cracker 们也就在我们身边。如何正确运用破解技术才是关键, 当 Cracker 目的不是破解软件, 而是通过跟踪软件, 了解程序思路, 学习别人的编程技巧, 这样提高自己, 使自己能写出更好的程序。破解不在多, 而在于你要掌握它, 尽量了解注册码计算原理, 写出注册机等等。

很多初学者都希望找一部完整的破解技术教程, 由浅到深, 系统学习破解知识, 但很难如愿以偿, 毕竟这方面技术太多太杂, 涉及的领域也很广, 所以很难系统化。为了尽可能多地帮助新手, 我们从网上搜集了大量相关资料, 按类别分开章节, 制作出这部“黑客防线四”——《破解大师速成宝典》, 这份资料主要是和大家探讨一些加密解密的问题, 之所以敢称“宝典”, 不是说编书的人水平如何高深, 而是在于文中引用的大量文献资料绝对都是此道高手所著, 尽管很多没有署名, 但文章基本保持原样。

要想成为一名出色的 Cracker, 除了精通各种破解技术外, 得心应手的工具也是必不可少的, 这些工具多数是个人开发的, 散布在网上, 我们将它们尽数收录进“黑客防线四”光盘中。选择称手的工具, 可以使你的破解事半功倍。

这里还要多说几句, 望大家别嫌我罗嗦。从这本书中学到的破解技能去破解软件是可以的, 但千万不要把破解后的东东发布或用于商业用途, 那是非法的。切记, 切记……



目 录

引言	1
光盘内容检索	6
第一章 初窥门径	
1.1 必要条件	23
1.2 何谓破解	23
1.3 对立面——加密	24
1.3.1 首先说说依赖硬件的加密方案	24
1.3.2 再谈谈不依赖硬件的加密方案	25
1.4 散布世界各地的破解组织	27
第二章 破解之本	
2.1 汇编语言基础	30
2.1.1 寄存器	30
2.1.2 寻址方式	32
2.1.3 汇编指令集	33
2.1.4 伪操作	37
2.1.5 跳转指令小结	39
2.2 软件分析跟踪技术	40
2.3 常用工具介绍	41
第三章 动态跟踪分析利器——“SOFTICE”&“TRW2000”	
3.1 SOFTICE for win9x 安装与设置	44
3.1.1 SOFTICE 安装	44
3.1.2 显卡配制	45
3.1.3 鼠标的配制	45
3.1.4 装载 SOFTICE 的主文件 winice.exe	45
3.1.5 Symbol Loader 的使用	46
3.1.6 winice.dat 配制	47
3.2 SOFTICE for NT/2K 安装与配制	50



3.3 TRW2000 的安装与配制	51
3.3.1 安装 TRW2000	51
3.3.2 TRW2000 的配制	52
3.4 熟悉 SOFTICE 和 TRW2000	52
3.4.1 操作窗口	52
3.4.2 常用命令	53
3.4.3 关于中断点指令的使用	56
3.4.4 其他指令	57
3.5 小试牛刀——破解实例一	57
3.6 破解实例二——“ask Lock”(ED! SON 设计制作)	61
3.7 破解实例三——Command Line 95 (ED! SON 设计制作)	64
3.8 Win API 函数与中断点设置技巧	66
3.8.1 基本 Win API 函数	66
3.8.2 中断点设置技巧	70

第四章 静态反汇编三剑客——“W32Dasm”、“HIEW”、“IDA”

4.1 W32Dasm	72
4.1.1 开始	72
4.1.2 反汇编源代码的基本操作	73
4.1.3 复制汇编代码文本	76
4.1.4 装载 32 位的汇编代码动态调试	76
4.1.5 运行, 暂停或终止程序	77
4.1.6 单步跟踪程序	77
4.1.7 设置激活断点	77
4.1.8 偏移地址和虚拟地址转换	77
4.2 Hiew 简要说明	78
4.3 关于 IDA 与 W32Dasm 的比较	79
4.4 破解实例	80

第五章 注册表破解技巧浅析

5.1 注册表的备份	83
5.2 注册表结构分析	84
5.2.1 注册表的六大根键	84
5.2.2 注册表的层次结构	85
5.3 注册表的文件组成	86
5.3.1 系统配置注册表文件 System. dat	86
5.3.2 系统配置注册表备份文件 System. da0	87



5.3.3 用户平台配置注册表文件 User. dat	87
5.3.4 用户平台配置注册表备份文件 User. da0	88
5.3.5 网络管理注册表文件 Config. pol	88
5.3.6 网络管理注册表备份文件 Config. po0	88
5.4 注册表分析工具	88
5.5 破解范例	91
第六章 剥除软件的外衣——脱壳技术	
6.1 一切从“壳”开始	95
6.2 手动脱壳	97
第七章 实例	
7.1 FlashGet(JetCar Ver0.77) 破解实录	101
7.2 ACDSer V3.0 破解	104
7.3 美萍网管大师 v5.2 破解及注册机制作	105
7.4 WINZIP8.0 牛刀小试	108
7.5 呼吸小秘书(javagirl)的破解	114
7.6 最流行的离线浏览器 Teleport Pro 的破解	115
7.7 Explor2000 V1.51 强迫注册法	119
附录 softice&trw2000 指令详解	122

<p>策 划：《家庭电脑世界》编辑部 制 作：北京地海森波网络技术公司 出 版：金版电子出版公司出版 ISBN7-900059-79-2/G.17 通信地址：北京市中关村邮局 008 信箱 邮 编：100080 技术支持电话：(010)82672099 E-mail：Pcfriend@mail.263.net.cn</p>	<p>Pcworld@public.gb.com.cn</p> <p>编 辑：郭聪辉 王 远 刘东亚 制 作：王进才 施剑峰 袁 刚 美术设计：温 洋 王 凤 发行部电话：(010)62141360 发行部传真：(010)62141446 定 价：19.80 元 (光盘+手册)</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



光盘内容检索

反编译工具

软件名称:W32DASM 黄金版本

软件说明:同时对 VB/DELPHI 提取字符给予最强的支持。

使用平台:win9x 版本:8.93 黄金版本。

光盘路径: \Fanbianyi \Wasm32gold.zip

软件名称:W32Dasm Ver8.93 最新超级中文版

软件说明:增强了很多功能。可以反编译原来针对 w32 做了手脚的软件。而且还可以查看中文字符串。使用平台:win9x

版本:8.93 超级中文版

光盘路径: \fanbianyi \pw32dsmpower.zip

软件名称:W32Dasm Ver8.93 最新超级英文版

软件说明:可以反编译原来针对 w32 做了手脚的软件。使用平台:win9x

光盘路径: \fanbianyi \w32dsmpower.zip

\fanbianyi \Wdasm8.93.zip(含补丁)

软件名称:IDA Pro Advanced v4.04

软件说明:巨酷的反编译软件,破解高手们几乎都喜欢用这个软件。不会用当作经典的收藏软件也不错。使用平台:win9x/dos 版本:v4.04

光盘路径: \fanbianyi \IDA v4.04.zip

软件名称:PLUGINS FOR IDA PRO VERSION 0.6 IDA 4.04 插件。

软件说明:IDA 功能是强大,但对 String References 等不能提供好的界面和操作,对我们菜鸟来说,已习惯了 W32DASM 的 String References、Import 和 Export 三种功能形式,幸好有了这个插件,使 IDA 这三个功能更加方便使用,大大有利于破解。安装时将文件解压到 IDA 的 plugins 目录。

光盘路径: \fanbianyi \ida_plugins06.zip

软件名称:反编译专家 unfoxall v 2.0 专业版

软件说明:目前我见过的最棒的反编译 fox 系列软件的工,可完整的从 FOX 所有版本。绝对经典,不容错过。使用平台:win9x 版本:2.0 增强版

光盘路径: \fanbianyi \unfoxall20full.zip

软件名称:反编译专家 unfoxall v 2.0

软件说明:目前我见过的最棒的反编译 fox 系列软件的工,可完整的从 FOX 所有版本。绝对经典,不容错过。软件授权:演示版

使用平台:win9x 版本:2.0

光盘路径: \fanbianyi \UnFoxAll20.zip

软件名称:VBDSRA 1.0

软件说明:vbW32Dasm 反编译出来无法察看其中的字符串。怎么办?用这个试试,看看怎么样?使用平台:win9x 版本:1.0

光盘路径: \fanbianyi \vbref.zip

软件名称:反编译专家 unfoxall

软件说明:国产的一个反编译所有的 fox 系列编写的。功能十分强大,可惜演示版不能编译超过 40 个软件。使用平台:win9x 版本:1.2

光盘路径: \fanbianyi \ unfoxall12.zip

软件名称:DeDe

软件说明:一个反编译 DELPHI 的工具。看起来比 Decompiler 要好。使用平台:win9x 版本:v1.05b1 v1.06b1

光盘路径: \fanbianyi \DeDe105b1.zip \fanbianyi \DEDE106B1.zip

软件名称:mDeJava v1.0b

软件说明:一个新的 java class 的反编译软件。可以把 2 进制的 class 文件全部反编译成源代码。使用平台:win9x 版本:1.0b

光盘路径: \fanbianyi \mDeJava.zip

软件名称:foxpro 反编译软件包

软件说明:里面有几个反编译 foxpro 的软件。使用平台:Dos

光盘路径: \fanbianyi \Foxpdec.zip

软件名称:Decompiler

软件说明:现在越来越多的软件都用 DELPHI 编写了,可是它编写的又无用其它软件反编译出字符串等。这是一个最新出来的很不错的反编译 DELPHI 的东西!反编译必备!使用



Pc friend

平台:win9x

光盘路径:\fanbianyi\DecompilerSrc. zip

软件名称:Sourcer V7.00

软件说明:一个强大的反汇编工具,反汇编出来的代码甚至比源代码还好看!这个版本已经支持 Windows 的 PE 和 NE 文件格式了。使用平台:win9x/Dos 版本:7.0 Serial:SW 601745 - JHJM

光盘路径:\fanbianyi\sourcer7. zip

软件名称:Sourcer V6.51

软件说明:一个强大的反汇编工具,反汇编出来的代码甚至比源代码还好看!使用平台:Dos 版本:6.51 SN:SR322449 - TAWÉ

光盘路径:\fanbianyi\sourcer. zip

软件名称:IDA Pro 4.00

软件说明:目前最强大的静态反汇编软件,无论你是编程或者是 Crack 软件,都会用到它的,但它比较专业,在 Crack 软件方面没有 Wdasm32 好用,它支持 DOS、NE、PE 等各种文件格式,这是最新的版本,是 Windows 界面的。使用平台:win9X 版本:4.00

光盘路径:\fanbianyi\demo400. zip

软件名称:IDA 3.85b

软件说明:目前最强大的静态反汇编软件,无论你是编程或者是 Crack 软件,都会用到它的,但它比较专业,在 Crack 软件方面没有 Wdasm32 好用,它支持 DOS、NE、PE 等各种文件格式,这是 DOS 界面的最后版本,已破解。使用平台:win9x 版本:3.85b

光盘路径:\fanbianyi\demo385b. zip

软件名称:IDA3.84B

软件说明:目前最强大的静态反汇编软件,无论你是编程或者是 Crack 软件,都会用到它的,但它比较专业,在 Crack 软件方面没有 Wdasm32 好用,它支持 DOS、NE、PE 等各种文件格式,这是 Cracked 的完全版本。使用平台:win9x 版本:3.84B

光盘路径:\fanbianyi\ida384b. zip

软件名称:W32Dasm Ver8.93 中文版

软件说明:鼎大名的 W32dasm,可以对程序进行反汇编操作,而且对 WinApi 有良好的支持,反汇编出的代码可读性非常强。它可以记录下程序静态代码,是 SoftICE 的最好补充。你可以下载由龙文汉化的修正版,无需原程序。使用平台:win9x 版本:8.93

光盘路径:\fanbianyi\pwdasm893. zip

软件名称:W32Dasm Ver8.93

软件说明:鼎大名的 W32dasm!可以对程序进行反汇编操作,而且对 WinApi 有良好的支持,反汇编出的代码可读性非常强。他可以记录下程序静态代码,是 SoftICE 的最好补充。你

可以下载由龙文汉化的修正版,无需原程序。使用平台:win9x 版本:8.93

光盘路径:\fanbianyi\wdasm893. zip

软件名称:Process View v1.00

软件说明:内存 ASM 反编译工具。有了它就可以不用 TRW, Winice 浏览内存代码,而且还能将反编译代码 SAVE 到文件上。使用平台:win9x 版本:1.0

光盘路径:\fanbianyi\pview. zip

软件名称:Refox 8.0

软件说明:FoxPro v3.0 v5.0 v6.0 反编译工具,使用平台: Dos 版本:8.0

光盘路径:\fanbianyi\refox8d. zip

软件名称:Refox7.06

软件说明:Foxpro 2.5&2.6 反编译工具,使用平台: Dos 版本:7.06

光盘路径:\fanbianyi\refox706. zip

软件名称:Refox5.01

软件说明:Foxpro 反编译工具,使用平台: Dos 版本:5.01

光盘路径:\fanbianyi\refox501. zip

软件名称:i5Comp v2.01

软件说明:Installshield 反编译工具。有了它们 Installshield 的安装过程就能一目了然。使用平台:win9x

光盘路径:\fanbianyi\i5comp. zip

软件名称:DIS v1.00 Installshield

软件说明:Installshield 反编译工具。使用平台:win9x

光盘路径:\fanbianyi\dis. zip

软件名称:exwise05

软件说明:Exwise 反编译工具(带 C 源程序),从安装程序 Setup. ins 生成 Wise 的安装脚本源程序。最新版本:V0.5 使用平台: DOS

光盘路径:\fanbianyi\exwise05. zip

软件名称:vb4tools

软件说明:VB 4.0 的反编译工具(不支持类)

光盘路径:\fanbianyi\vb4tools. zip

软件名称:Java Class 反编译工具

软件说明:反编译 Java 的 Class 的工具

光盘路径:\fanbianyi\jadnt157. zip

软件名称:idaPro_started

软件说明:idaPro_started 电子文档

光盘路径:\fanbianyi\idaPro_started. zip

软件名称:VB56Ded



软件说明:VB56Ded 这是一个不错的 VB5/6 反编译器,能协助破解 VB5/6 程序 Win95/98
光盘路径:\fanbianyi\VB56Ded.zip

侦测工具

软件名称:filemon

软件说明:监视系统文件运行状况,一般配合破解 Key File 保护。

光盘路径:\zhence\filemon\filemon.zip

软件名称:SMU Winspector

软件说明:显示 windows 程序的各项信息,如 Window - Handle, Window - Class Name, Window - Text 等。

光盘路径:\zhence\Winspector\SMU.zip

软件名称:gtw 2.56

软件说明:是一个文件格式观察软件,它现在是同类软件中最有活力和认识最多格式软件了。

光盘路径:\zhence\gtw\gtw.zip

软件名称:FileInfo v2.40

软件说明:在的软件越来越多的使用了加壳工具,给破解带来非常大的不便,要想知道这个软件使用了什么加壳软件非常的难,但是有了这个软件你就不用怕了他可以检测出这个软件是使用什么加壳软件加的壳,可以检测出 ASPACK 2001 了,推荐,十分好用。

光盘路径:\zhence\FileInfo\Fi240.zip

调试工具

软件名称:trackit

软件说明:作者是 RuFeng.这样我们除了 SOFTICE 和 TRW 2000 外,又有一款调试器可选用了,这款调试器与前两者有一点不同,它是针对 Crack 而设计优化的,其计划将 winsoftice、icedump、frogice、procdump、peedit、hexview 等与一身。目前版本是测试版,希望大家支持其发展,也希望大家将自己的建议提出,以便不断改进,建议运行前认真读 readme.txt。

光盘路径:\tiaoshi\tianyit\trackit045.zip

软件名称:Memory Dumper Version 1.0

软件说明:可抓取内存中文件的指定片段数据,可协助手动脱壳。

光盘路径:\tiaoshi\Memory\memdump.zip

软件名称:IceDump 6.016 and nticedump 1.8

软件说明:该版本较上一版做了较多的调整,命令操作完全不同。

光盘路径:\tiaoshi\IceDump\id6016.zip

软件名称:IcePatch 增强补丁

软件说明:让 Winice 不被加密程序检测到 Win9x

光盘路径:\tiaoshi\IcePatch\IcePatch.zip

软件名称:SoftICE Backdoor Keeper

软件说明:配合 FROGSICE,修改 2 个会被发现的 BUG Win9x

光盘路径:\tiaoshi\Backdoor\si_bd.zip

软件名称:FrogsICE v1.07.3

软件说明:适用 SoftICE 4.00 以上版本,欺骗程序 SOFTICE 没装载。 Win9x

光盘路径:\tiaoshi\frogs\FrogsICE.zip

软件名称:SmartCheck 6.03

软件说明:由 NuMega 公司出品,主要用来调试 VB 程序,支持 VB6。

光盘路径:\tiaoshi\smart\SmartCheck 6.03.zip

软件名称:FrogsICE v1.08.7 for win95/98/ME

软件说明:SoftICE 隐藏工具

光盘路径:\tiaoshi\softice\FrogsICE1087.zip

软件名称:Soft - ICE

软件说明:是目前公认最好的跟踪调试工具,此版又新增了对 AGP 的支持

光盘路径:\tiaoshi\softice\si405w9x\si405w9x.exe

软件名称:Winsoftice 4.05 for WinNT2K

软件说明:Windows NT 下的跟踪调试工具。Windows 2000 (NT 5.0) Beta 3 支持

光盘路径:\tiaoshi\softice\si405wnt.zip

软件名称:trw2000

软件说明:TRW2000 是一个运行于 Window 9x 的系统级高级调试工具。什么是系统级?它意味着 TRW2000 是工作于操作系统和硬件之间的,因此 TRW2000 能够调试或跟踪任何运行于 Winodws 平台上的程序代码(包括 DOS COM、DOS EXE、DOS 保护模式程序、16 位的 NE 程序、32 位的 PE 程序和工作于 0 级系统核心的 VxD 等等,也包括其他的系统级调试器)

光盘路径:\tiaoshi\trw\

编辑工具

软件名称:Hex Workshop 3.0

软件说明:强大的十六进制编辑工具,本人就用这个,觉得非常好用。

name: lee company: fs code: 00481 - 122411 - d3f9

光盘路径:\edit\Hex\hw32v30.zip

软件名称:Qview 2.8v

软件说明:功能强大。

光盘路径:\edit\Qview\Qview.zip



Pc friend ·

软件名称: HIEW 6.40 Registered Version
软件说明: 强大的十六进制编辑工具, 相当的好的反汇编功能, 破解利器。 Win95/98
光盘路径: \edit\HIEW\hiew640reg.zip

软件名称: Ultra - Edit v7.20a
软件说明: 最好的多用途编辑器
光盘路径: \edit\ultra\uedit32.zip \edit\ultra\uedit32\

脱壳工具

软件名称: UNASPACK
软件说明: 专门对付压缩软件 ASPACK 的工具! EXE 相关
光盘路径: \tuoke\UNASPACK1091.zip \tuoke\UNASPACK1090.zip

软件名称: UnSafeDisc
软件说明: 一个对付光盘加密软件 SafeDisc 的工具! EXE 相关
光盘路径: \tuoke\UnSafeDisc134.zip

软件名称: DBPE
软件说明: DBPE 1.5 BETA 3 不用多说, 一个巨大的 WIN9X EXE 加密软件, 当然, 它也是一个制作试用版本软件的利器。由 1.2 版本到现在已经有几个月的时间了, 现在我们来看看新版本有那些改进:

1. 修正不可同时运行两个加密程序的 bug。
2. 防脱壳性能进一步提升。
3. 修正限制流程的 bug。
4. 防跟踪, 防脱壳性能进一步提升。
5. 用 DLL 方式改写密码, 注册界面。
6. 支持用户编写密码, 注册界面, 加密后文件, 须带 dial.dll 运行。
7. 新增注册提示功能。
8. 修正加密文件在某些 windows 95, 97 系统下不能运行的 BUG。
9. 暂时去掉加密 DLL 文件支持。
10. 自动为加密文件生成 BAK 备份文件。EXE 相关

光盘路径: \tuoke\dbpe15b3.zip

软件名称: PEBundle
软件说明: 合并程序需要调用的 DLL 文件到 EXE 文件里面! 一来加密二来让软件简洁。这个版本加强了兼容性和改善了操作界面! EXE 相关。
光盘路径: \tuoke\pebsetup.exe

软件名称: Frogsice
软件说明: 我认为最好的 SOFT-ICE 加强软件! 它并不是简单的将 SICE 隐藏, 而是让你可以配合 SICE 避开现在流行的各种加密、保护软件里面的各种防止 SICE 的陷阱。有了它, 你再也不用怕在装入一个程序准备调试的时候, 程序告诉你发现 SICE 的存在而终止运行, 或者干脆把你的机器

从新启动, 又甚至触发更残酷的报复手段。EXE 相关
光盘路径: \tuoke\Frogsice.zip

软件名称: PECompact
软件说明: 一个很好的 WIN 32 EXE、DLL 压缩软件 EXE 相关 6-3
光盘路径: \tuoke\pesetup.exe

软件名称: Frogsice
软件说明: 我认为最好的 SOFT-ICE 加强软件! 它并不是简单的将 SICE 隐藏, 而是让你可以配合 SICE 避开现在流行的各种加密、保护软件里面的各种防止 SICE 的陷阱。有了它, 你再也不用怕在装入一个程序准备调试的时候, 程序告诉你发现 SICE 的存在而终止运行, 或者干脆把你的机器从新启动, 又甚至触发更残酷的报复手段。EXE 相关 5-31
光盘路径: \tuoke\Frogsice106.zip

软件名称: PECompact
软件说明: 一个 WIN9X 下还保持着频繁更新的 EXE 压缩软件, 当然, 出了更新快, 它的性能也是非常出色的。EXE 相关
光盘路径: \tuoke\pecsetup.exe

软件名称: PC Guard
软件说明: 一个相当不错的加密软件, 和 Armadillo 1.82、DBPE 等功能相似。哎, 现在也就只剩这几个同类软件了! EXE 相关 5-25
光盘路径: \tuoke\pcgw32d.zip

软件名称: PEBundle Write - To - Disk Edition
软件说明: 展开被 PE Bundle 0.6 合并了的 DLL 文件 EXE 相关 5-24
光盘路径: \tuoke\PEBundle-wtd015.zip \tuoke\PEBundle06.zip

软件名称: Armkiller
软件说明: 可以脱 Armadillo 1.82 壳的软件。EXE 相关
光盘路径: \tuoke\Armkiller.zip

软件名称: Tnopeunc
软件说明: 专门针对 PECompact 的脱壳软件, 这个版本支持 PECompact 1.30 EXE 相关
光盘路径: \tuoke\Tnopeunc15.zip

软件名称: Frogsice
软件说明: 我认为最好的 SOFT-ICE 加强软件! 它并不是简单的将 SICE 隐藏, 而是让你可以配合 SICE 避开现在流行的各种加密、保护软件里面的各种防止 SICE 的陷阱。有了它, 你再也不用怕在装入一个程序准备调试的时候, 程序告诉你发现 SICE 的存在而终止运行, 或者干脆把你的机器从新启动, 又甚至触发更残酷的报复手段。深入简出就只能这样描述它了, 有兴趣的朋友就快拿来研究、珍藏吧! 顺便对 DB 说说, 希望 DBPE 1.5 别让它继续漏网哦!;) EXE 相关



光盘路径:\tuoke\Frogsice10.zip

软件名称:SEX

软件说明:大家不要误会哦,这里的SEX是Softice Extension的简写,看来作者的取名功夫还真了得。它也是一个为SOFTICE添加了几个实用功能的SOFTICE增强工具。EXE相关

光盘路径:\tuoke\sex116b.zip

软件名称:GTW

软件说明:彻底侦察文件类型 EXE 相关

光盘路径:\tuoke\gtw256.zip

软件名称:PECompact

软件说明:能够存活下来同时的确是很不错的 EXE 压缩软件 EXE 相关

光盘路径:\tuoke\PEComp126b3.zip

软件名称:PEBundle Write - To - Disk Edition

软件说明:展开被 PE Bundle 0.6 合并了的 DLL 文件 EXE 相关

光盘路径:\tuoke\PEBundle-wtd014.zip \tuoke\PEBundle06.zip

软件名称:unpcguard

软件说明:UNPACKER FOR PC - GUARD 脱 PC - GUARD FOR DOS 的壳 脱壳

光盘路径:\tuoke\unpcguard.zip

软件名称:IceDump

软件说明:玩高级脱壳必备!脱壳

光盘路径:\tuoke\IceDump6015.zip

软件名称:UnArmadillo

软件说明:一个解除 Armadillo 所加壳的软件,支持最新的 1.80 版本。以前就有这个软件的前几个版本,但总是发觉不能跟上 Armadillo 的更新步伐,现在看来 UCF 的速度快多了,几天就搞出了这个新版本。看来还是等 DBPE 1.5 好点,起码我对它的防跟踪能力有信心点!)脱壳

光盘路径:\tuoke\UnArmadillo12.zip

软件名称:Codecrypt

软件说明:用加密保护软件,反跟踪等性能不错加壳

光盘路径:\tuoke\Codecrypt.zip

软件名称:tNO - Peunc

软件说明:脱 PE - COMPACT 压缩壳之工具,支持 WIN2K/NT 脱壳

光盘路径:\tuoke\tnoPeunc142.zip

软件名称:ASPack

软件说明:EXE 压缩

光盘路径:\tuoke\ASPack21.zip

软件名称:Blast Wave 2000 v0.2

软件说明:D.boy 冲击波 2000,它能轻易的找到任何加密壳的入口点.包括ASProtect以及幻影的加密壳。

光盘路径:\tuoke\Blast\bw2k02.zip

软件名称:UnAspack 1.0.9.1

软件说明:专门用来脱 ASPACK 壳的软件,这个版本支持 ASPack ASPack 2.1。 Win95/98

光盘路径:\tuoke\UnAspack\2UnAspack.zip

软件名称:ProcDump32 v1.6.2

软件说明:FINAL Windows 下最强的脱壳工具。 Win95/98

光盘路径:\tuoke\ProcDump\ProcDump32162.zip

帮助文件反编译工具

软件名称:Help & Manual 汉化补丁

软件说明:这个软件是第一个所见即所得的 Windows 帮助系统开发工具,并且支持中文。虽然现在已经有很多所见即所得的同类开发工具,但是这个软件的历史地位还是不可抹杀的。汉化补丁:phelpandmanualv14h.exe

光盘路径:\help\phelpandmanualv14h\phelpandmanualv14h.exe

软件名称:Helpme 汉化补丁

软件说明:一个基于 RTF 的小巧的帮助系统开发工具。汉化补丁:phelpme9.exe

光盘路径:\help\phelpme9\phelpme9.exe

软件名称:Help Workshop

软件说明:微软公司的 Help Workshop 是开发帮助系统必不可少的帮助文件编译器。可惜的是至今为止还没有中文版,即使在微软自己的中文版语言包如 Visual Basic 里也是这样。现在,公仆已经将它汉化了大部分,供开发和汉化帮助文件系统的网友们使用。相信汉化之后,微软公司也会在它的下个正式中文版的语言包里推出中文的 HCW 来吧。

光盘路径:英文版 \help\hew403.zip 汉化包(1600K): \help\phcw403.zip

软件名称:HTML Help WorkShop

软件说明:相当专业的超文本图形制作管理软件,可用于制作 Windows98 的帮助文件。

光盘路径:英文版 \help\htmlhelp\htmlhelp.exe 汉化包 \help\phtmlhelpa\phtmlhelpa.exe

软件名称:Web2HTMLHelp

软件说明:一个易于使用的全向导模式的帮助文件制作工具,它可以将您的网站或 HTML 文件转换成微软 HTML 格式的帮助文件。

Web2HTMLHelp 甚至允许您使用 HTMLHelp 的一些 undoc



Pc friend ·

umented 功能。

光盘路径:\help\p_web2hh1.zip

软件名称:HELPDECO 窗口界面程序

软件说明:它是著名的帮助文件反编译程序,和那个 DOS 程序一起运行。类似 ARJ.EXE 的界面程序

光盘路径:\help\duffos21.zip

软件名称:Help to RTF

软件说明:一个非常好的 Windows 帮助文件的转换工具,可将 .hlp 格式的文件转换成 .RTF 文件,这种 RTF 格式的文件是可以用 Microsoft Word 打开去阅读、编排或打印成册。因此这个软件又是个极好的帮助文件汉化工具!强烈推荐!

注册机 j-hlprtf.zip

光盘路径:英文版 \help\hlp2rtf\hlp2rtf.exe 汉化包\help\phlp2rtf\phlp2rtf.exe

Help to RTF 2.12 汉化中文版 \help\Hlp2rtf212k.zip

软件名称:KeyTools

软件说明:可以把 Windows 97 以后的编译 HTML 格式的帮助用户反编译,生成可以重新编译的源文件。这下对汉化 Windows97/98 的帮助文件不用愁了。

光盘路径:英文版 \help\keytoolssetup\keytoolssetup.exe 汉化包\help\pkeytools\pkeytools.exe

软件名称:Window Help Designer

软件说明:Windows Help Designer 是一款非常优秀的帮助系统制作开发工具,其所见即所得的特性让你非常轻松地入手,强大的宏功能,简便的图片、AVI、表格插入,可视化窗口、按钮定制,屏幕捕获、拼写检查、模板管理等,对开发帮助系统的专业人员和翻译帮助的汉人来说都是非常好的选择。(2.33 版本注册机)

光盘路径:英文版(3797K,版本:2.33) \help\whdprod233\whdprod233.exe 汉化包\help\whdprod233-p1.zip

英文版(3797K,版本:2.34) \help\whdprod\whdprod.exe 汉化包 \help\whd234-p.zip

Help Decompiler 2.1

其他相关工具

软件名称:iWatch

软件说明:这是一个由个人开发的全中文上网计费软件(适用于拨号用),它支持多个 ISP 帐号,完全符合中国国情的资费设置(包括按分钟和按固定小时计算的计费方案),上网费和电话费分别计算和显示,可设定超时报警,定时置零,可方便地查看和打印历史记录,还有美观而简洁的用户界面,可以说,这是目前为止能在网上找到的最好的中文上网计费软件。软件授权:共享软件。注册费用:10 RMB。使用平台:Win95/98

光盘路径:\examples\iWatch 311.zip

软件名称:侠客系统修改器 sysset.zip

软件说明:侠客系统修改器是共享软件,但未注册版也能进

行所有的功能设置,同时没有使用时间上的设置 运行平台:中文 Windows95/98/NT

光盘路径:\examples\sysset.zip

软件名称:离线浏览器 Teleport Pro

软件说明:Teleport Pro 是一款功能强大的离线浏览器,不论规模多大的网站,只要你设置妥当,无论网站目录、内容、图片影像、背景音乐,甚至 Java Applet 都能够完整地复制一份在你的硬盘中。

光盘路径:\examples\pro12\pro12.exe

软件名称:EXESCOPE 4.50

软件说明:其是 EXE、dll 资源修改器,很棒的哟!这个版本汉化很彻底,连帮助文件也汉化了!

光盘路径:\others\EXESCOPE\pexesc45.zip

软件名称:Windows Customizer

软件说明:对屏幕上出现的任何窗口,进行你想要的任何操作,比如使灰色的按钮变亮。

光盘路径:\others\Customizer\Custom.zip

软件名称:Masm32 v6

软件说明:最好的汇编编程工具

光盘路径:\others\masm\masm32v6.zip

软件名称:Regmon for Windows NT/9x v4.32

软件说明:注册表读写监视工具

光盘路径:\others\Regmon\Regmon95.zip

软件名称:MAKEPE 1.30

软件说明:一个 PE EXE 格式文件的组织重编译器,优化器,主要是用于优化被 PROCDUMP、TRW 等 WIN95 下的脱壳工具脱出来的 EXE 文件,很好的东西哦! Win95/98

光盘路径:\others\MAKEPE\makepe13.zip

软件名称:peditor1.5

软件说明:可修复 PE 文件头,并且可修复部分在 win98 脱壳后的程序不能在 win2000/NT 下运行的情况

光盘路径:peditor.zip

软件名称:icedump 6.016 & nticedump 1.8

软件说明:内存 DUMP 工具

光盘路径:\others\icedump\id6016.zip

软件名称:ERU

软件说明:这是 windows 安装盘自带的小工具,备份注册表等一些 windows 重要的配制文件,强烈推荐! Win95/98

光盘路径:\others\zhucebiao\ERU\ERU.zip

软件名称:reg101i

软件说明:比较注册表变化的软件,这个版本完善了一些功能,加上了一篇教学。 Win95/98



光盘路径: \others\zhucebiao\reg101i\reg101i. zip

软件名称: Regsnap 2.6

软件说明: 它可以详细地向你报告注册表及其他与系统有关项目的修改变化情况。RegSnap 对系统的比较报告非常具体, 对注册表可报告修改了哪些键, 修改前、后的值各是多少; 增加和删除了哪些键以及这些键的值。报告结果既可以从纯文本的方式, 也可以 html 网页的方式显示, 非常方便 Win95/98

光盘路径: \others\zhucebiao\Regsnap\Regsnap. zip

软件名称: CrackCode2000

软件说明: 强劲的内存读取注册码工具, 编程水平不高的你可以做出很优秀的注册机。带几个教学例子。Win95/98

光盘路径: \others\zhuceji\crackcode\CrackCode2000. zip

软件名称: Serials 2000

软件说明: 这我所用的所有注册码软件中最好的一个, 这不仅仅在于它的界面等小的方面, 他最大的特点就是能够升级资料库, 这样以来, 我们只需下载一次, 以后, 我们只要再下载几十 K 大小的升级库就可以了……(注册器的使用方法。) 升级文件 3 2000 年 11 月 1 日升级文件 Sn2000 v1.41 2000 年 11 月 9 日升级文件

升级文件 4 2000 年 11 月 15 日升级文件

Serials 2000 (10.15)

Serials 2000

serials 2000 8.15 号 升级库 26K

serials 2000 8.1 号 升级库 24K

serials 2000 7.15 号 升级库 22K

serials 2000 7.1 号 升级库 24K

serials 2000 6.15 号 升级库 20K

serials 2000 6.1 号 升级库 15K

注意: 这种升级为累记升级, 也就是说, 最新的一版并不包括以前更新的内容, 望朋友们注意。

光盘路径: \others\zhuceji\serials\

软件名称: Ghost 6.0 注册版

软件说明: 这是克隆硬盘的好工具, 特别是第一次装好系统后, 用其备份一系统, 因为我们 windows 系统软件装多, 系统性能会严重下降, 用它几分钟使系统恢复, 适合我们 Cracker。恢复操作时要仔细, 不要大意。不要将要恢复的分区搞错。

光盘路径: \others\fouzu\Ghost\ghost. zip

软件名称: Sync - It with Atom 1.50.863

软件说明: 玩 SOFTICE 或 TRW2000 时系统时间会停止, 每次校正时间是不是很烦。用它自动在 Internet 上搜索时间服务器, 后台自动校准你的系统时钟, 始终保持你的系统时钟的准确无误。ID: toye serial: 29e5ab59 Win95/98

光盘路径: \others\fouzu\Sync - It\syncit15. zip

软件名称: Process Patcher v3.60 内存补丁。

软件说明: 一个很棒的制作内存补丁工具, 同类软件的表表

者! Win9x/2K

光盘路径: \others\paths\Patcher\pPatcher. zip

软件名称: Patcher v1.5 内存补丁。

软件说明: 一个不错的内存动态补丁制作软件, 在同类软件中也可算是老牌“选手”了, 经过多次的升级, 现在性能已经很不错了。Win95/98

光盘路径: \others\paths\Process\pppv15. zip

软件名称: aPATCH v0.24b 文件补丁。

软件说明: APACK 作者写的一个制作补丁程序的软件 Win95/98

光盘路径: \others\paths\PATCHaPATCH24. zip

软件名称: CodeFusion 3.0 文件补丁

软件说明: 支持标准 windows 界面, 一个很好的做 PATCH (补丁程序) 软件。Win9x/NT

光盘路径: \others\paths\CodeFusion\codefs30. zip

软件名称: Ptasiek's CrackMaker 1.32 文件补丁

软件说明: 一补丁制作工具, 功能简单, 但实用。Win95/98

光盘路径: \others\paths\Ptasiek's\perkm. zip

安全工具

软件名称: WebWatch

软件说明: WebWatch 可以检测到个人主页的变化情况, 哪怕是微小的变化, 它也能检测到。只要将站点添加到 Web Watch 然后点击 Run 就可以了。

光盘路径: \safe\web1106watchv\web1106watchv1. exe

软件名称: IP 守护天使

软件说明: Nfrbof 只要有人扫描你, 它就会立即弹出窗口, 并告诉你此人的 IP, 然后怎么办, 自己看这办吧! 而且有可能对方还会掉线哦!

光盘路径: \safe\nfrbof\nfrbof. exe

软件名称: 网络卫兵

软件说明: 网络卫兵完全解密版。

光盘路径: \safe\webws. zip

软件名称: zonalM20

软件说明: 一个不错的防火墙软件, 它可以检查全部在你的计算机上与因特网的连接, 并控制哪个程序可以进行因特网的存取, 可报出于你联结的 ip, 还可看出是什么程序。

光盘路径: \safe\zonalM20\zonalM20. exe

软件名称: Anony cookie

软件说明: 能隐藏你上网的电话, IP, 帐号, 你只要在网上网前运行它就 OK 了。

光盘路径: \safe\setupac_b2. zip



Pc friend ·

软件名称: WithGate

软件说明: WithGate 是功能强大而且简单易用的 Internet 连接共享和网络安全防火墙软件,只需要一条电话线,一个 Modem,一个 Internet 帐号,安装了 WithGate 之后,整个局域网中的所有 PC 都可以访问 Internet,同时 WithGate 通过内建的安全防火墙,提供对局域网内部资源的周到保护,防止信息泄漏和黑客的攻击。

光盘路径: \safe\wgset901upwgset901up.exe

软件名称: getpass

软件说明: 如果你有机会在别人的机器上运行程序的话,运行这个程序,你就能得到他机器上所有能连网的电话号码、帐号、密码等。

光盘路径: \safe\getpass.zip

软件名称: 木马克星

软件说明: 通过对 179 种黑客程序的跟踪观察,经过对 6 种经典木马源代码的详细分析,终于找到了黑客软件的共性,产生了本软件,本软件采用纯动态监视网络连接技术,可以有效查杀目前绝大多数黑客程序,对未一定的感知功能,特别是对第 3 代文件关联型木马更可以动态识别,本软件占用系统资源较少,为你创造安全、快速的网络环境!新版本减少了对正常文件的误报!曾加了查杀的准确性!并且加入了远程查找木马功能。

光盘路径: \safe\iparmor1106iparmor1106.exe

软件名称: Trojan Remover

软件说明: 是一个专门用来清除特洛伊木马和自动修复系统文件的工具。能够检查系统登录文件、扫描 WIN.INI、SYSTEM.INI 和系统登录文件,且扫描完成后会产生 Log 信息文件,并帮你自动清除特洛伊木马和修复系统文件。

光盘路径: \safe\trjsetup1031trjsetup1031.exe \safe\trjsetup\trjsetup.exe

软件名称: Norton Personal Firewall 2001

软件说明: Norton 出品的个人防火墙将提供完整的网络安全,防止重要资料被窃,并有过滤网站的功能,能够阻隔各种网络黑客可能的入侵方式 Java applets, ActiveX 控制,以您的私人信息被窃取和损坏。

光盘路径: \safe\NPFtry1023\NPFtry1023.exe

软件名称: ZoneAlarm

软件说明: ZoneAlarm 是一个因特网安全实用程序和防火墙,它可以检查全部在你的计算机上与因特网的连接,并控制哪个程序可以进行因特网的存取。2.0 版结合了许多 ZoneAlarm 的改进性能和可用性,包括了完全而易用的安全级设置以及高级本地和因特网地区的本地防火墙能力。ZoneAlarm 来保护你的电脑,防止 Trojan (特洛伊木马)程序, Trojan 也是一种极为可怕的程序。ZoneAlarm 可以帮你执行这项重大任务喔。而且还是免费的。使用很简单,你只要在安装时填入你的资料,如有最新的 ZoneAlarm,你就可以免费网上更新。安装完后从新开机, ZoneAlarm 就会自动启动,

帮你执行任务。当有程序想要存取 Internet 时,如网络浏览器可能会出现连不上网络,这时你可以在右下角 ZoneAlarm 的小图示上按两下鼠标左键,选取 Programs 的选项,勾选你要让哪些软件上网,哪些不可以上网,利用此种方法来防治一些来路不明的软件偷偷上网。最好的方法是锁住(Lock)网络不让任何程序通过,只有你核准的软件才可以通行无阻。你还可利用它来看看你开机后已经使用多少网络资源,也可以设定锁定网络的时间。可以运行在 Windows 2000 上,可截获来自任何地方的点击和连接。并报出 IP 地址,以及是何种程序。界面非常漂亮!尤其适合于控制局域网内的 Internet 共享。

光盘路径: \safe\zonealarm.2.1.42.hh.bz\zonealarm.2.1.42.hh.bz.exe \safe\pzonealarm2026a_bz\pzonealarm2026a_bz.exe

杂项工具

软件名称: 追捕

软件说明: 修正 OICQ 号码探测功能,现在可以探测 OICQ 2000 测试版的 OICQ 号码,修改探测 OICQ 号码的方式,不再提示有人追踪。它能追查指定 IP 地址使用者的 OICQ 号码及信息!

光盘路径: 1.62 版本 \zaxiang\wryzip162.zip 1.61 版本 \zaxiang\wryzip161.zip

软件名称: 木马克星 2.10

软件说明: 可以查杀入侵微软的 qaz 木马类病毒,这个版本的扫描功能不需要注册。

光盘路径: \zaxiang\iparmor2.10.exe

软件名称: AWSPS v4.0 (Atelier Web Security Port Scanner 4.0)

软件说明: 功能很全的一个深度评估网络安全状况的工具,其中一些功能是该软件所特有的。下面列举部分它的功能:

- * 高速 TCP 扫描引擎,可定义同时打开端口的最大并发数和调整连接超时设置。
- * 高速 TCP 嗅探扫描引擎可做 Windows 2000 平台下 TCP/IP 和 ICMP 数据包捕获嗅探器。
- * 快速可靠的 UDP 端口扫描可自行判断主机是否打开。
- * NetBIOS 扫描器。
- * 端口扫描器。
- * 完整的本机网络状态,包括:连接侦听端口报告,TCP,UDP 和 ICMP 统计报告,路由,DNS 服务器报告,IP 统计设置报告,局网的详细信息……
- * 完整的 TCP/IP 端口数据库。

光盘路径: \zaxiang\shareall1.1.zip

软件名称: 鹦鹉螺网络助手

软件说明: 鹦鹉螺网络助手是一个集成了用于 TCP/IP 协议的多种网络工具的应用软件。她基于 Windows Socket2.0 版本,功能包括: Ping; Host lookup(主机查询); Finger(帐号查询); 同步本地主机时钟的 Time(网络时钟); WhoIs(域名查询); TraceRoute(路由跟踪); ISPPinger(以一定时间间隔持续



ping 同一台主机); QoD 服务; 增强的快速拨号; 支持多帐号的电邮检查等等。其他特性包括多功能的托盘图标, 在线检查软件升级, 获得本机 IP 地址, 将主机查询结果存入本地 HOSTS 文件等等。本软件适用于安装了 TCP/IP 协议的 Windows 9x 操作系统(包括 Windows 95, 97, 98 和 Windows ME)。本软件需要有 Microsoft Winsock 2.0 或更高版本才能正常工作。Windows 98 及以上版本在安装时即已带有, 而 Windows 95 用户可以从微软公司的网站下载有关的升级包。

光盘路径: \zaxiang\nautink160c.zip

软件名称: 局域网密码探测器 2.0

软件说明: 可以探测局域网网上共享文件夹的密码, 具有多种探测方式。

光盘路径: \zaxiang\lanpass2.zip

软件名称: Relco

软件说明: 专门修改冰河的图标工具。

光盘路径: \zaxiang\Relco.zip

软件名称: QQCAT1.0.ZIP

软件说明: 国产木马, 功能还可以, 端口 1001, 执行程序 c:\windows\system\internet.exe

光盘路径: \zaxiang\QQcat1.0.zip

软件名称: IP 炸弹 2.3 版本

软件说明: 只能炸没安补丁的机器, 还可知道被炸机器死掉没, 本身还带防护程序。

光盘路径: \zaxiang\nuke23.zip

软件名称: RecoverNT

软件说明: 作者提供恢复被“恶作剧之王”破坏数据后的程序。恢复率 100%。(前提是被格后不要再往硬盘写任何东西, 以免恢复不完全)。如果 C 盘有重要资料, 请拿到别人的电脑上作为从盘来恢复。这个是 WINDOWS NT 下运行的。

光盘路径: \zaxiang\RecoverNT.zip

软件名称: Recover98

软件说明: 作者提供恢复被“恶作剧之王”破坏数据后的程序。恢复率 100%。(前提是被格后不要再往硬盘写任何东西, 以免恢复不完全)。如果 C 盘有重要资料, 请拿到别人的电脑上作为从盘来恢复。这个是 WINDOWS 98 下运行的。

光盘路径: \zaxiang\Recover98.zip

软件名称: Last2000

软件说明: 国产木马黑洞 2000, 11 月 8 日的最后版本, 功能有密码、端口设置, 屏幕观察和控制屏幕多了几个选择, 彻底卸载及其它。

光盘路径: \zaxiang>Last2000.zip

软件名称: synflooder

软件说明: 最新的攻击 WIN2K 的工具, 属于傻瓜类型的。

光盘路径: \zaxiang\synflooder.zip

软件名称: dlme

软件说明: 网管们, 想限制你机器上的设备哪些可以被使用吗, DeviceLock 软体可以帮上忙这个是 for me/9x 的版本。

光盘路径: \zaxiang\dlme.zip

软件名称: 木马滴滴响“1.8 版本

软件说明: 是个扫描木马的软件, 同时还可以偷取本地机的上网帐号, OICQ, 邮箱等 * * * * 号。

光盘路径: \zaxiang\mmd1.8.zip

软件名称: WinGenocide

软件说明: 中文版可以对连续的 IP 进行大规模轰炸。

光盘路径: \zaxiang\WinGenocide.zip

软件名称: irckill

软件说明: 专用的 irc 聊天室捣乱工具, 非常不错。

光盘路径: \zaxiang\irckill.zip

软件名称: win-ftp

软件说明: 将自己的机器变成一台 ftp 服务器, 也可以将别人的……刷屏机 v1.01 版今天加上一个刷屏机, 可以刷几乎所有的聊天室(包括 oicq, IRC 等)

光盘路径: \zaxiang\win-ftp.zip

软件名称: 猎鹿人。

软件说明: 新加入了聊天室抓 IP 的功能和欺骗追捕误报木马的功能

光盘路径: \zaxiang\deerhunter.zip

软件名称: blade

软件说明: \zaxiang\小榕的解密码软件, 穷举法。

光盘路径: \zaxiang\blade.zip

软件名称: netknife

软件说明: 多线程高速穷举代理服务端口, 帮助系统管理员找出简单的用户口令。本版本更改了一个明显的 Bug, 同时优化了线程处理, 速度可以更快

光盘路径: \zaxiang\netknife.zip

软件名称: autochat

软件说明: 自动将指定的信息发送到网上的程序, 可以在任意的聊天室和社区内发表(我没试, 你可以试试)。

光盘路径: \zaxiang\autochat.zip

软件名称: iasetupfull

软件说明: 这是一个很不错的防火墙, 通过一个发图命令, 也能查到聊天室每个人的 IP, 宅主也是用这个防火墙的, 别人踢你, 你可以知道踢你 IP 是多少, 反正自从宅主用了他, 很少被人踢了, 除了网管……

光盘路径: \zaxiang\iasetupfull.zip

软件名称: 7thsph



Pc friend ·

软件说明: 瘟疫, 强劲而有力的攻击性武器!

光盘路径: \zaxiang\7thsph. zip

软件名称: NETSPY

软件说明: 基于 TCP/IP 文件传送的一个软件, 有兴趣的话就试一试, 和 BO 一样, 很爽啊!

光盘路径: \zaxiang\NETSPY

软件名称: Kaboom! 3

软件说明: Email 炸弹, 一次可发送匿名邮件 X 封。

光盘路径: \zaxiang\Kaboom! 3

软件名称: lockdown2000

软件说明: 是目前最好的防范特洛伊术的工具, 任何木马都逃不过它的眼睛, 自己的机器最好有一个。

光盘路径: \zaxiang\lockdown2000. exe

软件名称: firebustah

软件说明: 专门攻击防火墙工具。

光盘路径: \zaxiang\firebustah. zip

软件名称: pckbuilder

软件说明: 攻击软件, 包括: URG ACK PSH RST SYN FIN。

光盘路径: \zaxiang\pckbuilder. zip

软件名称: shangquan

软件说明: 山泉密码工具集, 可以远程查看口令, 文件, 进程, 运行远程程序等。

光盘路径: \zaxiang\shangquan. zip

软件名称: uloveme

软件说明: 一个和“妖之吻”差不多的恶作剧软件。破解方法: 在 dos 下把 windows 和 windows\system\目录下的 interenat. exe 删去, 把 system. ini 的 shell = c:\windows\interenat. exe 这一行去掉。

光盘路径: \zaxiang\uloveme. zip

软件名称: wnuke

软件说明: 新款炸弹, 据说可以饶过天网攻击 IP。(强力推荐)

光盘路径: \zaxiang\wnuke. zip

软件名称: rocketv

软件说明: 是一款踢外猫下线的东东

光盘路径: \zaxiang\rocketv1_0. zip

软件名称: Genius

软件说明: 包含了几十个非常有用的 internet 工具: ping, finger, smtp, telnet, time, TraceRoute, Whois, lookup, DNS 扫描仪, 邮件检查, 本机当前连接, FTP 搜索, IP 扫描仪, pop 邮件删除, FTP 客户端, HTTP 浏览器, 端口信息, 闹钟, 文本表格编辑器, 字典制作, 端口保护……反正功能有好多

光盘路径: \zaxiang\Genius. exe v3. 1

软件名称: length08. zip

软件说明: 黑客字典

光盘路径: \zaxiang\length08. zip

软件名称: godmessageIII. zip

软件说明: 一个前所未有的 Active X 木马! 压缩包里只有两个 html 文件和 readme 文件, 只要别人浏览此 HTML 文件, 那么内在的 Active X 程序就会对他硬盘进行操作(二进制传输), 在 IE5. X, WinNT, Win98 测试通过, 请仔细看 readme. txt!

光盘路径: \zaxiang\godmessageIII. zip

软件名称: igmp

软件说明: 全名是 IGMP Nuke OSR, 最新的 IP 攻击工具, 可以任意设置包裹大小和时间。

光盘路径: \zaxiang\igmp. zip

软件名称: HappyBrowser

软件说明: 是一个可以扫描到目标机器信息的工具。扫描包括 DNS、FTP、Finger、Server Info、Security 以及/cgi-bin/里的所有资料包括 cgi、asp 的错误代码以及 FTP 是否可以用 anonymous 等等! 你也可以当它是浏览器! 但是浏览的却是代码! 其感觉有点像是 Unix 下的 SATAN 和 Nt 下的 Retina 合并!

光盘路径: \zaxiang\HappyBrowser. zip

软件名称: 雪狐狸 IP 锄刀

软件说明: 国产 IP 炸弹。

光盘路径: \zaxiang\fox1. zip

软件名称: 雪狐狸 IP 天堂之路

软件说明: 国产 IP 炸弹。

光盘路径: \zaxiang\fox2. zip

软件名称: nthunterv2

软件说明: 最新的 WIN NT 攻击工具, 利用重复的 DOS 攻击和 OOB 攻击, 导致 WIN NT 服务器崩溃。

光盘路径: \zaxiang\nthunterv2. zip

软件名称: cs

软件说明: 远程控制计算机的源代码, 还有伪装功能, 每次编译后把 server. exe 改名为 getip. ocx, 运行一次 getip. exe 后, 因为修改了注册表, 每次开机都运行服务器端程序 server. exe, 你就可利用客户端程序控制主机了, 站长现在只加了不到二十条控制指令, 其它的请你自己来完成, 本程序仅供学习, 如果用此程序破坏别人的机器, 本人概不负责。最新版本加入了 clnsver. exe, 用于清除开机运行 server. exe, 这样你的计算机就不会被别人通过这个程序控制了

光盘路径: \zaxiang\cs. zip

软件名称: Iris

软件说明: eEye. com 公司新出的网络通信分析器——一个有



革新意义的网络管理软件,它能帮助 IT 人员用来监视他们内部网络的通信情况,可作为一个完全的系统工作管理看门狗。我简单的试用了下它,功能确实不错,如果不用它来管理局网的话把它当作一个网络协议分析器或者说是嗅探器我觉得也很好。平台:win9x/NT/2000(Internet Explorer 4.01 以上)

光盘路径:\zaxiang\lris.exe 1.0

软件名称:流光 2000

软件说明:Gold Edition Build 2150 (Preview 1) POP3/FTP/HTTP/PROXY/IPC Scanner 小榕的流光 2000 发布了,不错的工具,先看看它的说明吧。运行平台:win2000/winNT4.0

光盘路径:\zaxiang\flux2ksetup.exe

软件名称:RATCracker1.4.1

软件说明:有些木马患者的机器经常被人加密码,RATCracker 就是破解其密码的东东,这个最新版可以破解包括 sub7, netbus 在内的 10 多种木马密码。

光盘路径:\zaxiang\RATCracker.zip

软件名称:languard

软件说明:使用最新的网络嗅探技术,能监听所有进出的TCP/IP 包,功能:网络监视器,检测口令嗅探器,网络存取控制(可堵住外来数据也可限制网内用户的 internet 访问权限)。平台:win2000, winNT4.0

光盘路径:\zaxiang\languard.exe

软件名称:tini1

软件说明:一个用汇编写的 windows 后门(仅 3KB),它监听 TCP 端口 7777 并允许任何远程连接。1.2 版本修正前面版本的 bug,可以运行在 win9x 上了。平台:win95/98 win2000 winNT

光盘路径:\zaxiang\tini1.2.exe

软件名称:storm1.0

软件说明:一个在线暴力法破解 FTP、POP 用户密码的国产工具。用过 FTPhack 或者 FTPpass 的应该不会对这个界面陌生的。感觉不错,操作极其简单。

光盘路径:\zaxiang\storm.zip

软件名称:HCWC v1.0

软件说明:一种相当不错的攻击软件包,内含多种攻击武器,有些已经使用的相当普遍,但是其中一些攻击武器至今仍无可靠的防御办法所以仍然很实用。

光盘路径:\zaxiang\HCWC.zip

软件名称:ScanIP 2.0

软件说明:扫描你指定 IP 地址段上计算机的信息,包括:Net BIOS 信息,是否有共享,是否有 FTP、HTTP 和 TELNET 服务等,可调整扫描速度(如果你的带宽够宽的话),扫描速度极快(在登录到网络后再打开)。

光盘路径:\zaxiang\ScanIP.zip

软件名称:Inziderv1.2

软件说明:是用来发现监听端口的进程的软件。它能有效的发现隐藏在其它进程中的 Back Orifice 2000。平台:Windows 2000, Windows 95/98, Windows NT。

光盘路径:\zaxiang\Inzider.exe

软件名称:狐狸之眼 2.0(测试版)

软件说明:类似特洛伊木马的远程控制程序(前一版本是 1.0)。

光盘路径:\zaxiang\foxyeyesv2.zip

软件名称:ExploitGenerator - srb1

软件说明:很好的攻击工具,不可太过分哦,一切后果自负!

光盘路径:\zaxiang\ExploitGenerator - srb1.zip

软件名称:Evilftp

软件说明:微型 FTP 远程登陆程序,断口为 23456,删除方法 line Run = C:\windows\system\msrun.exe

光盘路径:\zaxiang\Evilftp.zip

软件名称:Cain v1.51

软件说明:一个用于破解局域网内共享资源密码的程序,速度比较快,支持断点破解。同时具有读取本机缓存中密码文件的功能。平台:Windows 2000, Windows 95/98, Windows NT。

光盘路径:\zaxiang\Cain.zip

Indoc 可对对方的机器信息,OUTLOOK,ICQ,硬盘,以及网络消息发送出去的木马。

软件名称:WyvernWorks Firewall

软件说明:使你的公开部分免受不法侵害,保护你的 IP 地址。

光盘路径:\zaxiang\41591fierwall.zip

软件名称:东方神钥 1.0b

软件说明:国产木马 1. 查看远程机屏幕变化;2. 实时跟踪鼠标和键盘输入;3. 获取系统信息:包括注册公司、当前用户、CPU 类型、系统路径、物理及逻辑磁盘信息等多项系统数据;4. 远程系统功能:包括远程关机、远程重启计算机、锁定鼠标、锁定注册表、禁止自动拨号等多项功能;5. 远程文件操作,完全像本地机一样方便;6. 注册表操作:包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能;7. 通讯:以聊天室形式同被监控端进行交谈。8. 发送信息:以四种图标及六种提示按钮向目标机发送简短信息;该版本在 Windows 9X/NT 下测试正常。

光盘路径:\zaxiang\netkey.zip

软件名称:打碎南瓜

软件说明:用来拿 ASP 的源文件,还可以实际检测一些 IIS 的路径暴露问题。

光盘路径:\zaxiang\asp.zip

软件名称:winsniff WinSniffer



Pc friend ·

软件说明:是支持 MS Windows 95/NT/2000 的第一个控制台嗅探器,拥有大量的功能。它能重新找回 POP3/TELNET/HITP/FTP/IMAP/NNTP 密码,并以 UNIX 信箱格式保存所有邮件信息。在这个程序中有一个创新:能个别分析每个协议(只提取登录名和密码),并把新情况保存下来。

光盘路径: \zaxiang\winsniff. zip

软件名称: starkun

软件说明:开玩笑的东东,运行后,会把你的 C 盘文件全部隐藏起来。这样下次启动的时候电脑就起不来了,需要 VB6 库文件才能运行。starkun. zip

光盘路径: \zaxiang\starkun. exe

软件名称: nassetup

软件说明:能够监视你计算机的 TCP/IP 端口,并在检测到远程连接时告警。该软件使用一个域名服务器解析出远程系统的 IP 地址。重新设计的 Net Alert 增强了软件稳定性,并更为轻巧和易用。

光盘路径: \zaxiang\nassetup. exe

软件名称: 灌水机的控件

软件说明:运行下面那个聊天室灌水机所需的控件,把里面的两个文件 copy 到 window 下的 system 目录里面就行了。

光盘路径: \zaxiang\dll. zip

软件名称: 聊天室灌水机 V1.0 测试版

软件说明:这是一个很有特色的刷屏工具噢!基本上能刷所有的聊天室~包括 oicq 的,千万别用来捣乱哈。感谢激光小子给我提供程序。

光盘路径: \zaxiang\chatbomb. exe

软件名称: 网络 Shotgun 之 Finger000618

软件说明:可以 finger 主机的用户(自动使用多个常用账号测试)可以做 whois 查询(查看 ip 地址或域名的注册信息)。

光盘路径: \zaxiang\fingerf. zip

软件名称: firebot 2.7 复仇者 2.7。

软件说明:是一个适合初学者到骨灰级网虫使用强大的聊天工具,为 263 和浪子网管所推荐,首都在线全国聊天网络<263 irc>多数的网管使用此程序管理聊天室。此程序具备完全自动的管理功能并且所有的功能参数均能直接修改,而无须修改代码。复仇者能在 10 个房间同时管理无限的人员的秩序,计算准确,每个参数取值均经过 2 年的网管管理经验所得,是每个 aop 到 admin 的好帮手。全面的打架、骂人和泡妞功能,收集长期活跃于 irc 的几位老网虫招式,并且有英文版本的招式。本 bot 收集了 irc 协议中几乎所有的命令,其命令从一个 user 到 admin 都全部具备。并且支持隐藏密码功能,更适合网吧中使用。

光盘路径: \zaxiang\firebot2.7. exe

软件名称: 网狐

软件说明:功能强大的一个 IP 工具包

光盘路径: \zaxiang\netfox. zip

软件名称: 白鸽 V0.2

软件说明:查看 ASP 的简易工具,内附源程序。

光盘路径: \zaxiang\dove. zip

软件名称: Iphaker

软件说明:独孤剑客神剑之一,是一个很好的 IP 炸弹,推荐经常在聊天室被炸的人用一下,感觉一定很好!被炸的人 = 系统变慢 = 蓝屏 = 重新启动

光盘路径: \zaxiang\ip1. exe

软件名称: iphaker 2

软件说明:独孤剑客神剑之一的第二版,宅主随便抓了一个 IP 试了一下,效果绝对不错!而且在界面上有了很大的修改,增加了不少功能,有兴趣的不妨试一试。

光盘路径: \zaxiang\ipzd. zip

软件名称: 歼击机 V0.01

软件说明: igmp 炸弹

光盘路径: \zaxiang\fighter. zip

软件名称: ICQ 木马程序

软件说明:是一个新版本的 ICQ 木马程序,没有用过,自己试试吧!

光盘路径: \zaxiang\icqbo. zip

软件名称: CrazyTalk 快聊

软件说明:网上聊天辅助软件,分为“常用”、“表情”、“动作”、“玩笑”、“爱情”、“OpenICQ”六栏。内置数千条聊天记录,支持昵称代换,界面声效。可以方便地增加、修改、删除、移动、导出、导入聊天记录,并为 OpenICQ 的聊天室聊天指令定制了聊天代换功能。

光盘路径: \zaxiang\kuailiao. zip

软件名称: 视窗幽灵 2.0

软件说明:本程序能够记录目标计算机上一切活动,并且将记录文件发送到你预先设定好的邮箱内。

光盘路径: \zaxiang\mf20. zip

软件名称: 网络刺客

软件说明:这个软件是天行的产品,我想信大家都有所了解,我在这里就不用多说,自己当一个试试吧!

光盘路径: \zaxiang\tx. zip

软件名称: WebPosition Gold

软件说明:分析你的站点在顶级搜索引擎的排列情况,然后生成一份易懂的报告帮助提高站点的排名。

光盘路径: \zaxiang\wpgoldsetup1030. exe

软件名称: TopDog Web Position Analyzer/Submitter

软件说明:分析你的站点在顶级搜索引擎的排列情况,然后



生成一份易懂的报告帮助提高站点的排名。

光盘路径: \zaxiang\TopDogSetup1024.exe

软件名称: Jelawat

软件说明: 一个用于 MP3 文件大范围搜索、交换、共享的中文网络软件, 类似于 Napster, 但具有很强的中文搜索能力, 及支持多线程下载, 加快下载速度。

光盘路径: \zaxiang\jelawat1b31017.exe

软件名称: SuperBot SuperBot

软件说明: 帮您将整个网站搬回家 SuperBot 是个全自动的离线浏览软件, 您不需要做太多的设定, 便可以将自己想看的网站给整个搬回家! SuperBot 与一般的离线浏览软件最大的不同处在于它的操作使用相当简单, 您只要设定好想要下载的网站路径以及下载网页存放的路径, SuperBot 便可以自动为您进行网页下载的工作了, 不过这坪要注意的是, 如果您想要下载存放的网站相当大的话, 您可能要花相当长的时间等待。

光盘路径: sb1101 版本 \zaxiang\sb1101.exe sb0905 版本 \zaxiang\sb0905.exe

软件名称: WebZip

软件说明: 把一个网站下载并压缩到一个单独的 ZIP 文件中, 可以帮您将某个站全部或部份之资料以 ZIP 格式压缩起来, 可供你日后快速浏览这个网站。且新一版的功能包括可排定时间来下载, 亦加强相当漂亮的立体界面及传输的曲线图。

光盘路径: \zaxiang\WebZip.exe

软件名称: Hyper Maker HTML

软件说明: 是一个离线浏览器, 让你把 HTML 页面及其相关图片、多媒体文件打包在一个压缩文件里, 从而建立和发布一个基于 HTML 的出版物, 支持多个语种。

光盘路径: \zaxiang\hypermaker20001024.exe

软件名称: Personal Internet Engine

软件说明: 离线浏览器, 可以下载指定网站, 并用树型结构进行显示, 支持进行查找。

光盘路径: \zaxiang\pie_s810etup.exe

软件名称: SuperBot

软件说明: 帮您将整个网站搬回家 SuperBot 是个全自动的离线浏览软件, 您不需要做太多的设定, 便可以将自己想看的网站给整个搬回家! SuperBot 与一般的离线浏览软件最大的不同处在于它的操作使用相当简单, 您只要设定好想要下载的网站路径以及下载网页存放的路径, SuperBot 便可以自动为您进行网页下载的工作了, 不过这坪要注意的是, 如果您想要下载存放的网站相当大的话, 您可能要花相当长的时间等待。

光盘路径: \zaxiang\sb_beta.exe

软件名称: 流影 POP3 Edition Beta 1

软件说明: 远程 POP3 扫描工具, 远程运行, 本地用 Telnet 控制。适合于 NT 熟练用户使用。For Windows NT/2000

光盘路径: \zaxiang\fspop.zip

软件名称: 流影 HTTP Edition Beta 1

软件说明: 远程 HTTP 401 登陆方式扫描工具, 远程运行, 本地用 Telnet 控制。适合于 NT 熟练用户使用 fshttp.zip For Windows NT/2000

光盘路径: \zaxiang\fspop.zip

软件名称: fromset

软件说明: [流光 II]2.5 置文件使用方 fromset.zip

光盘路径: \zaxiang\fromset.zip

软件名称: 溯雪 Beta 7

软件说明: 溯雪英文版基于 WEB 的探测器 For Win98/NT/2000 dansnowb7setup.exe

光盘路径: \zaxiang\dansnowb7setup.exe

软件名称: RunAsEx

软件说明: 指定帐号创建进程工具 runasex.exe For NT4.0/2000

光盘路径: \zaxiang\runasex.exe

软件名称: 乱刀 1.25SE

软件说明: 乱刀 1.25SE Unix Password Killer bladese.exe

光盘路径: \zaxiang\bladese.exe

软件名称: IIS4 DOS (IIS4 拒绝服务检测工具)

软件说明: IS4 DOS (IIS4 拒绝服务检测工具) i

光盘路径: \zaxiang\iis4dos.exe

软件名称: 诱鼠器

软件说明: 诱鼠器(一个恶作剧的小软件 7K)Ctrl + Alt + Del 结束任务

光盘路径: \zaxiang\allure.zip

软件名称: 黑客字典 II(中文版 200K)

软件说明: Name: Banyet Code: O8G22M cultradict.zip

光盘路径: \zaxiang\cultradict.zip

软件名称: 黑客字典 II(英文版 180K)

软件说明: Name: Banyet Code: O8G22M eultradict.zip

光盘路径: \zaxiang\eultradict.zip

软件名称: DES 算法源代码(C++ 38K) des.zip

软件说明: Fancy Bunny (Java Game) fencybunny.exe

光盘路径: \zaxiang\des.zip

软件名称: ucgi200.c CGI 漏洞扫描器 2.00 版。

软件说明: 可以检测 173 个 CGI 漏洞, 在 linux, freebsd 和 ir



Pc friend ·

ix 上运行

光盘路径:\zaxiang\ ucgi200. c

软件名称:Distributed Sniffer Pro netxray

软件说明:大家用过吧,功能的强大恐怕也有所领会,可是这么强大的东西只是 NAI Snaffer Pro 3 的一小部分,网络信息截取的最强者。不过这个软件太庞大了

光盘路径:\zaxiang\ dspconsl. exe

软件名称:PowerTerm InterConnect/32

软件说明:一个界面友好的 telnet 工具。支持 UNIX、VAX、IBM AS/400 及 IBM Mainframe,拥有容易使用的工具条以及一个有用的 FTP 终端。

光盘路径:\zaxiang\ ptwd32e2000-2-16. exe

软件名称:ShadowScan

软件说明:一个很棒的软件,有多种探测方法,还有多种破解密码的功能,还可以破解 unix、zip、rar 等的密码。可谓全方面发展的一个软件呀!强烈推荐!注册码 name: yangnanpassword : PDH33DNZE32Y ShadowScan. zip

光盘路径:\zaxiang\ ShadowScan. zip

软件名称:IPeye

软件说明:是为 windows2000 设计的扫描工具,具有 TCP port scan, SYN scan, FIN scan 和 Null scan 的功能。ipeye. zip

光盘路径:\zaxiang\ ipeye. zip

软件名称:诱鼠器

软件说明:(一个恶作剧的小软件 7K)Ctrl + Alt + Del 结束任务

光盘路径:\zaxiang\ alluresource. zip

软件名称:webscanner

软件说明:国产 WEB 扫描器 webscanner. zip

光盘路径:\zaxiang\ webscanner. zip

sniffit. 0. 3. 5. tar 这才是真正意义上的 SINFFER sniffit . 0. 3. 5. tar

软件名称:NukeNabber

软件说明:是炸弹,但也有扫描功能

光盘路径:\zaxiang\ nm29. exe

软件名称:OGRE

软件说明:这个东东是我推荐大家使用的,网络上稍有漏洞的机器就会被它扫到,我这里就不多介绍了

光盘路径:\zaxiang\ OGRE. zip

软件名称>Password Recovery Kit

软件说明:一套密码恢复软件包。能恢复十七种密码软件

光盘路径:\zaxiang\ 17866kitd. exe

软件名称:Invisible KeyLogger nt

软件说明:你想知道 administrator 的口令吗?用它吧!

光盘路径:\zaxiang\ 2693iksnt10d. exe

软件名称:Windows NT Key

软件说明:可以帮助你恢复忘记或遗失 Windows NT 操作系统启动密码。支持 Windows NT Workstation 和 Server 3. 50/3. 51/4. 0 所有启动密码。使用上相当简单,程序本身会将文件安装到安装 NT 时所制作的紧急开机磁片,在使用该紧急开机磁片开机执行 Windows NT Key,即可将密码恢复。另外,如果你没有安装 NT 时所制作的紧急开机磁片也可以利用 Windows NT Key 这个程序制作紧急开机磁片,不过你得有 NT 的光盘才行。ntkd2. 90. exe ntkd2. exe

光盘路径:\zaxiang\ ntkd2. 90exe \zaxiang\ ntkd2. exe

软件名称:Fast zip

软件说明:快速破解 ZIP 文件的密码 速度超快

光盘路径:\zaxiang\ Fastzip. zip

软件名称:Pwl viewer

软件说明:直接查看 Pwl 中存放的网络密码

光盘路径:\zaxiang\ pwl. zip

软件名称:letmein

软件说明:著名台湾黑客 Coolfire 所写的 Telnet (23) 密码破解软件需要 VB40032. DLL 文件

光盘路径:\zaxiang\ letmein. zip

软件名称:openpass

软件说明:WINDOWS 下查看密码的工具

光盘路径:\zaxiang\ openpass. zip \zaxiang\ openpass1. zip

软件名称:claym

软件说明:破解用户密码的工具。LETMEIN 都是用它改编的 claym. zip

光盘路径:\zaxiang\ claym. zip

软件名称:psender

软件说明:如果你入侵的主机运行一下的话,那么以后主机再上网,其所有用到的密码就被秘密发送到你指定的信箱了,所以,建议大家只要机器以前中过木马什么的,所有的密码可就不一定安

光盘路径:\zaxiang\ psender. zip

软件名称:cnem40195. exe

软件说明:IE4. 01 简体中文版补丁。微软出。这个补丁可以防止 IE4 受恶意破坏。某些包含“EMBED”标签的网页会令你的 IE4 崩溃,千万小心!!

光盘路径:\zaxiang\ dxun9. exe

软件名称:gdiupd. exe

软件说明:IE5 补丁修正 IE5 中 GDI 的补丁,GOOD。



光盘路径: \zaxiang\gdiupd. exe

软件名称: vtcpup20. exe

软件说明: 158K 微软 tcp/ip 的补丁 vipup20. exe 176K 微软 tcp/ip 的另一个补丁

光盘路径: \zaxiang\vtcpup20. exe

软件名称: scr31. exe

软件说明: 472K 你一定遇到过上网时 EXPLORE 崩溃的情况吧! 这个东西能够使这种情况不在发生。这个程序是在 WINDOWS UPDATE 上得到的, 肯定有效。

光盘路径: \zaxiang\scr31. exe

软件名称: scr31

软件说明: 你一定遇到过上网时 EXPLORE 崩溃的情况吧! 这个东西能够使这种情况不在发生。这个程序是在 WINDOWS UPDATE 上得到的, 肯定有效。

光盘路径: \zaxiang\scr31. exe

软件名称: SecureCRT

软件说明: 有流行 CRT Telnet 客户机的所有特点, 包括: 自动注册、对不同主机保持不同的特性、打印功能、颜色设置、可变屏幕尺寸、用户定义的键位图和优良的 VT100, VT102, VT220 和 ANSI 竞争。能从命令行中运行或从浏览器中运行。其它特点包括文本手稿、易于使用的工具条、用户的键位图编辑器、可定制的 ANSI 颜色等。

光盘路径: \zaxiang\scrt312. exe

软件名称: VIEWPWD?1. 0

软件说明: 与十字星一样的 PASSWORD 观看工具, 更小巧, 无需安装

光盘路径: \zaxiang\viewpwd. exe

软件名称: wsockupd

软件说明: MS DUN12 升级文件

光盘路径: \zaxiang\ wsockupd95. exe

软件名称: antimuke

软件说明: Windows 95 和 Windows NT, 免疫程序:

光盘路径: \zaxiang\ antimuke. exe

软件名称: martWhois

软件说明: 网络查询工具, 能查询 IP 地址或域名的位置、注册人、联系信息等, 它还可以对数据进行缓存, 使你可以建立自己的数据库, 支持 Socks5 防火墙。

光盘路径: \zaxiang\ sw21102. zip

软件名称: ommViews

软件说明: 对于网管人员来说, 可以利用“CommView”来观察网络连线、重要的 IP 资料统计分析, 如 TCP、UDP、及 ICMP, 并可显示内部及外部 IP 位址、Port 位置、主机名称等重要资讯, 且可将所取得资料储存至硬盘中以备查阅。

光盘路径: \zaxiang\ cv21101. zip

软件名称: Boss Everywhere Boss Everywhere

软件说明: 是一个无害的安全应用, 它隐蔽的运行, 记录使用者的使用情况。记录什么程序被人用了, 用了多长时间, 和相关软件的情况。还能报告访问过的 URL。

光盘路径: \zaxiang\b1019ssevrwr. zip

软件名称: OstroSoft Internet Tools OstroSoft Internet Tools

软件说明: 能帮助你发现网络上被隐藏的资源, 发现安全漏洞并且修补它。它还是一个 Ping/Finger 工具, 提供主机和端口扫描功能。

光盘路径: \zaxiang\ ostronet5. 2Build40927. exe

软件名称: newglacier

软件说明: 著名木马 - 冰河的最新版本

光盘路径: \zaxiang\ newglacier. zip

软件名称: topbv1

可将木马隐藏到别的文件之中去, 应某些网友的需要, 近且放上来。

光盘路径: \zaxiang\ topbv1. zip

软件名称: thing16

软件说明: 这个木马再国外的黑站里的木马下载排行中, 仅次于 SUB7 和 NETBUS

光盘路径: \zaxiang\ thing16. zip

软件名称: TELNET 软件

软件说明: 很好用的 TELNET 软件。这是一个终端仿真程序, 是连接远程运行 UNIX 和 VMS 系统主机的理想选择。它支持 VT100, VT102, VT220 和 ANSI 终端仿真, 包含基于文件的脚本, 简单易用的工具条等等。

光盘路径: \zaxiang\ crt370332bt. exe

软件名称: 0

软件说明: 新易超级搜索器的出现使所有目前流行的搜索工具软件和新闻阅读工具软件黯然失色, 该软件一经推出, 就被国内许多著名专业站点评为五星级软件, 并在几乎国内所有著名下载站点提供其试用版本的免费下载。如果您发现有比我们这款软件功能强的其他同类软件, 可来信告知。

光盘路径: \zaxiang\ NewSearch2. exe

软件名称: Remote Administrator

软件说明: 远程控制你的计算机, 你可以在本地看见远程计算机的屏幕显示, 本地的鼠标、键盘的有关反应也会传送到远程计算机

光盘路径: \zaxiang\ 9354radmin11. zip

软件名称: absturz

软件说明: 木马, 可关闭其机器

光盘路径: \zaxiang\ absturz. zip



Pc friend ·

软件名称:gf135

软件说明:GIRLFRIEND 的最新版本 1.35

光盘路径:\zaxiang\gf135.zip

软件名称:WINCRASH

软件说明:WinCrash13 的改进型,增加了许多功能

光盘路径:\zaxiang\WINCRASH2.zip

软件名称:exejoiner

软件说明:将木马加入其他可执行文件中

光盘路径:\zaxiang\exejoiner.zip

软件名称:bosniffer

软件说明:监听 BO 端口,使用起来就象 SpeakEasy

光盘路径:\zaxiang\bosniffer12.zip

软件名称:acidshiver

软件说明:高级木马,可以发送 MAIL 到控制端

光盘路径:\zaxiang\acidshiver.zip

软件名称:phucker

软件说明:类似 BO 的东西,目前没有工具能查杀!

光盘路径:\zaxiang\pphucker.zip

软件名称:pcAnywhere

软件说明:远程控制软件,你可以将你的电脑当成主控端去控制远方另一台同样安装有 pcANYWHERE 的电脑(被控端),你可以使用被控端电脑上的程序或在主控端与被控端之间互传文件。你也可以使用其闸道功能让多台电脑共享一台 MODEM 或是向网路使用者提供打进或打出的功能。

光盘路径:\zaxiang\pcanywhere.exe

软件名称:pcAnywhere 9.20Build

软件说明:远程控制软件,你可以将你的电脑当成主控端去控制远方另一台同样安装有 pcANYWHERE 的电脑(被控端),你可以使用被控端电脑上的程序或在主控端与被控端之间互传文件。你也可以使用其闸道功能让多台电脑共享一台 MODEM 或是向网路使用者提供打进或打出的功能。

光盘路径:\zaxiang\pcanywhere920.exe

软件名称:spiderce

软件说明:国产木马,很出色,但不是很出名

光盘路径:\zaxiang\spiderce.zip

软件名称:Girlfriend

软件说明:一个超级木马,非常罕见的东东

光盘路径:\zaxiang\Girlfriend.zip

软件名称:master97

软件说明:比较少见的木马,但功能还不错,可以试一试。

光盘路径:\zaxiang\master97.zip

软件名称:sspy

软件说明:这个软件功能很简单,就是你自己设定监视的端口,如果有人扫描你,它就会报警,告诉你企图入侵者的主机名和 ip 地址,比如你就开个 7626、7306 端口。相信不少木马爱好者对你感兴趣,当然,都在你的掌握之中

光盘路径:\zaxiang\sspy.zip

软件名称:mp3 easy

软件说明:你只需在输入栏里填入乐曲名或作家名或其他相关因素,就能自动搜索并将之下载的工具。

光盘路径:\zaxiang\mp3easy.exe

软件名称:sinps

软件说明:使用十分方便的端口扫描工具,其默认的端口范围从 1 到 65535,速度不错哦

光盘路径:\zaxiang\sinps.zip

软件名称:Msunke

软件说明:一个 WIDWOS 的端口攻击器

光盘路径:\zaxiang\Msnuke.zip

软件名称:GateScan

软件说明:扫描 WINGATE 的 IP 的工具。

光盘路径:\zaxiang\GateScan.zip

软件名称:whatsrunning

软件说明:识别对方操作系统的工具

光盘路径:\zaxiang\whatsrunning-1.zip

软件名称:Sd - Searcher

软件说明:强大的桌面搜索引擎。

光盘路径:\zaxiang\sd_searcher20.zip

软件名称:AddAce

软件说明:看看你的站点都在那些搜索引擎上注册了,这个程序能够追踪从搜索引擎访问你站点的记录,并且给你一份详细的报告和一份参考报告,告诉你应该怎么做,你的站点才能在搜索引擎上频繁出现,增加你的访问量。

光盘路径:\zaxiang\asetup.exe

软件名称:Sasquatch Sasquatch

软件说明:使你可以关闭或者重新启动任何运行着 Sasquatch Server 的计算机,这个 TCP/IP 程序作为一个 telnet 服务器在系统的托盘中运行,等待任何标准的 telnet 客户端发出请求。基本的安全功能包括让用户输入帐号和密码以便确定用户有权远程关闭计算机。当 telnet 会话建立后,用户可以得到远程计算机系统的时间信息,并且可以关闭或者重新启动计算机。用户还可以选择在系统被远程关闭前需要确认或者是运行一个应用程序,这个程序可以手动启动也可以自动随 Windows 启动。

光盘路径:\zaxiang\sasqutch.zip



软件名称:jufmp3seek205

软件说明:飓风 MP3 搜索通整合了中文 MP3 歌曲的搜索,验证,下载等全方位功能,是一款必备的网络利器,它立即以最快的速度在国内各大音乐库搜索您的歌曲并按歌名,文件大小,下载地址等详细显示结果,您如果记不得一首歌的详细名字,只要输入歌名的部分文字,飓风 MP3 搜索通照样可以帮您找到您的歌曲。

光盘路径:\zaxiang\ jufmp3seek205.exe

软件名称:cyberkit

软件说明:功能强大的 TCP/IP 的跟踪工具。强烈推荐

光盘路径:\zaxiang\ cyberkit.zip

软件名称:ATLAS

软件说明:WINDOWS/DOS 的 CGI 漏洞扫描工具,能扫 65 种漏洞

光盘路径:\zaxiang\ atlas.zip

软件名称:nss_2000pre71

软件说明:Narrow Security Scanner 2000 的新版本,可以查找出 341 远程漏洞,用 PERL 写成,在 Redhat, FreeBSD, and OpenBSD, Slackware, and SuSE 通过了测试

光盘路径:\zaxiang\ nss_2000pre71.tar

软件名称:Research Spider

软件说明:快速的网上查找工具。与其他同类软件不同的是,它不是依托其他搜索引擎的搜索结果进行查找的,而是自己访问网络然后返回相关内容的。您还可用它对返回的查找结果进行再查找!

光盘路径:\zaxiang\ rspider.zip

软件名称:Traffic Seeker

软件说明:在 10 分钟就能把你的站点注册到超过 8000 个搜索引擎上,成采用开放式的管理,让你能够对搜索引擎数据库进行添加/编辑/删除,这样你就能把中国的搜索引擎加进去,好让你的中文网站能够注册。同时提交多个 URL。未注册版只能发送到 50 个搜索引擎。

光盘路径:\zaxiang\ trafficpro.exe

软件名称:b1868full

软件说明:一防黑工具,能侦察谁在扫你的端口(port),也可给对方一个忠告

光盘路径:\zaxiang\ b1868full.zip

软件名称:geoboy

软件说明:一个地理跟踪的有力工具能跟踪并且显示穿越因特网走的线路,是从地图上显示出的,挺新颖的。

光盘路径:\zaxiang\ geoboy.exe

软件名称:LeapFTP

软件说明:功能强大,媲美 Bullet Proof FTP 的 FTP 软件。跟 Netscape 相仿的书签形式,连线更加方便。下载与上传文件

支持续传。可下载或上传整个目录,亦可直接删除整个目录。可让你编列顺序一次下载或上传同一站台中不同目录下的文件。浏览网页时若在文件连上按鼠标右键选[复制捷径]便会自动下载该文件。具有不会因闲置过久而被站台踢出的功能。可直接编辑远端 Server 上的文件。可设定文件传送完毕自动中断 Modem 连接。

光盘路径:\zaxiang\ leapftp.zip

软件名称:FTP Control FTP Control (TransSoft)

软件说明:是一个用于下载和上传文件的程序,它支持 Web 下载与 FTP 下载,并可自动续传,具有搜寻服务器端文件目录、自动拨号上网、书签管理、支援 Proxy,支持上下下载续传等功能。

光盘路径:\zaxiang\ ft1104pcontr.exe

软件名称:ftpctrl400

软件说明:ftp 客户端软件

光盘路径:\zaxiang\ ftpctrl400.exe

软件名称:FTP Voyager

软件说明:类似 Windows Explorer 的 FTP 客户程序,可以自动恢复中断的上载或下载,支持文件拖放,能在同一时间存取和浏览不同的站点,后台在一个 FTP 站点上查找文件。内建超过六十余个名下载站点供您选择,包括微软站点、共享软件、游戏及网络工具等等;其操作介面与文件管理器相似,您只要花几分钟即可熟悉。在功能方面,除了拖曳功能外,尚包括直接执行或阅读远端的文件、背景传输、背景文件搜寻以及一边下载软件一边浏览其他站点等,另有过滤功能让您选择列出或不要列出特定的文件。它还提供 Queue 功能,可以把一个 FTP 站中您所下载的各个目录中的文件,先拉到这个 Queue 窗口,最后再一次下载。

光盘路径:\zaxiang\ftpvsetup1103.exe

软件名称:AddWeb

软件说明:自动提交你的网站到上百个查询引擎,主要特色包括:多站点简介,自动频繁引擎数据更新,多站点提交允许你一次提交多个网站,查询引擎检查,PageBuilder 产生更好的查询效果,HTML、TXT 和 E-Mail 报告,Proxy 支持等等。

光盘路径:\zaxiang\ addweb1011.exe

软件名称:CuteFTP

软件说明:使用容易且很受欢迎的 FTP 软件,下载文件支持续传、可下载或上传整个目录、具有不会因闲置过久而被站台踢出站台。可以上载下载队列,上载断点续传,整个目录覆盖和删除等

光盘路径:\zaxiang\ cute4232bc1030.exe

软件名称:SureSync Real-Time

软件说明:该软件可以实现多个服务器间文件的实时镜像。

光盘路径:\zaxiang\ sync1028nst.exe



第一章 初窥门径

1.1 必要条件

要想成为一名出色的 Cracker, 以下条件是必备的: 1. 知识 2. 经验 3. 感觉 4. 耐心 5. 运气。

如果你刚开始学 Crack, 也许你遇到不少麻烦, 并且有点想退却, 这时切忌不要着急, 只要你认真学习, 成功就在眼前。没有人是生来就什么都会的, 如果你有问题, 就大胆地去问你周围的人或者到网上求助。计算机水平不高怎么办? 没关系, 这个领域只要努力学习就能成功。

所谓“知识”只要你肯学就可以了, 刚入门时如你没汇编知识是不行的, 你要掌握一下这门编程语言, 能看懂就能上手, 但是你想很顺手的话, 除了把汇编掌握好, 还要有编程的基本功夫。

“经验”是跟你破解软件时间, 掌握程度有关, 接触多了, 拿到一软件应该知道用哪种方法比较省事, 比较有把握。

“感觉”这点不可言传, 就像我们做语文题目时, 一句话有语法错误一看就知道, 这时我们有可能从语法上也说不出什么道道, 就知它是错的, 这就是语感。我们 crack 多了, 也会有这方面的体会, 拿一个软件跟踪, 到关键点时凭感觉就能找到。

“耐心”就不多说了, 成功与失败的关键也在这一步。

“运气”也很重要! 破解一个程序一般都需要使用软件, 经过反复的调试和追踪, 能否用最短的时间、最少的次数破解成功, 运气的因素就体现出来了。

1.2 何谓破解

破解, 从广义上来讲, 范围很大, 包括密码破解, 系统破解, 软件破解……我们在这里所谈及的破解则以软件破解为主。而破解作为一门高深技术来讲, 又是怎样一步步成长起来的? 最早的时候, 它们首先被软件盗版组织应用, 但是当时他们并不以盈利为目的。而在 DOS 时代, 由于没有现在这么多的共享软体, 当时的软件要么是正式版, 要么是功能不全的 DEMO 版, 中看不中用。所以 DOS 时代的破解, 都是给你一些 0-9、A-Z 的字符, 然后用 PCtools 改成机器码, 来把程式中的限制关掉, 或是跳过原版磁片检查。到了 Win95 年代, 出现了大量的共享软件, 采用了注册码保护, 但由于开发者都使用 MessageBoxA 等 API 函数, 这时的破解, 基本上就是给一个用户, 一



个口令。发展到 Win98、Win2000 时代,加密技术和开发者的成熟,软盘加密、卡加密、软件锁加密、光盘加密、密码表加密、序列号加密、许可证加密的大量应用,破解已经不是那么简单。破解者需要精通汇编,学会静态反汇编,动态跟踪分析技术,因此需要学会使用调试工具、反汇编工具、脱壳工具等等。因此这时的破解已经含有很高的技术含量,不仅仅是对序列号的破解、时间限制的解除……更具意义的应该是对加密技术的挑战。

1.3 对立面——加密

加密一词来源已久。自从人们希望对自己私人的信息得到保护开始,就有了加密这个概念。软件行业的加密是软件厂商为了保护软件的利润而采取的一种软件保护方式,加密的好坏直接影响到软件的销售。从 AppleII 的年代开始,加密与解密的斗争就一直没有停止过。时至今日,软件加密的方案已经多种多样,在这里我将介绍一下各种加密方案的特点和优劣,当然这只是一家之言,持不同观点者可一笑置之。当前软件加密方法多种多样,已经不可能找出一种分类方法来把各种加密方案很好地区分开来,基本上来说可以分为依赖特定硬件的加密方案和不依赖硬件的加密方案。

1.3.1 首先说说依赖硬件的加密方案

1. 软盘加密

这是在计算机上最为古老的一种加密方案,它的原理是在软盘的特殊位置写入一些信息,软件在运行时要检验这些信息。这种软盘就好像一把钥匙。软件开发商只需一次投资购买一套加密工具就可以自己制作多张钥匙盘。此方法加密简单,成本低,在软件发展的不同时期都能看到其闪光点,像中文之星 2.97 还在延用这种方式。但用户在执行软件时必须插入此软盘,因为软驱是慢速设备,多次检查软盘上的加密点会大大拖慢程序的运行速度,所以一般加密软件只在软件运行开始的时候检查一次,这样不能避免用户用一张加密盘启动多份软件。而且由于软盘是一种易损载体,加密软件对软盘加密点的反复读写很容易造成软盘的损坏;而这张加密盘又不能备份,软件公司要不断应付用户更换加密盘的请求。另外,由于这种加密技术出现的较早,硬解密的技术相对比较成熟,像双星公司的 King - Copy 软件能拷贝大多数的加密软盘,连加密点一起复制,复制后的软盘还是加密的。

2. 卡加密

在 90 年代初,各种各样的汉卡涌现出来,而随之而来的卡加密技术也开始风行。卡加密的好处是:由于加密卡上面不仅仅可以存放数据,还可以用硬件实现简单的算法,而且在软件的执行过程中可以随时访问加密卡,不会对软件运行的速度带来太多的影响。由于加密卡是与计算机的总线交换数据,数据通讯协议完全由卡的厂家制定,没有统一的标准接口,让软件解密者有无从下手的感觉。像北大方正早期的印刷软件都是采用这种方法来加密的。但这种加密方案需要打开计算机的机箱,占用扩展槽,一般还需要专门的人员来安装。另外,由于加密卡设计上的某些问题



,还很容易同现有的硬件发生冲突。考虑到成本,加密卡必须要批量生产,厂商一般不会对低价值的软件一下投入这么大的资金。由于种种问题,这种加密技术现在已经难得一见了。

3. 软件锁加密

软件锁加密是在国外首先出现的,它是一个插在计算机打印口上火柴盒大小的设备,国内俗称为加密狗。在加密锁内部存有一定的数据和算法,计算机可以与之通讯来获得其中的数据,或通过加密锁进行某种计算。软件无法离开加密锁而运行。由于它不像卡加密那样需要打开计算机的机箱来安装,但又像加密卡那样可以随时访问,而且访问速度很快,所以一推出就受到软件开发者的青睐,很快成为当今世界上主流的加密方案。目前,所有的加密锁都提供了可编程的接口。用户可以控制加密锁中的内容,在程序中通过加密锁的接口任意访问加密锁。国外加密锁一般仅提供若干种算法,但好的加密锁不但可以向客户提供加密算法,也容许客户根据自己的意愿自定义加密算法,容许客户自定义用户 ID 号……比如:北京飞天诚信科技公司推出的 ROCKEY-IV 锁就是一种加密强度很高的产品。但加密锁也是有一定缺欠的,由于加密锁利用的是计算机的打印口,而打印口原来是为打印机而设计的,软件锁一方面要保证用户加密操作的正确,同时也要保证打印机工作的正常。但由于打印机驱动程序设计上千差万别,没有任何一家的加密锁能够完全做到这一点。但这一问题随着技术的进步有希望得到彻底的解决,那就是 USB 接口的加密锁。USB 是 Microsoft、Intel、Compaq、NEC 联合开发的一种全新的硬件接口标准,能够同时支持 128 个不同的外部设备,而且互相之间没有冲突。在新的 PII 计算机主版上大多都可以看见两个小小的长方形接口,那就是 USB 接口。USB 接口的加密锁不但拥有并口加密锁的所有优点,而且没有打印上的问题,其前景十分看好。但美中不足的是只有 Windows 98 和 Windows 2000 目前能够支持 USB 设备。在国内市场上,有几种国外 USB 加密锁,但售价很高。北京飞天诚信科技公司推出的一款 ROCKEY-USB 加密锁是国内目前惟一的民族品牌,其安全性优于国外产品的同时,售价还不足 100 元,仅是国外产品的一半。

4. 光盘加密

随着光盘的普及,光盘几乎成了软盘的替代产品。即然有软盘加密成功在先,为什么不能有光盘加密呢?有很多人在思考这个问题。但实际操作上确实是有一些问题的,因为光盘有 ISO 9660 标准协议规定,其可控制性比软盘还要严格,想找出一种只能运行而不能复制的方式确实很困难。但现在确实已经有几家这样的产品出来了,而且加密方法也不尽相同。其主要原理是利用特殊的光盘母盘上的某些特征信息是不可再现的,这些特征信息大多是光盘上非数据性的内容,光盘复制的时候复制不到的地方。因为投入是一次性的,对于大规模的生产这种加密方案可以将成本降得很低。而且软件数据和加密在同一载体上,对用户无疑是很方便的。但这是一种较新的加密方案,很多方面还需进一步验证。由于加密方式所限,不可能在用户自己刻录的光盘上实现这种加密,必须是生产线上生产的光盘才能够实现。这对于一些小规模的软件生产厂商还是有一定困难的,而且由于光盘的只读性,一旦加密有错是无法修复的。

1.3.2 再谈谈不依赖硬件的加密方案

所有的带有附加硬件设备的加密方案都有一定的加密成本在里面,对于那些价格高昂的软



件当然无所谓,但对于那些共享软件或价格本身就就很低的软件来说,硬件加密成本可能比软件本身的售价还高,当然不会被考虑了。但不加密,往往就变成了免费软件,所以近年来产生了很多软加密方案。

1. 密码表加密

在软件运行的开始要求用户根据屏幕的提示信息输入特定的答案,答案往往在用户手册上的一份防复印的密码表中。用户只有正确输入密码后才能够继续运行。这种加密方案实现简单,不需要太多的成本,但用户每次运行软件都要查找密码,使用户感到十分的不便。像台湾的游戏大多采用此加密方式。而且往往有一些有耐心者把整个密码表输入到计算机中存成一个文件,同软件的盗版一同公布出来,让加密者无可奈何。基本上是一种防君子不防小人的加密方式。

2. 序列号加密

这种加密方式从某种角度来讲不是一套完整的加密方案。现今很多 Shareware(共享软件)大多采用这种加密方式,用户在软件的试用期是不需要交费的,一旦试用期满还希望继续试用这个软件,就必须到软件公司进行注册,然后软件公司会根据你提交的信息(一般是用户的名字)来生成一个序列号。当你收到这个序列号以后,并在软件运行的时候输入进去,软件会验证你的名字与序列号之间的关系是否正确,如果正确说明你已经购买了这款软件,也就没有日期的限制了。这种加密方案实现简单,而且购买过程也完全在 Internet 上实现,无论是开发者和购买者都觉得很方便。不过有心的人可能已经注意到软件的名字与序列号之间的验证是在你的计算机上完成的,很多黑客利用这个漏洞找出了名字和序列号之间的换算关系,编写出一种叫 KeyMaker 的程序,你只要输入你的名字,这个程序会帮助你计算出序列号,你再用你的名字和这个序列号输入进软件中就变成正版软件了。目前还没有什么更好的方法来阻止用户扩散他注册后得到的序列号。

3. 许可证加密

这种方式在某种角度上说可以是序列号加密的一个变种。你从网上下载的或购买过来的软件并不能直接使用,软件在安装时或运行时会对你的计算机进行一番检测,并根据检测结果生成一个你的计算机的特定指纹,这个指纹可以是一个小文件,也可以是一串谁也看不懂的数,你需要把这个指纹数据通过 Internet、Email、电话、传真等方式发送到开发商那里,开发商再根据这个指纹给你一个注册码或注册文件,你得到这个注册码或注册文件并按软件要求的步骤,在你的计算机上完成注册后方能使用。这个方法的买卖也是完全通过网络来进行的,而且用户购买的软件被限制了只能在他自己的计算机上面运行,换到其他的计算机上,这个注册码或注册文件可能不再有效。但用户更换某些硬件设备也可能造成注册码的失效,而且用户得到软件后在完成注册工作前会有一段时间无法使用。对于软件开发商来说服务与管理的工作量无疑也是非常巨大的。网络上有个 ZIP Download 公司专门替软件开发商来完成这种加密与服务工作。将来 PIII 处理器内部有了特定的序列号,将会减少这种加密方案的硬件依赖性,但估计普及起来还有很长的一段时间。



1.4 散布世界各地的破解组织

最早的破解组织在 20 世纪 70 年代末 80 年代初就已经出现了。这是在国外诞生的一种奇怪的自发性民间组织。它的成员是一些青少年电脑爱好者。他们是运用自己的技术破解各类机种中运行]的软件(包括个人电脑和电视游戏机),以非法方式传播,但不以赢利为目的的纯技术团伙。在早期没有互联网的情况下,他们用电话线传输游戏以及一些自制运行的展示程序(DEMO),并展开不定期的技术交流,同一地区之间还经常性地交换成员,这些组织遍布在南、北美洲、欧洲和南非等地。

20 世纪 90 年代,PC 机在全球的普及和互联网日益发展,为这些组织的成长壮大创造了良好的土壤。这个组织是无形的,他们有自己的信念和约定俗成的行规,他们没有自己的网站,不赚钱,破解的游戏只用 FTP 上传以供下载,并通过 BBS 交流信息。其组织成员很有奉献精神,以自己是“WAREZ”或“O DAY”组织成员为荣。在美国的一些大学中,如果一个学生是“O DAY”成员,他的计算机教师甚至会考虑在他的成绩中加分——因为加入此种破解组织意味着你在技术上的优秀。这些组织早期的首脑有的现已成为律师、医生和政府官员等社会中坚力量。

这里我们要解释一下“WAREZ”的含义,它是国外从事软件破解者的统称。“WARE”表示破解软件,“Z”表示零(ZERO),意为在不到一天的时间里破解软件。那么“O DAY”的意思也就不言而喻了。下面我们再介绍一下这类组织破解正版软件的流程。首先是提供组负责购买游戏或取得资料,然后是解密组织负责将软件解密。这个组的成员往往是最多的,也是技术含量最高的。再往后是包装组。在这里光盘破解组织和硬盘破解组织的“行规”是不同的。硬盘版要求 2.8 乘 65,即不能超过 65 个压缩包,每个压缩包的大小不能超过 2.8 兆,他们认为超过这个标准就不能算硬盘版,对下载者就是一种欺骗。光盘版则没有这种限制,15 兆一个 ISO 光盘换像包,使用者全部下载后再将其解压刻录于光盘,就可以玩完整的光盘游戏。具体压缩一般的规矩是这样:一个 ISO 包内含一个 ZIP 包。ZIP 包内含的多媒体文件再用 ACE 压缩。这样保证了 1:12 的压缩率,便于网上传播——以上所说的完全是一种对玩家利益的考虑。最后是发行组,负责在 FTP 上上传破解后的游戏软件。

这些组织破解的游戏通常放在国外地下站点,通过 FTP 下载时需要验证你的 IP,看是否是它的成员,而且 IP 通过检验进入 FTP 后你会看到欢迎词,以及“本站是 XX 组织北美第 XX 发行站”之类的字样。它还将告诉你今天有哪些游戏上传,昨天有哪些游戏上传、你上传过多少游戏,下载过多少游戏,制作过多少有趣的 DEMO 程序。如果你长期没有破解游戏上传记录,将取消你的 IP 记录。各种组织没有自己专门的 FTP 下载基地,你可以自愿提供资源,当然站长也可以加入到各类组织中去。无论是组织成员还是站长,凡是自愿加入这种组织的,都具有相当的责任心,当某一成员破解上传的游戏在其他的站上被别人抢先破解上传过了,那么你破解的将被 CANCEL。而如果他做的硬盘版没有你的完美,那么他也将自动 CANCEL 掉自己的那个版本。这个规则保证了优胜劣汰,保证了所有破解软件只有一个版本,但它肯定是最完美的。

各大组织的外围成员来自世界各地,只要他们愿意,而且技术上能做得到,就可以同时加入



几个盗版组织。而当你从学校毕业有了一份正当的职业后,再没有精力做这种义务劳动,那么你将自动从组织中淡出。

由此可见,这种组织从加入到管理到退出完全依赖一种自我完善的机制。它是松散的,同时又非常合理。但由于它的开放性,有时也会出现某方面人员的匮乏。如果你用写字板打开破解软件中的 NFO 文件,很可能看到“我们目前缺乏解密组和提供组人员,诚邀有志者加盟”等字样。

除去这种非法的破解游戏传播工作,“0 DAY”组织成员还热衷于制作一种自动播放的有动画、有音乐的小 DEMO 程序。他们通过它来宣传自己的组织,炫耀自己的技术,有时还通过这种小程序来攻击竞争对手——这招实在算不得文明。这种程序字节数越小、播放时间越长就越好,在这方面创记录的是 CLASS 组成员的一个程序,它只有 27K。在 PC 机硬盘版游戏解压缩的执行文件也是破解组织比拼技术的一种方式。英国的老牌组织 MYTH 的安装界面甚至提供俄罗斯方块游戏,用以打发你在安装游戏时等待的时光。

目前国际知名的 PC 游戏软件盗版组织中专门破解制作光盘版的有 RAZOR 1911、FAIRLIGHT 和 DEVIANCE,专门制作硬盘版的有 CLASS、MYTH 和 DD。应用软件盗版组织中 CORE、FOREST、ING 和 PARADIGM 是最有名的。其中 FOREST 专门破解图形软件。目前世界上所有流通的破解图形软件几乎都是由这个组织破解的。RAZOR1911 组织从 1985 年至今在 Commodore 64、Amiga 和 PC 机上的经历(C64 和 Amiga 都是 80 年代的 4 位/8 位游戏机),决定了它是此类组织发展历程中最具代表性的一个。1985 年 10 月一个雨后的傍晚,3 个年轻的挪威计算机爱好者决定成立一个计算机小组,破解 Commodore 64 机种的游戏软件。他们并不很清楚成立一个小组都需要些什么,但他们从 1941、Sectuion 8、Jedi 2001、Hellmates、SCC 等著名的软件破解小组那里得到了很多灵感。

好的组织要有个好名字,一个朋友为他们起名叫 RAZOR2992。他们不喜欢这个名字,不久就改名为 RAZOR1911。许多人问他们为什么用这个名字,他们就回答说因为在 PC64 游戏机被破解组织中,有太多没脑子的孩子用类似 666 这种号码在他们的 DEMO、信笺和盘盒上,他们觉得这很幼稚,他们需要神秘感。1911 年在 16 进制算法中可转化为 777,是对 666 的一种讽刺。后来他们也曾用 Project\$777 的名字制作 Amiga 游戏机的 DEMO。

C64 时代很短暂,他们做了许多 DEMO 和一些软件破解,成为挪威有名的小组之一。他们的名作不多,其中一些至今还在 Commodore 64 纪念光盘里流通(C64 可在 MS-DOS 和 UNIX 系统中模拟运行)。后来该小组一些成员分裂出去,进入 TCC 和 Megaforce。其余的人决定加入 Active Cracking Crew(ACC)组织。在那里他们学会如何像一个专业的软件破解者那样工作,并第一次把视线投向了整个世界。他们为自己广泛宣传,6 个月后又参加了在丹麦举办的被称为“顶级精英”者的国际聚会,这种聚会的另一种称谓是“拷贝团拜”(COPY-PARTIES)。他们在会上评选出 1987 年年度最佳解密高手。TRIAD 小组的 Mr. Z 以微弱票数险胜 Raw Deal 的 Laffen,获得了“年度最佳解密高手”的称号。当时 FAIRLIGHT 还和 ACC 现场合作破解了一个詹姆士·邦德的 007 游戏。从丹麦回到挪威,兴奋的年轻人重组了 RAZOR1911,在 AMIGA 机种上和 RAW DEAL 合作,东山再起。

在 AMIGA 上的发展开始非常缓慢,1988 年才开始陆续做出一些 DEMO,并在全球有了一些成员。当时的许多 DEMO 相当原始,但是有好的想法,好的图象和动听的音乐,后来它们大部分



都遗失了。不象许多新成员所想象的那样,RAZOR1911的老成员们都明白他们真正希望成为的是一个最好的游戏破解组织,而不仅是一个 DEMO 制作组。当他们在 DEMO 制作上有了些名气后时常与许多专门的游戏软件破解组织联系,1989年,当一些组织解散后,其成员都被 RAZOR 1911 吸收过去。其中 Zodact 和 Onyx 分别是美国和欧洲的主力游戏破解组织,由于这些富有经验的成员的加入,RAZOR1911 很快转型为一个真正的游戏破解组织——在后来的 PC 机时代,那时吸收的成员仍然是 RAZOR1911 最好,最有力的成员。

他们同时还掌握了大量盗用电话线路的技术,这使得他们可以将自己的联系网轻易地扩展到全世界。在 1989 年的最后两周里,他们有了两个世界第一的破解作品——Pocket Rockels 和 StriPPoker II。同时他们也受到了其他组织的恶性竞争。到了 1991 年 4 月,他们已经破解了 50 个 AMJGA 游戏软件。这之后,AMIGA 机种软件很难破解了,它的每张盘都有密码锁,你不得不一次次面对各种不同的新问题,而 NTSC/PAL 两种制式的差别使得美国人没有补丁就不能玩欧洲的游戏。而且现在有太多的小组在竞争,大家常常为破解同一个游戏而暗中比赛,压力变大了,这时的整个社会经济都处于疲软状态,许多组织没有足够的钱支持下去。

对未来,RAZOR 的创建者没有足够明确的方向。但这时一个富有才华的 PC 软件破解者 Danwin 将 PC 机带入了他们的视线。RAZOR 很快关闭了 AMIGA 专线,他们彻底地重组了组织,包括匿名的投资者和 Doctor、NO、Onyx、Zodact 等一批过去的精英。他们合作破解了一大批电脑游戏软件,在业内口碑甚好。他们由紧凑、精干、高效率的小组很快变成了一个庞大无形的游戏破解机构。RAZOR 变成了一个大公司式的玩意儿,他们不断地破解游戏、制作修改器、提取游戏动画……4 年内他们几乎破解了 600 个游戏和无数的其他产品。

1995 年后,国际互联网有了长足发展,RAZOR 组织充分利用它并有了更广阔的发布渠道,他们比以前任何时候都更快更多地接触到饥渴的人群。这一年他们还插足 CD-ROM 领域。开始只是以 RAZOR1911 的名义零星地破解一些光盘版游戏。他们一开始没有过多关注这个领域,直到软盘游戏越来越少,他们也真正重视起光盘游戏并取得了这个领域的主导地位。目前他们仍然是全球最大的 PC 光盘游戏盗版组织并深受一些年轻人的崇拜,他们同样着迷于对游戏破解技术的攻坚,并喜欢穿着印有 RAZOR1911 标志的外套招摇过市。

作为一个如此庞大的组织,他们也存在着这样那样的问题。他们在 1994 和 1995 年有过两次大分裂,甚至有些人被警方逮捕和备案。但他们还是渡过了难关,继续发展着。关于这些盗版组织更详细的历史材料都在他们这些年来破解的 PC 游戏所附的 .nfo 文件中,你从中可以了解到他们许多被遗忘的秘密。



第二章 破解之本

想在破解方面有一定发展的人,最好是买一本汇编书来学习。现在计算机专业毕业的学生,汇编都学过,一网友说学过汇编,是 8088 等,说太老了用不上。现在我告诉大家,足够了,目前硬件都兼容 X86 系统,明白吗?再多复杂的程序,最终都需 X86 指令执行,你就可以跟踪它,看到的都是汇编代码。所以并不需多高的水平,只要能看得懂就行了,买来的汇编书只要看看前两章就可以了,了解各种指令的含义,了解寄存器,还有数据在内存存储顺序,堆栈等概念。但你如想有所作为,还是在汇编上花点时间吧。另外,各种破解工具一定要熟练运用,比如“SOFTICE”、“TRW 2000”、“W32DASM”等等,本书中都会有详细教程。

2.1 汇编语言基础

系统的讲解汇编语言是办不到了,但基础知识和与破解相关的内容还是要提一下的,基础部分我抓了本大学时的教科书节选了一下,相关破解则是高手发布在网上的文章。

2.1.1 寄存器

任何程序的执行归根结底都是存放在存储器里的指令系列执行的结果,寄存器用来存放程序运行中的各种信息,包括操作数地址、操作数及运算的中间结果等。下面我们来熟悉一下 8086/8088 的寄存器。

1. 数据存储器

包括 AX、BX、CX、DX4 个通用寄存器,用来暂时存放计算过程中所用到的操作数、结果或其他信息。

· AX(Accumulator)作为累加器用,所以它是算术运算的主要寄存器。

BX(Base)可以作为通用寄存器使用,此外在计算存储器地址时,它经常用作基址寄存器。

CX(count)可以作为通用寄存器使用,此外在循环(L000)和串处理指令中用作隐含的计数器。

DX(Data)可以作为通用寄存器使用。一般在作双字长运算时把 DX 和 AX 组合在一起存放一个双字长数,DX 用来存放高位率。

2. 指针及变址寄存器



包括 SP、BP、SI、DI 四个 16 位寄存器。

SP(Stack Pointer)称为堆栈指针寄存器,用来指示栈顶的偏移地址。

BP(Base Pointer)称为基址指针寄存器,它们都可以与 SS 寄存器联用来确定堆栈段中的某一存储单元的地址。可作为堆栈区中的一个基地址以便访问堆栈中的其他信息。

SI(Source Index)源变址寄存器和 DI(Destination Index)目的变址寄存器一般与 DS 联用,用来确定数据段中某一存储单元的地址。

3. 段寄存器

包括 CS、DS、SS 和 ES4 个段寄存器。其中 SS 寄存器和 SP、BP 寄存器联用来确定堆栈段中的某一存储单元的地址, DS 寄存器和 SI、DI 寄存器联用来确定数据段中的某一存储单元的地址。

4. 控制寄存器

包括 IP 和 PSW 两个 16 位寄存器。

IP(Instruction Pointer)为指令指针寄存器,它用来存放代码段中的偏移地址。

PSW(Program Flag)程序状态字寄存器,是一个 16 位寄存器,由条件码标志(flag)和控制标志构成,如下所示:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
			OF	DF	IF	TF	SF	ZF		AF		PF			CF

条件码:

- ① OF(Overflow Flag)溢出标志。溢出时为 1,否则置 0。
- ② SF(Sign Flag)符号标志。结果为负时置 1,否则置 0。
- ③ ZF(Zero Flag)零标志,运算结果为 0 时 ZF 位置 1,否则置 0。
- ④ CF(Carry Flag)进位标志,进位时置 1,否则置 0。
- ⑤ AF(Auxiliary carry Flag)辅助进位标志,记录运算时第 3 位(半个字节)产生的进位置。有进位时 1,否则置 0。

- ⑥ PF(Parity Flag)奇偶标志。结果操作数中 1 的个数为偶数时置 1,否则置 0。

控制标志位:

- ⑦ DF(Direction Flag)方向标志,在串处理指令中控制信息的方向。
- ⑧ IF(Interrupt Flag)中断标志。
- ⑨ TF(Trap Flag)陷阱标志。

以上讲的都是 8 位和 16 位的寄存器,32 位的区别不大。下面简单介绍一下。

通用寄存器

AH/AL AX (EAX) 累加器

BH/BL BX (EBX) 基址

CH/CL CX (ECX) 计数器

DH/DL DX (EDX) 数据



(FS) 386 新增的段寄存器

(E_{xx}) 为 386 新增的 32 位寄存器(GS)386 新增的段寄存器

段寄存器和 8、16 位的寄存器相同。

指针寄存器

SI (ESI) 源索引指针 SP (ESP) 栈指针

DI (EDI) 目的索引指针 BP (EBP) 基址指针

IP 指令指针

首先必须强调的是,在用 32 位汇编语言编程的时候,所有的地址偏移量都是 32 位的,在寻址时千万不要还用原来的 16 位方式。

基址寄存器默认的段寄存器

BP or SP SS

SI or DI DS

DI strings ES

SI strings DS

2.1.2 寻址方式

我们知道程序最终是通过执行指令序列来解决问题的,而指令必须对操作数地址进行寻址,采用什么样的寻址方式会对程序运行的速率和效率造成影响。什么?跑题了!别急,下面就言归正传。

1. 立即寻址方式

操作数直接放在指令中,作为指令的一部分存放在代码段里,也称立即数寻址。例 `MOVAL,5`

2. 寄存器寻址方式

操作数在寄存器中,指令指定寄存器号。例 `MOV AX,BX`

3. 直接寻址方式

汇编中把操作数的偏移地址成为有效地址 EA,直接寻址方式时,EA 就作为指令的一部分。
例 `MOV AX,[2000]`

4. 寄存器间接寻址方式

操作数的有效地址在基址寄存器 BX,BP 或变址寄存器 SI,DI 中,而操作数则在存储器中。
例 `MOV AX,[BX]`

5. 直接变址寻址方式

操作数的有效地址是一个基址或变址寄存器的内容和指令中指定的位移量之和。例 `MOV AX,COUNT[SI]`

6. 基址变址寻址方式

操作数的有效地址是一个基址寄存器和一个变址寄存器的内容之和,两个寄存器均由指令



指定。例 MOV AX,[BX][DI]

下面的寻址方式和转移地址有关,用来确定转移指令及 CALL 指令的转向地址。

7. 段内直接寻址

转向的有效地址是当前 IP 寄存器的内容和指令中指定的位移量之和。例 JMP PTR PROGIA

8. 段内间接寻址

转向有效地址是一个寄存器或是一个寄存单元的内容。单元的内容可用数据寻址中除立即数之外的任何一种寻址方式获得。例假设:(DS) = 2000H (BX) = 1256H (SI) = 528H 位移量 = 20AH (232F7H) = 3280H (263E5H) = 2450H

JMP BX 执行该指令后(IP) = 1256H

JMP[BX][SI]执行该指令后(IP) = 3280H

9. 段间直接寻址

指令中直接提供了转向段地址和偏移地址,要用指令中指定的偏移地址取代 IP 寄存器的内容。例 JMP FAR PTR NEXTROUTINT

10. 段间间接寻址

用存储器的两个相继字的内容来取代 IP 和 CS 寄存器的原始内容以达到段间转移的目的。例 JMP DWORD PTR[INTERS + BX]

2.1.3 汇编指令集

当我们对软件进行反汇编的时候,面对的都是——行行的汇编指令,如果你对 these 指令不熟悉,那你还是先静下心来研究下面的这些指令吧,它是你进入破解天堂的钥匙。

1. 数据传送指令集

MOV

功能:把源操作数送给目的操作数

语法:MOV 目的操作数,源操作数

格式:MOV r1,r2

MOV r,m

MOV m,r

MOV r,data

XCHG

功能:交换两个操作数的数据

语法:XCHG



格式: XCHG r1,r2 XCHG m,r XCHG r,m

PUSH,POP

功能: 把操作数压入或取出堆栈

语法: PUSH 操作数 POP 操作数

格式: PUSH r PUSH M PUSH data POP r POP m

PUSHF,POPF,PUSHA,POPA

功能: 堆栈指令群

格式: PUSHF POPF PUSHA POPA

LEA,LDS,LES

功能: 取地址至寄存器

语法: LEA r,m LDS r,m LES r,m

XLAT(XLATB)

功能: 查表指令

语法: XLAT XLAT m

2. 数运算指令

ADD,ADC

功能: 加法指令

语法: ADD OP1,OP2 ADC OP1,OP2

格式: ADD r1,r2 ADD r,m ADD m,r ADD r,data

影响标志: C,P,A,Z,S,O

SUB,SBB

功能: 减法指令

语法: SUB OP1,OP2 SBB OP1,OP2

格式: SUB r1,r2 SUB r,m SUB m,r SUB r,data SUB m,data

影响标志: C,P,A,Z,S,O

INC,DEC

功能: 把 OP 的值加一或减一

语法: INC OP DEC OP

格式: INC r/m DEC r/m

影响标志: P,A,Z,S,O

NEG

功能: 将 OP 的符号反相(取二进制补码)

语法: NEG OP

格式: NEG r/m

影响标志: C,P,A,Z,S,O

MUL,IMUL



功能：乘法指令

语法：MUL OP IMUL OP

格式：MUL r/m IMUL r/m

影响标志：C,P,A,Z,S,O(仅 IMUL 会影响 S 标志)

DIV, IDIV

功能：除法指令

语法：DIV OP IDIV OP

格式：DIV r/m IDIV r/m

CBW, CWD

功能：有符号数扩展指令

语法：CBW CWD

AAA, AAS, AAM, AAD

功能：非压缩 BCD 码运算调整指令

语法：AAA AAS AAM AAD

影响标志：A,C(AAA,AAS) S,Z,P(AAM,AAD)

DAA, DAS

功能：压缩 BCD 码调整指令

语法：DAA DAS

影响标志：C,P,A,Z,S

3. 位运算指令集

AND, OR, XOR, NOT, TEST

功能：执行 BIT 与 BIT 之间的逻辑运算

语法：AND r/m,r/m/data OR r/m,r/m/data XOR r/m,r/m/data TEST r/m,r/m/data

NOT r/m

影响标志：C,O,P,Z,S(其中 C 与 O 两个标志会被设为 0) NOT 指令不影响任何标志位

SHR, SHL, SAR, SAL

功能：移位指令

语法：SHR r/m,data/CL SHL r/m,data/CL SAR r/m,data/CL SAL r/m,data/CL

影响标志：C,P,Z,S,O

ROR, ROL, RCR, RCL

功能：循环移位指令

语法：ROR r/m,data/CL ROL r/m,data/CL RCR r/m,data/CL RCL r/m,data/CL

影响标志：C,P,Z,S,O

4. 程序流程控制指令集

CLC, STC, CMC

功能：设定进位标志

语法：CLC STC CMC



标志位: C

CLD,STD

功能: 设定方向标志

语法: CLD STD

标志位: D

CLI,STI

功能: 设定中断标志

语法: CLI STI

标志位: I

CMP

功能: 比较 OP1 与 OP2 的值

语法: CMP r/m,r/m/data

标志位: C,P,A,Z,O

JMP

功能: 跳往指定地址执行

语法: JMP 地址

JXX

功能: 当特定条件成立则跳往指定地址执行

语法: JXX 地址

注:有关跳转指令的详细内容请看第五小节。

LOOP

功能: 循环指令集

语法: LOOP 地址

LOOPE(Z)

地址 LOOPNE(Z) 地址

标志位: 无

CALL,RET

功能: 子程序调用,返回指令

语法: CALL 地址 RET RET n

标志位: 无

INT,IRET

功能: 中断调用及返回指令

语法: INT n IRET

标志位: 在执行 INT 时,CPU 会自动将标志寄存器的值入栈,在执行 IRET 时则会将堆栈中的标志值弹回寄存器

5. 字符串操作指令集



MOVSB,MOVSW,MOVSD

功能：字符串传送指令

语法：MOVSB MOVSW MOVSD

标志位：无

CMPSB,CMPSW,CMPSD

功能：字符串比较指令

语法：CMPSB CMPSW CMPSD

标志位：C,P,Z,S,O

SCASB,SCASW

功能：字符串搜索指令

语法：SCASB SCASW

标志位：C,P,Z,S,O

LODSB,LODSW,STOSB,STOSW

功能：字符串载入或存储指令

语法：LODSB LODSW STOSB STOSW

标志位：无

REP,REPE,REPNE

功能：重复前缀指令集

语法：REP 指令 S REPE 指令 S REPNE 指令 S

标志位：依指令 S 而定

2.1.4 伪操作

汇编语言的语句除了指令之外还有伪操作，伪操作又称为伪指令，它不像机器指令那样是在程序运行期间由计算机来执行的，它是在汇编程序对源程序汇编期间由汇编程序处理的操作，它可以完成如数据定义、分配存储区、指示程序结束等功能。我们这里说明一些常用的伪指令。

1. 数据定义及存储器分配伪操作

这一类伪操作的格式是：

[Variable] Mnemonic operand, ..., operand[;Comments]

其中变量(Variable)字段是可有可无的，它用符号地址表示，其作用与指令语句前的标号相同，但它的后面不跟冒号。如果语句中有变量则汇编程序使其记以第 1 个字节的偏移地址。

注释(Comments)字段用来说明该伪操作的功能，它也是可有可无的。

助记符(Mnemonic)字段说明所用伪操作的助记符，常用的有以下几种：

DB 伪操作用来定义字节，其后的每个操作数都占有 1 个字节。

DW 伪操作用来定义字，其后的每个操作数占有 1 个字(低位字节在第一个字节地址中，高位字节在第二个字节地址中)。

DD 伪操作用来定义双字，其后的每个操作数占有 2 个字。



DQ 伪操作用来定义 4 个字,其后的每个操作数占有 4 个字。

DT 伪操作用来定义 10 个字节,其后的每个操作数占有 11 个字节,形成压缩的 BCD 码。

2. 表达式赋值伪操作 EQU

有时程序中多次出现同一个表达式,为方便起见可以用赋值伪操作给表达式赋予一个名字。其格式如下:EXpttgsion_name EQU Expression

此后,程序中凡需要用到该表达式之处就可以用表达式名来代替了。上式中的表达式可以是任何有效的操作数格式,可以是任何可以求出常数值值的表达式,也可以是任何有效的助记符。

例

CONSTANTEQU256 数赋以符号名

DATAEQUHEIGHT + 12 地址表达式赋以符号名

ALPHAEQU7 这三条语句是一组赋值伪操作,把

BETAEQUALPHA - 27 - 2 = 5 赋以 BETA, VAR + 5 赋以

ADDREQUVAR + BETAADDR

必须注意 EQU 语句的表达式中如果有变量或标号的表达式,则在该语句前应该先给出它们的定义。例如,语句

AB EQU DATAONE + 2

则必须放在 DATA - ONE 的定义之后才行,否则汇编程序将指示出错。

另外还有一个与 EQU 相类似的 = 伪操作也可以作为赋值伪操作使用。它们之间的区别是 EQU 伪操作中的表达式名是不允许重复定义的,而 = 伪操作则允许重复定义。

3. 段定义伪操作

存储器的物理地址是由段地址和偏移地址组合而成的,汇编程序在把源程序转换为目标程序时,必须确定标号和变量的偏移地址,并且需要把有关信息通过目标模块传送给连接程序,以便连接程序把不同的段和模块连接在一起形成一个可执行程序。为此,需要用段定义伪操作,段定义伪操作的格式如下:

```
segment name SEGMENT
```

```
segment nameENDS
```

其中删节号部分,对于数据段、附加段和堆栈段来说,一般是存储单元的定义、分配等伪操作;对于代码段则是指令及伪操作。

4. 程序开始和结束伪操作

在程序的开始可以用 NAME 或 TITLE 为模块取名字,NAME 的格式是:

```
NAMEModule_name
```

汇编程序将以给出的 module_name 作为模块的名字。如果程序中没有 NAME 伪操作,则也可使用 TITLE 伪操作,其格式为:

```
TITLE text
```

TITLE 伪操作可指定每 1 页上打印的标题。



5. 对准伪操作

· EVEN 伪操作使下一个字节地址成为偶数。一个字的地址最好从偶地址开始, 所以对于字数组, 为保证其从偶地址开始, 可以在它前面用 EVEN 伪操作来达到这一目的。

6. 基数控制伪操作

汇编语言默认的数为十进制数, 因而除非专门指定, 汇编把程序中出现的数均看作十进制数, 当要用基数表示的常数时, 就需要专门的标记。

. RADIX 可以把默认的基数改变为 2 ~ 16 范围内的任何基数。格式 . RADIXexpression
其中表达式用来表示基数值(用十进制表示)

例 MOV BX, 0FFH

MOV BX, 178

与

. RADIX 16

MOV BX, 0FF

MOV BX, 178D

是等价的。

2.1.5 跳转指令小结

1. 直接标志转移

指令格式	机器码	测试条件	如...则转移	指令格式	机器码	测试条件	如...则转移
JC	72	C = 1	有进位	JNS	79	S = 0	正号
JNC	73	C = 0	无进位	JO	70	O = 1	有溢出
JZ/JE	74	Z = 1	零/等于	JNO	71	O = 0	无溢出
JNZ/JNE	75	Z = 0	不为零/不等于	JP/JPE	7A	P = 1	奇偶位为偶
JS	78	S = 1	负号	JNP/IPO	7B	P = 0	奇偶位为奇

2. 间接标志转移

指令格式	机器码	测试格式	如...则转移
JA/JNBE(比较无符号数)	77	C 或 Z = 0	> 高于/不低于或等于
JAE/JNB(比较无符号数)	73	C = 0	>= 高于或等于/不低于
JB/JNAE(比较无符号数)	72	C = 1	< 低于/不高于或等于
JBE/JNA(比较无符号数)	76	C 或 Z = 1	<= 低于或等于/不高于
JG/JNLE(比较带符号数)	7F	(S 异或 O) 或 Z = 0	> 大于/不小于或等于
JGE/JNL(比较带符号数)	7D	S 异或 O = 0	>= 大于或等于/不小于
JL/JNGE(比较带符号数)	7C	S 异或 O = 1	< 小于/不大于或等于
JLE/JNG(比较带符号数)	7E	(S 异或 O) 或 Z = 1	<= 小于或等于/不大于



3. 无条件转移指令 JMP

指令格式	执行操作	机器码	说明
段内直接短转移 <code>Jmp short</code>	$(IP) \leftarrow (IP) + 8 \text{ 位位移量}$	EB	转移范围 -128 到 +127 字节
段内直接近转移 <code>Jmp near</code>	$(IP) \leftarrow (IP) + 16 \text{ 位位移量}$	E9	转移到段内的任一位置
段内间接转移 <code>Jmp word</code>	$(IP) \leftarrow (\text{有效地址 EA})$	FF	
段间直接(远)转移 <code>Jmp far</code>	$(IP) \leftarrow (\text{偏移地址})$ $(CS) \leftarrow (\text{段地址})$	EA	
段间间接转移 <code>Jmp dword</code>	$(IP) \leftarrow (EA)$ $(CS) \leftarrow (EA + 2)$		

到此为止,该了解的基础知识我们差不多都已经全部提到了,很简单不是?剩下的就是该你自己去多多找破解工具、软件实践了。只有这样,你才能不断积累宝贵的经验,成为一个真正的 Cracker。

2.2 软件分析跟踪技术

在进行软件的破解、解密以及计算机病毒分析工作中,一个首要的问题是对软件及病毒进行分析。软件的根本都是机器代码程序,对于它们分析必须使用静态或动态调试工具,分析跟踪其汇编代码。

1. 从软件使用说明和操作中分析软件

欲破解一软件,首先应该先用用这软件,了解一下功能是否有限制,阅读一下软件的说明书或手册,特别是自己所关心的关键部分的使用说明,这样也许能够找点线索。

2. 静态反汇编

所谓静态分析就是从反汇编出来的程序清单上分析。从提示信息入手进行分析。目前,大多数软件在设计时,都采用了人机对话方式。所谓人机对话,即在软件运行过程中,需要由用户选择的地方,软件即显示相应的提示信息,并等待用户按键选择。而在执行完某一段程序之后,便显示一串提示信息,以反映该段程序运行后的状态,是正常运行,还是出现错误,或者提示用户进行下一步工作的帮助信息。为此,如果我们对静态反汇编出来的程序清单进行阅读,可了解软件的编程思路,以便顺利破解。常用的静态分析工具是“W32DASM”、“IDA”和“HIEW”等。

3. 动态跟踪分析

虽然从静态上可以了解程序的思路,但是并不可能真正详细了解软件的细节,这时就要运用到动态分析程序。另外,碰到压缩程序,静态分析也无能为力了,只能动态分析了。所谓动态分析是利用“SOFTICE”或“TRW2000”一步一步地单步执行软件。为什么要对软件进行动态分析呢?这主要是因为:



(1)许多软件在整体上完成的功能,一般要分解成若干模块来完成,而且后一模块在执行时,往往需要使用其前一模块处理的结果,这一结果我们把它叫中间结果。如果我们只对软件本身进行静态地分析,一般是很难分析出这些中间结果的。而只有通过跟踪执行前一模块,才能看到这些结果。另外,在程序的运行过程中,往往会在某一地方出现许多分支和转移,不同的分支和转移往往需要不同的条件,而这些条件一般是由运行该分支之前的程序来产生的。如果想知道程序运行到该分支的地方时,到底走向哪一支,不进行动态跟踪和分析是不行的。

(2)有许多软件在运行时,其最初执行的一段程序往往需要对该软件的后面各个模块进行一些初始化工作,而没有依赖系统的重定位。

(3)有许多加密程序为了阻止非法跟踪和阅读,对执行代码的大部分内容进行了加密变换,而只有很短的一段程序是明文。加密程序运行时,采用了逐块解密,逐块执行的方法。首先运行最初的一段明文程序,该程序在运行过程中,不仅要完成阻止跟踪的任务,而且还要负责对下一块密码进行解密。显然仅对该软件的密码部分进行反汇编,不对该软件动态跟踪分析,是根本不可能进行解密的。

由于上述原因,在对软件静态分析不行的条件下,就要进行动态分析了。那么如何有效地进行动态跟踪分析呢?一般来说有如下几点:

(1)对软件进行粗跟踪

所谓粗跟踪,即在跟踪时要大块大块地跟踪,也就是说每次遇到调用 CALL 指令、重复操作指令 REP、循环操作 LOOP 指令以及中断调用 INT 指令等,一般不要跟踪进去,而是根据执行结果分析该段程序的功能。

(2)对关键部分进行细跟踪

对软件进行了一定程度的粗跟踪之后,便可以获取软件中我们所关心的模块或程序段,这样就可以有针对性地对模块进行具体而详细的跟踪分析。

一般情况下,对关键代码的跟踪可能要反复进行若干次才能读懂该程序,每次要把比较关键的中间结果或指令地址记录下来,这样会对下一次分析有很大的帮助。软件分析是一种比较复杂和艰苦的工作,上面的几点分析方法,只是提供了一种基本的分析方法。要积累软件分析的经验需要在实践中不断地探索和总结。

2.3 常用工具介绍

破解离不开工具,合适的工具使你事半功倍,这里主要是简单介绍几种破解工具,而详细的用法,本书后面章节有详解。

(1)SoftICE(动态跟踪工具)

(2)Trw2000(动态跟踪工具)

(3)Wdasm8.93、Hiew、IDA(反汇编工具)

(4)Smartcheck(Visual Basic 程序调试工具)

(5)Ultraedit、WinHex、Hex Workshop 等(十六进制编辑器)



- (6) RegShot、regmon 或 RegSnap(注册表监视工具)
- (7) TYP、gtw 或 FileInfo 等(侦测文件类型工具)
- (8) PROCDUMP(脱壳工具)
- (9) IceDump(调试工具)
- (10) Crackcode2000(注册机制作)
- (11) ERU(备份 Windows 配制文件工具)
- (12) Filemon(文件监视工具)
- (13) EXESCOPE(资源修改器)
- (14) Frogsice

一看这么多是不是吓坏了?其实你只需掌握一两种就能破解软件,当然要得心应手,最好还是全面掌握,因为现在软件什么手段都有可能采用。

1. Soft-ICE: 是目前公认最好的跟踪调试工具。使用 Soft-ICE 可以很容易地跟踪一个软件,或是监视软件产生的错误进行除错。你甚至可以用它来替代 C 语言的调试器——如果你不喜欢使用 C 语言自己的调试器的话。注意其有几种平台的版本, DOS, Windows 3.1, Win95/98/2000/NT, 所以别搞错了。

2. Trw2000: 国人自己编写的调试软件,完全兼容 SoftICE 各种指令。

3. Wdasm8.93: 反汇编的极品工具。可方便反汇编程序,它能静态分析程序流程,也可动态分析程序,操作简单,破解必备!

4. Hiew: 不用多说,是一个十六进制工具,它除了普通十六进制的功能外,它还有个特色,能反汇编文件,并可以汇编指令修改程序。是不是够酷的?

5. IDA: 强大的反汇编工具。

6. Smartcheck: VB 程序执行时从本质上讲是解释执行,它们只是调用 VBRUNxxx.DLL 中的函数,VB 的 exe 是伪代码,程序都在 vbXXX.dll 里面执行,你只能在 vbdll 里面用 SoftICE 打转转,什么都改不成,而且代码质量不高,结构还颇复杂。当然只要了解其特点用 SoftICE 也可破解,但 SmartCheck 的出现,大大方便了我们,它可将 VB 程序执行的操作完全记录下来,使我们轻而易举地破解大部分 VB 程序。

7. 十六进制编辑器: HIEW 就是一种是十六进制工具,但其是 DOS 界面,因此有必要再准备一款 windows 下的工具,这样的工具很多,如: Ultraedit、WinHex、Hex Workshop 等,其中 Hex Workshop 比较有特色,操作方便,但遗憾的是没有汉化版。

8. 注册表监视工具: 注册表是 Windows 95 及 Windows 98 的核心数据库,表中存放着各种参数,直接控制着 Windows 的启动、硬件驱动程序的装载以及一些 Windows 应用程序运行的正常与否。而应用软件安装时,有可能在注册表中注册,将一些必要的信息放进去,如安装时间,使用次数等。RegShot、regmon 或 RegSnap 就是一种监视注册表变化的工具,以了解应用程序在注册表何处修改了,以协助破解。

9. 侦测文件类型工具: 这样的工具有 TYP、gtw 或 FileInfo 等。这是一个能侦测你的软件是被哪一种“壳”给加密了(就好像侦测你的文件档是被 zip、rar、arj 哪一个给压缩了一样,如果连被哪种软体加了壳都不晓得,那要剥壳就难很多)。一般配合 PROCDUMP 使用。



10. PROCDUMP 脱壳工具,可剥许多壳。你使用的许多软件都是压缩过的,用该工具很方便把它们还原,然后再修改,并可自己编写脚本文件,以便能脱壳新版的壳。它也是一款优秀的 PE 格式修改工具,脱壳必备!

11. IceDump:是配合 SoftICE 而使用的,可抓取内存的数据,以重建 EXE 文件,脱壳必备;并可在 SoftICE 下边调试边听 MP3 哟!具体参考其 ReadMe。

12. Crackcode2000:一种全新的注册机工具,它可以从另一进程的内存中取出你想要的注册码,它可以令水平不高的你一夜之间成为破解高手!有了它,很多软件可以用 20 秒时间写出注册机来,而你不需要会任何的语言,因为它只是一个工具,一个操作很简单的工具,它的参数只有 4 行,实在简单到不能再简单了,它的体积也很少,只有 11K,如果再用其他压缩软件压一下一定会小于 10K,用它可以做出很优秀的注册机。

13. ERU 这是 Windows 安装盘自带的小工具,备份注册表等一些 windows 重要的配制文件,强烈推荐,在你破解一软件前,最好备份一下系统,因为你在破解某些软件的过程和寻找关键点时,在这时改动一下以验证自己的判断,结果正确注册成功,此时你再想回到那里看一看究竟,重装该软件都没用,哈哈!永远是注册版,除非你重装系统。此时你只要还原注册表和配制文件,再重装该软件,又可注册了,这次你就要好好研究它一下了……当然这种情况不多见,但破解某些软件前备份一下注册表,还是有必要的。

14. filemon 文件监视工具,可监视系统文件运行状况,如哪个文件打开,哪个文件关闭,在哪个文件读取了数据等,破解时非常有用,以便了解程序在启动、关闭或验证注册码时做了哪些手脚。

15. EXESCOPE 资源修改器 EXESCOPE 可以说是 exe 及 dll 等执行文件的解析终结工具,它有执行文件(exe, dll 等)的解析与显示功能;提取资源到外部文件;资源的重新写入;记录文件的记录及其再编辑(成批编辑)等功能。是汉化软件的常用工具,当然破解软件时也很有用。

16. Frogsice 最好的 Soft - ICE 加强软件!它并不是简单的将 Soft - ICE 隐藏,而是让你可以配合 Soft - ICE 避过现在流行的各种加密、保护软件里面的各种防止 Soft - ICE 的陷阱。有了它,你再也不用怕在装入一个程序准备调试的时候,程序告诉你发现 Soft - ICE 的存在而终止运行,或者干脆把你的机器从新启动,又甚至触发更残酷的报复手段。



第三章 动态跟踪分析利器—— “SOFTICE”&“TRW2000”

前面章节曾提到过,软件的动态跟踪分析对于破解来说是必不可少的环节,而要完成这项工作,“SOFTICE”和“TRW2000”这两款软件是必不可少的,本章将从“安装”、“操作”、“实例教程”几个角度对两款软件进行剖析。

3.1 SOFTICE for Win9x 安装与设置

- 显卡安装
- 鼠标安装
- 启动菜单配制
- Symbol Loader
- Winice. dat 配制及下载

3.1.1 SOFTICE 安装

(1)SOFTICE 目前最新版本是 4.05,如你的系统是 Win9x,就请下载 for Win9x 版本的 SOFTICE,建议下载 SOFTICE 的最新版本,这样稳定性好些。运行 setup. exe 开始安装,出现如图 3-1。

(2)然后点击下一步,输入安装序列号,如图 3-2(序列号一般在安装软件的 readme. txt 或其他说明文件里)

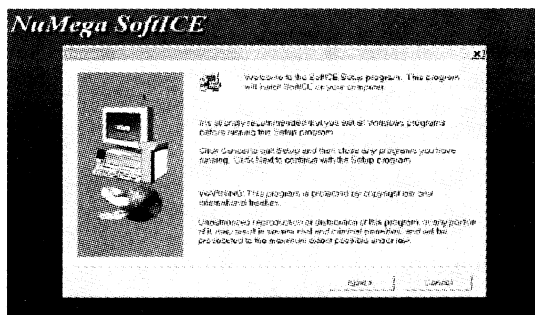


图 3-1

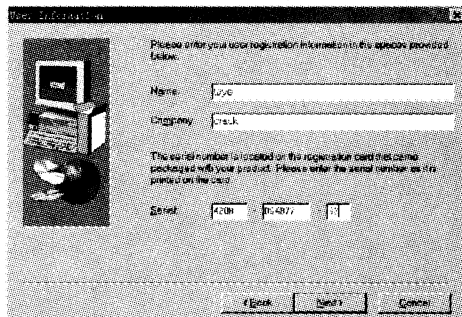


图 3-2

(3)下面几个画面是要求选定路径和安装组件,不久你会来到显卡配制对话框,如图 3-3。



3.1.2 显卡配制

(1)第一种配制是使 SOFTICE 激活状态时类似 DOS 全屏状态一样(也就是字符模式状态)。在显卡列表选择你的显卡类型,Universal Video Driver 和 Use monochrome card/monitor 这两项不要选,然后点击 Test 按钮,在测试过程中你能看到各种颜色的字符,说明显卡测试通过,就可点击下一步了。

(2)第二种配制是使 SOFTICE 在激活状态下类似 windows 应用程序的一个窗口那样,这样在调试时可避免显示器不停地在图形和字符模式转换,对提高显示器寿命大有好处。配制时,显卡列表一栏忽略,不用配制,只要把 Universal Video Driver 这一项选上,然后 Test,跳出如图 3-4 对话框,测试通过。(强烈推荐这种方式)

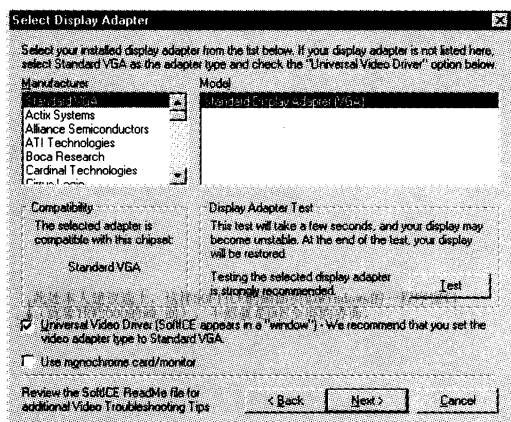


图 3-3



图 3-4

3.1.3 鼠标的配制

现在的鼠标常见的一般是串行口或 ps/2 接口,你根据自己的鼠标接口类型或位置选上合适的就可。如碰到鼠标在 SOFTICE 调试画面不能用或一用就死机,可能是没选好正确的选项,你可以在 SOFTICE 菜单里,如图 3-5 所示,运行 Mouse Setup 这个菜单项重新配制鼠标。

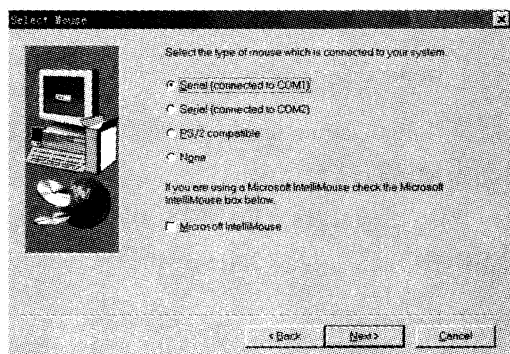


图 3-5

3.1.4 装载 SOFTICE 的主文件 winice. exe

首先要了解 SOFTICE for Win9x 版本是如何装载的。在 SOFTICE 的安装目录下有 winice. exe 这个文件,Windows 启动到纯 DOS 环境下,运行 winice. exe 这个文件,将装载 SOFTICE。安装时默认将 C:\PROGRA ~ 1\NUMEGA\SOFTIC ~ 1\WINICE. EXE 这一行放时进 Autoexec. bat(自



动批处理文件),这样 Windows 以后每次都运行 Autoexec. bat 这个文件,自动装载 SOFTICE。另外,你可根据自身需要配制启动模式,具体参考详见下文。

配置完鼠标后,会出现以何种方式装载 SOFTICE 的主文件 Winice. exe 的询问对话框,如图 3-6;然后安装程序将复制文件到硬盘里,来到最后一个电子注册对话框,如图 3-7,这里选最后一项 Register later。至此,安装完成,重新启动 Windows,微机先到 DOS 下,自动或手动运行相应批处理文件,运行其内的 Winice. exe 文件,装载 Windows。

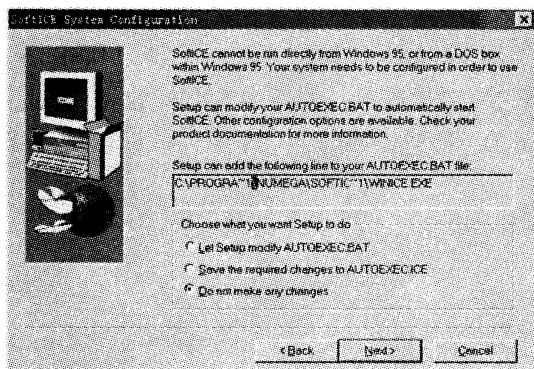


图 3-6

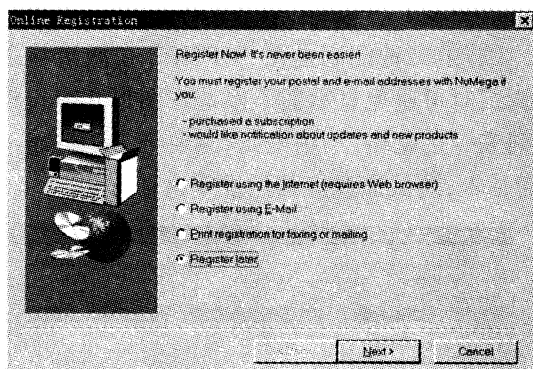


图 3-7

3.1.5 Symbol Loader 的使用

在开始 SOFTICE 的菜单里有一项 Symbol Loader 快捷方式,运行后,进入其菜单 EDIT→SOFTICE Initialization Settings 选项,打开后如图 3-8 所示。这里你就可配制 SOFTICE 了。

1. General 选项

在 Initialization string 里,你可填上需要 SOFTICE 一启动自动运行的命令。如:

WD 2; WC 14; FAULTS OFF; IXHERE OFF; IYHERE OFF; set font 2;lines 40;wd 4;wc 20;cod

2. Exports 选项

在这里可添加相关的 DLL 文件,以便在 SOFTICE 下拦截这些 DLL 的函数。特别是破解 VB 程序时,定要将 VB 运行库装载进去。

3. Keyboard Mappings 选项

这里配制各功能热键。如:F5 = “^x;”用 F5 键代替命令 X。

4. Macro Definitions 选项

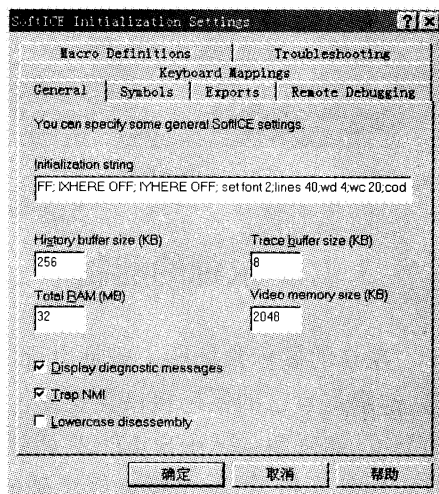


图 3-8



宏定义,你可定制各种命令宏,以方便平时的操作。

如:s7878 = “S 30:0 L ffffffff ’78787878’ ” 用命令 s7878 代替一串命令:S 30:0 L ffffffff ’78787878’

5. Remote Debugging

利用网络远程调试配制。

注:以上所有配制好后的参数,都保存在 winice. dat 文件里。

3. 1. 6 Winice. dat 配制

在 Windows 9x 下 SoftICE 配制除了用上面的方法外,也可通过文件 winice. dat 来实现的。Soft - ICE 在启动的时候通过它装入一些 DLL/EXE 的信息。你可在 SOFTICE 安装目录下发现 winice. dat,可用任何文本编辑软件打开它(如记事本)。

注意分号后是描述语言,不被执行。

PENTIUM = ON

NMI = ON

ECHOKEYS = OFF

NOLEDS = OFF

NOPAGE = OFF

SIWVIDRANGE = ON

THREADP = ON

LOWERCASE = OFF

WDMEXPORTS = OFF

MONITOR = 0

PHYSMB = 32

SYM = 1024

HST = 256

TRA = 8

MACROS = 32

DRAWSIZE = 2048

INIT = “ FAULTS OFF; IXHERE OFF; IYHERE OFF; set font 2;lines 40;wd 2;wc 20; code on;x;”;初始化

F1 = “h;”

F2 = “^wr;”

F3 = “PAGEIN B ProcDump32 - Dumper Server;”;脱壳用

F4 = “^rs;”

F5 = “^x;”



F6 = “^ec;”

F7 = “^here;”

F8 = “^t;”

F9 = “^bpx;”

F10 = “^p;”

F11 = “^G @ SS:ESP;”

F12 = “^p ret;”

SF3 = “^format;”

CF8 = “^XT;”

CF9 = “TRACE OFF;”

CF10 = “^XP;”

CF11 = “SHOW B;”

CF12 = “TRACE B;”

AF1 = “^wr;”

AF2 = “^wd;”

AF3 = “^S 0 L FFFFFFFF 8B,CA,F3,A6,74,01,9F,92,8D,5E,08;” ; VB3 特征字符串

AF4 = “^s 0 l ffffffff 56,57,8B,7C,24,10,8B,74,24,0C,8B,4C,24,14,33,C0,F3,66,A7;”

;VB4 特征字符串

AF5 = “^s 0 l ffffffff FF,75,E0,E8,85,EF,FF,FF,DC,1D,28,10,40,00,DF,E0,9E,75,03;”

;VB5 特征字符串

AF8 = “^XT R;”

AF11 = “^dd dataaddr→0;”

AF12 = “^dd dataaddr→4;”

CF1 = “altscr off; lines 60; wc 32; wd 8;”

CF2 = “^wr;^wd;^wc;”

;以下是宏操作命令:

MACRO s7878 = “S 30:0 L ffffffff '78787878' ”

MACRO sname = “S 0 L FFFFFFFF 'toye' ”

MACRO swide = “s 0 l FFFFFFFF '7','8','7','8','7','8','7','8','7','8','7','8','7','8','7','8','7','8' ”

MACRO reg = “bpx regqueryvalueexa if *(esp→8)>= 'Soft' do ”d(esp→14)“ ”

MACRO bpxpe = “bpx loadlibrarya do ”dd esp→4“ ”

MACRO bpxgeta = “bpx GetDlgItemTextA; bpx getwindowtexta; bpx getdlgitemint; bpx getdlgitemtext;”

; * * * * * Examples of sym files that can be included if you have the SDK * * * * *

; Change the path to the appropriate drive and directory

;LOAD = c:\windows\system\user.exe



```
;LOAD = c:\windows\system\gdi.exe
;LOAD = c:\windows\system\krnl386.exe
;LOAD = c:\windows\system\mmsystem.dll
;LOAD = c:\windows\system\win386.exe
; Exports - change the path to the appropriate drive and directory
```

EXP = c:\windows\system\advapi32.dll ;这四行前不要加分号,否则不被装载,SOFTICE 可能什么也拦不到 :

```
EXP = c:\windows\system\kernel32.dll
EXP = c:\windows\system\user32.dll
exp = c:\windows\system\gdi32.dll
exp = c:\windows\system\comctl32.dll ;
```

; 如你要破解 VB 程序,下面的 VB 运行库将要装载,SOFTICE 默认值是没有这几行,你需手动加上。

```
;EXP = c:\windows\system\msvbvm60.dll; Visual Basic 6 具体参考第十五课 VB 破解
```

EXP = c:\windows\system\msvbvm50.dll; Visual Basic 5 注意在这五个 DLL 中最好不要同时装载 2 个以上

```
; EXP = c:\windows\system\vb40032.dll; Visual Basic 4(32bit)
; EXP = c:\windows\system\vb40016.dll; Visual Basic 4(16-bit)较少见
; EXP = c:\windows\system\vbrun300.dll; Visual Basic 3
;EXP = c:\windows\system\vga.driv;
;EXP = c:\windows\system\vga.3gr
;EXP = c:\windows\system\sound.driv
;EXP = c:\windows\system\mouse.driv
;EXP = c:\windows\system\netware.driv
;EXP = c:\windows\system\system.driv
;EXP = c:\windows\system\keyboard.driv
;EXP = c:\windows\system\toolhelp.dll
;EXP = c:\windows\system\shell.dll
;EXP = c:\windows\system\commdlg.dll
;EXP = c:\windows\system\olesvr.dll
;EXP = c:\windows\system\olecli.dll
;EXP = c:\windows\system\mmsystem.dll
;EXP = c:\windows\system\winoldap.mod
;EXP = c:\windows\progman.exe
;EXP = c:\windows\drwatson.exe
; * * * * * Examples of export symbols that can be included for Windows 95 * * * * *
; Change the path to the appropriate drive and directory
```



```
EXP = c:\windows\system\kernel32.dll
EXP = c:\windows\system\user32.dll
EXP = c:\windows\system\gdi32.dll
EXP = c:\windows\system\comdlg32.dll
EXP = c:\windows\system\shell32.dll
EXP = c:\windows\system\advapi32.dll
EXP = c:\windows\system\shell232.dll
EXP = c:\windows\system\comctl32.dll
;EXP = c:\windows\system\crt.dll
;EXP = c:\windows\system\version.dll
EXP = c:\windows\system\netlib32.dll
;EXP = c:\windows\system\msshui.dll
EXP = c:\windows\system\msnet32.dll
EXP = c:\windows\system\mspwl32.dll
;EXP = c:\windows\system\mpr.dll
```

启动 Windows 装载 SOFTICE 后,咦!怎么没反应?没调试画面!哈哈,别着急,按 CTRL + D 看看,再按一下回到 Windows 下,或按 F5 也能回来。此时调试窗口像人 Windows 开的一窗口,如果像全屏 DOS 一样窗口,那就是安装显卡时参数没选好,此时按上文修正即可。下面的命令是调整 SOFTICE 窗口状态:

```
set font n(n=1,2,3)设置字体;本人建议 set font 2(在 800 乘 600 条件下)
set origin x,y(x,y)锁定窗口;
lines n n=(25-128)设置显示行数;本人建议 lines 40
Ctrl + Alt + 光标键 移动窗口;
Ctrl + Alt + home 重设窗口位置原点(0,0);
Ctrl + L 刷新。
```

如你以默认 winice.dat 启动 SOFTICE,有可能需用 WD 打开数据窗口;用 SET FONT 2 设置字体等重复工作。你可在 winice.dat 文件内设置自动执行命令操作,方法是在 INIT 这一行,各命令用分号分开,如:

```
INIT="WD 2; WC 14; FAULTS OFF; IXHERE OFF; IYHERE OFF; set font 2;lines 40;x;"这样配制后界面类似 TRW2000。(这些是在 800T 乘 600 条件下的情况,如你不是此分辨率可调整 set font n;lines n)
```

3.2 SOFTICE for NT/2K 安装与配制

1、SOFTICE for NT/2k 的安装与 for 9x 版本差不多,所不同的是在装载 SOFTICE 方式选择,如图 3-9 所示。可根据需要选择不同的装载方式,注:如你选择了 Manual 方式,要装载

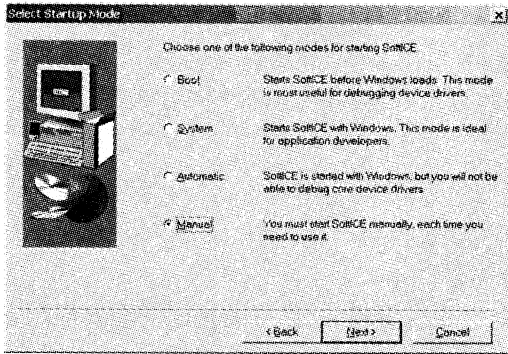


图 3-9

SOFTICE, 需要来 SOFTICE 的菜单里运行选项: START SOFTICE 快捷方式来装载 SOFTICE。

2、在 NT 下, 配制 SOFTICE 是用 SOFTICE Loader(从你的开始菜单选), 选择 Edit/SoftICE, 一般的选项是初始化, 这里你可参考手册了解不同的开关选项的详细描述。如:

```
CODE ON; FAULTS OFF; I3HERE OFF;
WD 3; WF; X;
```

其他两个重要的选项是 Symbols & Exports。

如果你拥有自己系统的 SDK (软件开发工具包),

你可用 SOFTICE 装载并调试它。那些没有 SDK 的, 应该用 exports 选项从 % WinNT% /System32 目录下增加下面的 dll 文件:

```
advapi32.dll, comctl32.dll, comdlg32.dll, gdi32.dll, kernel32.dll, msvbvm(50/60).dll
(如果需要), msvcrt.dll (如果需要), ole32.dll, oleaut32.dll, shell32.dll, user32.dll, version
.dll。
```

3.3 TRW2000 的安装与配制

国人自己编写的调试软件, 完全兼容 SOFTICE 各种指令, 但现在许多软件能检测 SOFTICE 存在, 而 TRW2000 在这方面就好多了。TRW2000 有它自己的独特方面, 是针对破解软件优化的, Windows 下的跟踪调试程序, 跟踪功能更强; 可以设置各种断点, 只是断点种类更多; 它可以像一些脱壳工具一样完成对加密外壳的去除, 自动生成 EXE 文件, 只是留给用户更多的选择; 在 DOS 下的版本为 TR。

3.3.1 安装 TRW2000

TRW 安装简单多了, 没有 SOFTICE 那样复杂, 但目前 TRW2000 不支持 Windows NT。它发布的版本是一个 ZIP 压缩包, 才 200 多 K。只要将其解压缩到一个目录下, 然后运行 TRW2000.EXE 即可, 如图 3-10 所示, 无须安装或者重启计算机。

激活方式同 SOFTICE 不一样:

(1) Ctrl + M 特权级 0 级的热键, 能够立即中断 Win9x。

相当于 Soft-ICE 的热键 Ctrl + D。

(2) Ctrl + N 特权级 3 级的热键。在绝大多数时候, 我们并不需要在 0 级上中断。Ctrl + N 可以中断 Windows 的特权级 3 级的前台线程。这应该是我们最常用的。其他指令同 SOFTICE 兼容, 但

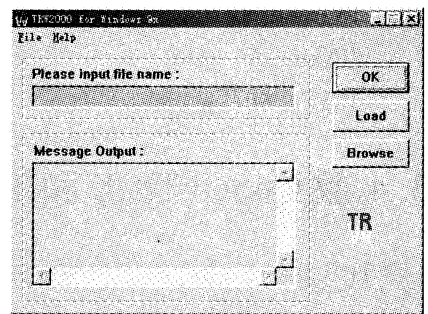


图 3-10



是 TRW2000 有许多更新的思想,具体看后面的介绍及范例。另外,TRW2000 可支持 plug-ins,也可装载 dll 文件。在 1.15 版本以上,在安装目录下有一 dll 目录,如你特别需要的 dll 复制到此目录,即可装载,如破解 VB 时,就需要将 VB dll 复制到此目录。具体参考后面的 VB 破解。其他的请读其 ReadMe。

3.3.2 TRW2000 的配制

TRW2000 的配制是通过其安装目录下的 TRW2000.ini 来实现的,你可按自己的需要配制它(一般按默认即可)。

```
; TRW2000 Initialize file
; Please modify it as your habit .
;PLUGS = C:\MY_PLUGS\HELLO.SYS
F1 = ^HELP ; Command length CAN'T be longer than 15 characters !
; This command length is 5 charcaters .
F3 = ^SRC
F4 = ^RS
F5 = ^X
F6 = ^EC
F7 = ^HERE
F8 = ^T
F9 = ^BPX
F10 = ^P
F12 = ^PRET
;HOTKEY = 320D ;Ctrl + M
;R3HOTKEY = 310E ;Ctrl - N
GRAPHICS = ON
;INTELLIMOUSE = OFF
WINMOUSE = ON
LINES = 50 ;in dec
```

3.4 熟悉 SOFTICE 和 TRW2000

TRW2000 的命令操作和 SOFTICE 兼容,因此 SOFTICE 的操作在 TRW2000 里一般都能实现。

3.4.1 操作窗口

按上一节方法装载好 SOFTICE 后,在 Windows 环境里,按下 CTRL + D 键即可激活 SOFT



ICE (如是 TRW2000, 则按 CTRL + N 激活) 出现如图 3-11 所示的调试画面(图片注释文字: 在数据窗口左半边是以二进制表示的内存数据, 右半边是以 ASCII 码表示的内存数据)。

大家可能注意到, 窗口中“代码窗口”与“命令窗口”之间的部分被称做“程序领空”, 这里就解释一下“领空”一词的由来和含义。我想大家肯定看过网上一些前辈们写的文章, 他们多是港台地区的, 所以称“程序”为“程式”, 而大陆的学生在学校里或书本上用“程序”一词较多。现在是赶时髦或叫做“称谓大融合”的时代, 叫什么都没有关系, 但有一点是肯定的, 我们说的都是同一档子事“PROGRAM”

所谓“领空”也是他们传出来的, 比较形象, 姑且就这么叫吧! “领空”实际上是指在某一时刻, CPU 的 CS:IP(EIP)所指向的某一段代码的所有者所在的区域。一个程序的“领空”实际上是指 SoftICE 所停下来时光棒所在的那一句代码是属于谁的, 属于该程序的就叫该程序的“领空”, 如果你想窥探该程序的代码, 就要在该程序的“领空”中进行跟踪。

3.4.2 常用命令

在这里, 我把 SOFTICE 一些常用命令列出, 详细解说请参阅附录中的 SOFTICE 指令详解。Soft-ICE 的所有动作都发生在一个可以随时激活的视窗中。Soft-ICE 的所有指令都可以显示在一个小视窗中, 这个视窗可以扩大到整个屏幕, 在视窗底部的状态行提供指令语法的辅助。

1. 激活视窗

载入 Soft-ICE 后, 你可以随时激活视窗。一开始你只要按 Ctrl-D 即可激活 Soft-ICE。

2. 由视窗中返回

使用 X 这个指令或者按 Soft-ICE 的热键均可以回到原先的画面。你在 Soft-ICE 中设定的所有中断点此时开始启动。

3. 改变视窗大小

你可以改变 Soft-ICE 视窗的宽度和高度。在独立模式中显示程序码时, 改变视窗大小的功能特别有用。视窗的高度为 8 到 25 行。

按 Alt + ↑ 使视窗变高

Alt + ↓ 使视窗变短

图 3-11



使用 WIN 的指令以改变视窗的宽度。直接输入 WIN 而不加参数会在下面两种模式中切换：

WIDE 模式——占满整个屏幕

NARROW 模式——46 个字节宽

有些指令像 D、E、R、U，使用 WIDE 模式以显示更多信息时较为方便。

4. 移动视窗

Soft - ICE 的视窗是可以移动且可以定位在屏幕上的任何地方。这功能在 NARROW 模式下特别有用。在你需要时移动视窗以便观看屏幕上被视窗挡到的地方。你可以用下列按键控制屏幕的移动：

Ctrl - ↑ 向上移一行

Ctrl - ↓ 向下移一行

Ctrl - → 向右移一列

Ctrl - ← 向左移一列

5. 窗口打开或关闭命令

WC 作用：打开或关闭代码窗口；或改变代码窗口大小

WD 作用：打开或关闭数据窗口；或改变数据窗口大小

WF 作用：以浮点或 MMx 形式显示浮点栈

WR 作用：打开或关闭寄存器窗口

WW 作用：打开或关闭监视窗口；或改变监视窗口的大小

6. 行编辑按键

Soft - ICE 有一个容易使用的行编辑器。以下按键可以帮助你命令窗中编辑指令：

→——光标右移

←——光标左移

Ins——切换插入模式

Del——消除现在字节

Home——把光标移到一行的开头

End——把光标移到一行的结尾

↑——显示上一个指令

↓——显示下一个指令

Shift - ↑——显示向上卷一行

Shift - ↓——显示向下卷一行

Page Up——显示向上卷一页

Page Down——显示向下卷一页

BackSpace——消除前一个字节

Esc——取消目前命令

当光标在数据窗口或代码窗口时，另有特殊的按键，这在后面将会讨论到。



7. 指令语法

Soft - ICE 是个由指令操控的调试工具。要让 Soft - ICE 进行操作,你要下指令给它。指令可以因不同参数而有改变。所有的指令都是 1 到 6 个字节的字串且不分大小写。所有的参数都是字串或计算式。计算式是典型的数字,也可以是数字和运算式的结合。所有的数字均以 16 进位表示。一个字节(byte)参数有 2 位,字(word)参数有 4 位。双字(double word)是两个由“:”分隔的字组参数。以下是一些参数的例子:

12——字节参数

10FF——字参数

E000:0100——双字参数

寄存器在计算式中可以拿来当字节或字参数用。例如:U CS:IP - 10 的指令会从现在指令指标所指地址向前 10 byte 开始反汇编。以下的寄存器名称可以用在计算式中:

AL、AH、AX、BL、BH、BX、CL、CH、CX、DL、DH、DX、DI、SI、BP、SP、IP、CS、DS、ES、SS、FL

8. 指定内存地址

许多 Soft - ICE 的指令要求以内存地址当参数。一个内存地址是由两个 16 位的字中间以“:”分隔而组成的。第一个字组表示节段地址(segment address),第二个字组表示偏移地址(offset segment)。

公用符号可以在所有 Soft - ICE 指令中用来取代地址。公用符号必需先由 Soft - ICE 的程序载入器(LDR. EXE)载入。

Soft - ICE 计算式的运算器接受一些特殊字节和地址的使用。这些字节是:

\$——现在 CS:IP 所指的地址

@ 地址——间接双字

. number——原始程序码行号

当你要输入目前指令指标的地址时,可以用\$代替 CS:IP。

使用@ 可以让你参考到地址所指处的双字。你可以使用多层的@。

如果用. 来代表地址,它是用来代表源程序码中的行号,而非实际的地址。这只有在原始程序码有载入的情形下才能使用。这种情况下,地址是以 10 进位表示。

例如:U. 1234——从原始程序码第 1234 行开始反汇编

U \$ - 10——从目前指令指标所指处向前 10 byte 开始反汇编

G @ SS:SP——假如你目前正在第一个中断程序,下这个指令会在堆栈的返回地址设个暂时中断点并跳过此中断程序。

9. 功能键

功能键可以代替一串 Soft - ICE 指令。功能键可以由命令行设定或在 WINICE. DAT 中定义。

Soft - ICE 的配制文件 winice. dat 已经对 12 个功能键有设定。你可以在任何时候改变任何一个设定。每个键定义如下表所示。这样设计是为了方便微软的 CodeView 的使用者。

F1——显示一般辅助画面 (H;)



- F2——在寄存器窗中切换 (^WR;)
- F3——改变目前原始码的模式 (^SRC;)
- F4——恢复屏幕内容 (^RS;)
- F5——回到原程序(^X;)
- F6——在命令窗中和程序码窗中切换(^EC;)
- F7——执行到光标所在那行(^HERE;)
- F8——单步执行 (^T;)
- F9——在光标所在那行设中断点 (^BPX;)
- F10——单步执行 (^P;)
- F11——执行到返回地址(^G @ SS:SP;)
- F12——让 SoftICE 单步执行代码,直到出现 RET(XXXX)命令,之后拦截 (^pret;)

指令前的^会让这个指令不显示出来。指令后的;则代表按下 Enter。输入 FKEY 的指令可以显示目前功能键所代表的意义。要使用功能键直接按下功能键即可,不需再键入指令。

10. 辅助

利用辅助的指令可以得到有关指令的简单解说、语法和使用例子。要得到辅助的信息,键入:

?或 H——显示所有指令和运算式的简短解说

?指令或 H 指令——显示关于指令语法和例子更详细的信息

?计算式或 H 计算式——把计算式的结果以 16、10 进位及 ASCII 码显示出来

3.4.3 关于中断点指令的使用

Soft-ICE 具有以往只有硬件调试器才具有的断点能力。因为 80386 芯片的威力和弹性,使我们不需要额外的硬件设备就能有更强大的断点能力。断点的触发可以由内存某地址的读取、内存范围的读取、程序的执行及端口的存取来达成。Soft-ICE 赋与每个断点一个一位的 16 进位号码(0-F)。这个断点号码是当你对断点作删除、中止、启动、编辑等动作时使用。Soft-ICE 的所有断点都是“sticky”。这个意思是这些断点在启动后不会自动消失。你必需以 BC 或 BD 命令来消除或关闭它。SoftICE 一次可以处理 16 个断点。同种形态的断点最多可以有 10 个。但内存地址的断点(BPM)因 80386 处理器的暂存器的缘故,最多只能设 4 个。

设置中断点是破解跟踪软件中最常用到的行为之一,这里只是列出相关指令让大家了解一下,详细的使用技巧和语法格式会在以后章节的实例及附录中的 SOFTICE 指令详解中列出。

设置中断点指令:

BPM BPMB BPMW BPMD——在内存地址被存取或执行时引发中断

BPR——对内存范围设置中断点

BPIO——对 I/O 端口存取时触发中断

BPINT——呼叫插断时触发中断

BPX——设置/清除执行中断点

CSIP——CS:IP 范围的检定判断



BPAND——等待复合中断点的发生

BPM BPMB BPMW BPMD——在内存地址被存取或执行时引发中断

处理指令：

BD——中止中断点

BE——启动中断点

BL——列出中断点

BPE——编辑中断点

BPT——把中断点当样板

BC——清除中断点

3.4.4 其他指令

除了中断点指令外,SoftICE 还有很多实用指令,如“显示及编辑类指令”、“转换控制指令”、“调试模式指令”、“公用指令”、“特别的调试指令”、“视窗指令”、“调试器设定指令”和“屏幕控制指令”。以后章节会通过实例对它们的使用方法进行讲解。

3.5 小试牛刀——破解实例一

你一定要看了前几章节的内容再来这节实战操作,在下手之前你要先掌握这些问题:F8、F12、F9、F7、F5、F11 等功能键含义;另外领空、断点、,数据窗口位置、子程序 CALL 等概念及 SOFTICE 的常用命令操作。

例:CRACKME 序列号保护难度:易(所有破解实例中所使用的程序均放置在光盘中)

方法一、利用函数 hmemcpy 来破解

hmemcpy 解释:是 Win32 的一函数;其功能:将内存中的一块数据拷贝到另一个地方,破解时非常实用。为什么要加个“h”在“memcpy”前面呢?因为它可以传送大于 64K 的数据。是“HUGE”的意思。(在 Win2k 或 WINNT 下,这函数不起作用,这时你可参考方法二)

操作步骤:

按前两节配制好,装载好 SOFTICE;

1、在对话内 Registration 输入:12345678(随意填些数字);

2、这时你点击按钮 Check,程序将跳出一出错对话框,我将以此为目标作为跟踪的目的;

3、按 CTRL + D 切入 SOFTICE 的环境

4、下断点: bpx hmemcpy (其作用时,当 Windows 应用程序一调用 hmemcpy 函数拷贝数据时,SOFTICE 将中断);

5、按 F5(或按 CTRL + D)回到 Windows 环境;

6、此时你不要运行其它程序,或点击 Windows 的其它菜单,而应直接点击刚才的练习软件的 Check 按钮;不然其它应用程序运行时也会调用 hmemcpy 函数导致 SOFTICE 意外中断;

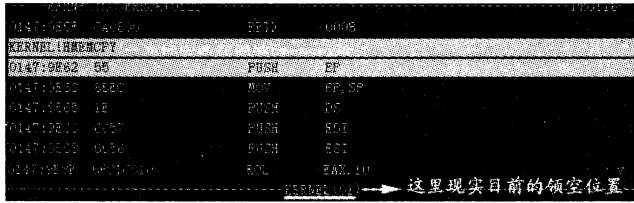


图 3-12

7、点击按钮 Check 后,SOFTICE 马上激活中断,如图 3-12 所示:

一般系统领空名称是 KERNEL??? 或 user(?),我们的目的是让领空来到刚才这个小程序(其文件是:Crackme.exe),因此我们的目标观察领空名为:

Crackme????

8、下命令:BD * 把拦截的功能关掉;此时你下命令:BL 可显示刚被禁止的中断点;BE * 命令恢复刚被禁止的断点;

9、此时你按 F12 从 Windows 的底层跳出(每按一下跳出一个子程序);

(重要技巧 F12 的应用:为什么要按 F12,因为 F12 是 SICE 的“快捷键”,代表了指令:P RET (这可以设置的),P RET 的意思是让 SICE 一直执行代码,直到出现 RET(XXXX)命令,再跳出来拦截,这时,当前 IP(EIP)会是停在 RET(XXXX)后的某一条语句上,通常是在某一个 CALL XXXXXXXX 后面。由于我们通常用 SICE 在某些底层的 Windows 函数上设断点,所以 F12 是很管用的。因为程序的作者用的是高级语言,Windows 又是提倡“透明”,不希望程序员知道底层的操作,而只提供给他们高层的接口,而相当多的高级函数调用某个一定的底层函数,所以当你在底层函数上下断点,再用 F12,就可以知道他用的是什么函数了。SICE 用于程序员可以很方便,很快捷地找出程序调用错在哪里,是哪个参数出了问题。当然用于拆解也是可以的,好象一个高明的医生,会医人,也会杀人,而且还轻车熟路!

由于 Windows 调用是很复杂的,一个调一个,所以 F12 可能要执行很多次才能看到这个 CALL 是谁发出的。)

10、按了大概 12~13 次 F12,来到 crackme 程序的领空:

```
0167:0040154E52PUSHEDX
~ ~~~~~ ~
```

前面的 0167 你和我的可能不同,但后面的偏移地址:0040154E 应和我的一样;第三组是机器码,在这里是:52

```
0167:0040154F68E8030000PUSH000003E8
```

```
0167:004015548B4DE0MOVECX, [EBP - 20]
```

```
0167:00401557E8A8050000CALL00401B04//我们按了这么多 F12,就会从此 CALL 里出来
```

```
0167:0040155C8D45F4LEAEAX, [EBP - 0C]//为了再次运行程序能拦截,将光标移到此行,按 F9 或双击鼠标强行设置断点;以后程序运行时会在这一行中断
```

```
----- -- CRACKME!.text + 0557(←注意 crackme 程序领空)----- --
```

11、此时按 F10,让指令一行一行执行,直到下面:

```
0167:004015B98B4DE0MOVECX, [EBP - 20]
```

```
0167:004015BCE83D050000CALL00401AFE//用 F10 一带过此就跳出注册失败的窗口
```

```
0167:004015C18BE5MOVESP, EBP
```

```
0167:004015C35DPOPEBP
```




Pc friend ·

0167:004015C4C3RET

在这我们已找到出错的对话框了。

12、再按 F5 回到 Windows,重新点击 Crackme 的检测序列号的按键 Check,将会中断在我们第 10 步设断处 0167:0040155C 这一行;

13、然后慢慢全面分析这段程序:

0167:0040154E52PUSHEDX

0167:0040154F68E8030000PUSH000003E8

0167:004015548B4DE0MOVECX, [EBP - 20]

0167:00401557E8A8050000CALL00401B04//按 F12 从此 CALL 里出来

0167:0040155C8D45F4LEAEAX, [EBP - 0C]

0167:0040155F50PUSHEAX

0167:00401560FF1504204000CALL[KERNEL32! strlen]

0167:004015668945F0MOV[EBP - 10], EAX

0167:00401569837DF001CMPDWORD PTR [EBP - 10], 01

0167:0040156D7316JAE00401585

0167:0040156F6A40PUSH40

0167:00401571682C304000PUSH0040302C

0167:004015766834304000PUSH00403034

0167:0040157B8B4DE0MOVECX, [EBP - 20]

0167:0040157EE87B050000CALL00401AFE

0167:00401583EB3CJMP004015C1

0167:004015858D4DE4LEAECX, [EBP - 1C]

~~~~~

//此时用 F10 过了这一行,再下命令:d ecx;在数据窗口(如图 3-13)看到正确的序列号<BrD - SoB>:

0167:0040158851PUSHECX

0167:00401589D55F4LEAEDX,

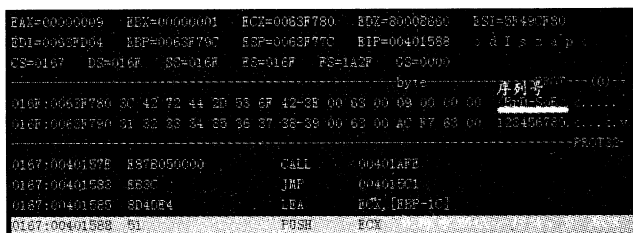


图 3-13

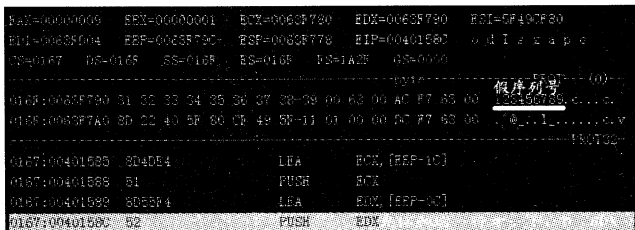


图 3-14

[ EBP - 0C ]

~~~~~

//此时用 F10 过了这一行,再下命令:d edx;在数据窗口(如图 3-14),我们刚输入的序列号 12345678:

0167:0040158C52PUSHEDX

0167:0040158DFF1500204000CALL[KERNEL32! strcmp]//用函数 strcmp 来比较序列号

0167:0040159385C0TESTEAX, EAX//相等 eax 返回 0



```
0167:004015957516JNZ004015AD//此处如不跳可躲过下面的出错的 CALL
0167:004015976A40PUSH40
0167:004015996850304000PUSH00403050
0167:0040159E6858304000PUSH00403058
0167:004015A38B4DE0MOVECX,[EBP-20]
0167:004015A6E85305000CALL00401AFE
0167:004015ABEB14JMP004015C1
0167:004015AD6A40PUSH40
0167:004015AF686C304000PUSH0040306C
0167:004015B46874304000PUSH00403074
0167:004015B98B4DE0MOVECX,[EBP-20]
0167:004015BCE83D05000CALL00401AFE//用 F10 一带过这就跳出注册失败的窗口
0167:004015C18BE5MOVESP,EBP
0167:004015C35DPOPEBP
0167:004015C4C3RET
```

方法二、利用函数 Messageboxa 来破解

1、我们输入假的序列号时,按 Check 按钮,程序跳出如下对话框,如图 3-15 所示。

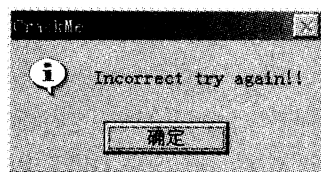


图 3-15

Windows 系统是利用函数 Messageboxa 来实现这个对话框的,因此我们用此函数设断拦截这个对话框。

2、输入假的序列号于 Crackme 里,在按 Check 按钮前,按 Ctrl + D 切换到 SOFTICE 环境下。

3、在 SOFTICE 里下命令:bpx messageboxa。

4、按 F5 返回到 Windows,按 Check 按钮,SOFTICE 将中断。

5、BD * 清除断点,按 F11 程序会回到 Windows 环境(不要按 F5),跳出如图的错误框,点击 OK 后,SOFTICE 将再次中断;

6、然后再按 1~2 下 F12,就会回到像方法一程序代码处。其他步骤类似方法一。

方法三 利用 TRW2000 来破解

1、TRW2000 的操作完全和 SOFTICE 一样,你完全依照 SOFTICE 的步骤用 TRW2000 来操作;

2、但 TRW2000 有一些自己特色的命令,下面简单描述一下:

3、在对话内 Registration 输入:12345678(随意填些数字);

4、按 Ctrl + N 切换到 TRW2000 的跟踪调试环境里;

5、下命令:bpx hmemcpy;

6、按 F5(或按 Ctrl + N)切换到 Windows 环境里;

7、直接点击刚才的练习软件 Cracme 的 Check 按钮;TRW2000 将中断,中断的位置与 SOFT-



Pc friend ·

ICE 一样;

8、此时可用 TRW2000 特有命令:pmodule(快速回到 Crackme 的领空);这个命令很好用,可以不用像 SOFTICE 一样按多次 F12 才能回到 Crackme 的领空;

9、以后的操作与 SOFTICE 一样。

另外,TRW2000 还有一命令:suspend(挂起 Crackme 程序,回到 Windows 下,你可自由操作其它东西,再将按 Ctrl + N 又可回到刚才中断点);这个命令很适用。

TRW2000 中的 G 命令和 SOFTICE 里的也不太一样,SOFTICE 必须在当前的段址 CS 下才可中断(也就是说 G 命令起作用的条件是在当前的段地址 CS 下,IP 等于设定的 OFFSET,SOFTICE 才中断);而 TRW2000 中,只要程序执行中 IP 等于设定的 OFFSET,就会停下。你不用担心段址在哪儿,代码是否动态生成。只要知道它会经过那儿,就会停下。

小结

在这个程序里我们发现程序是利用函数:lstrcmp 来比较序列号的,因此我们也可用此函数设断;另外也可用 getDlgItemTextA、getWindowTextA 等函数,它们作用:把文字框中的内容读出来。

本题中也可用如下函数设断:

- (1)bpx hmemcpy
- (2)bpx messageboxa
- (3)bpx getDlgItemTextA
- (4)bpx getWindowTextA
- (5)bpx lstrcmp

以上这几个函数断点很常用,应牢记,下一个破解实例使用到了 getWindowTextA。

3.6 破解实例二——“ask Lock”(ED! SON 设计制作)

类型:容易的注册码方式的注册

注册码通常在普通的 Windows 文字框中输入。为了检查输入的注册码,程序必须采用下面这些函数中的一个来把文字框中的内容读出来:

16 - bit32 - bit

GetWindowTextGetWindowTextA, GetWindowTextW

GetDlgItemTextGetDlgItemTextA, GetDlgItemTextW

32 - BIT 函数的最后一个字母告诉我们函数是使用单字节还是双字节字符串。双字节的注册码是很少见的。也许你已经体会到我的意思了,“如果能在 GetWindowText 时中断...”,你的确能这样做!但是你首先必须确认这些符号已经由 SOFTICE 载入了。

你可以用 exp getWindowtext 命令来检查 SoftICE 是否已经为 GetWindowText 装入了符号,像这样:



```
:exp getWindowtext
```

如果你没有得到所有 GetWindowText 函数的列表,你就得编辑 \SIW95\WINICE.DAT,在“Examples of export symbols that can be included for chicago”这段文字以后的那些“exp =”的行首去掉“;”,为了节省内存,选择最重要的几个就可以了:kernel32.dll、user32.dll、gdi32.dll。编辑完后,重新启动计算机使其生效。

在 SoftICE 中设定一个“陷阱”(实际上我们叫中断点),你得先按 Ctrl + D 进入调试状态,然后用命令 BPX,后面跟著是函数的名字或者内存地址。因为 Task Lock 是 32 位程序,所以我们在 GetWindowTextA 处设一个断点。如果这个不行,我们可以再试其他的。

像这样在 SoftICE 中输入:

```
:bpx getWindowtexta
```

如果你得到“No LDT”这样的错误信息,就要注意不要运行其它程序。注意 Norton Commander/Dos 会干扰这个功能。你可以列出所有断点来检查一下是否设好断点:

```
:bl
```

你会看到这样的信息:

```
00)BPX USER32! GetWindowTextA C = 01
```

你可以再按一次 Ctrl + D,从 SoftICE 中退出。

好了,不管怎么样,你已经设定好了断点以捕捉任何对 GetWinowTextA 的调用。

现在我们在该输入注册码的地方输入一些数字,然后按下 OK……你只得到了一个信息框告诉你输入的注册码是无效的。看来不是 GetWindowTextA……我们来试试 GetDlgItemTextA。首先删除旧的断点:

```
:bc 0
```

(0 表示在断点列表中的第 0 个断点)

然后设定新的断点:

```
:bpx getdlgitexta
```

再来试一次……行了!你已经在 SoftICE 中了,就在函数 GetDlgItemTextA 开始的地方。按 F11 键,回到调用函数的地方。现在你到了 SGLSET.EXE 的内部。如果你还没把握的话,看看代码窗和数据窗中间的一行的“程序领空”,你应该看到这样的东西:

```
----- - - SGLSET!.text + 1B13 ----- - -
```

你可以这样禁止刚才的断点:

```
:bd 0
```

以后想再开启它的话,可以这样:

```
:be 0
```

代码窗的第一行是:

```
CALL[USER32! GetDlgItemTextA]
```

按几次 Ctrl + Up 直到你看到下面这几行。如果对汇编不太熟悉的话,请看后面的注解:

```
RET; 函数结束
```

```
PUSHEBP; 函数开始
```



Pc friend ·

```

MOV EBP, ESP
SUB ESP, 0000009C
PUSHESI
>LEA EAX, [EBP - 34] ; EAX = EBP - 34
PUSHEDI
MOVEESI, ECX
PUSH32; 输入字符串的最大长度
>PUSHEAX; 输入字符串的缓冲地址
PUSH000003F4; 控制标识
PUSHDWORD PTR [ESI + 1C]; 对话框的句柄
CALL[USER32! GetDlgItemTextA]; 取得输入

```

PUSH 指令保存那些数值以供后面使用。我已经在重要的地方加上了一个“)”字符作上记号。看这几行我们就知道字符缓冲区的地址保存在 EAX 中,而 EAX 等于 EBP - 34。

所以我们来看看 EBP - 34 那里有什么:

```
:d ebp - 3
```

你应该能在数据窗中看到你输入的东西。下面我们得来找开始核对输入注册码的地方。按 F10 一步一步地单步运行直到你发现与 EBP - 34 有点关系的地方……你不用单步运行多久,就会看到这些代码:

```

>LEA EAX, [EBP + FFFFFFF64] ; EAX = EBP - 9C
LEA ECX, [EBP - 34]; ECX = EBP - 34
PUSHEAX ; 保存 EAX
PUSHECX ; 保存 ECX
>CALL00403DD0; Call 一子程序
ADD ESP, 08 ; 删除保存的信息
TESTEAX, EAX; 检查返回值
JNZ 00402BC0; 如果不是零的话跳转

```

对我来说,马上就可以看出这像是一个字符比较程序。它们工作起来就是这样:

输入两个字符串

如果相同就返回零

否则返回非零

那为什么程序要用一个字符串来和你输入的相比较呢?看它是不是合法的!(可能你已经想到了)。那么是什么东西躲在[EBP + FFFFFFF64]?SoftICE 处理负数还不是很好,所以得算算:

$$10000000 - FFFFFFF64 = 9C$$

在 SoftICE 用这样的命令:

```
:?0 - FFFFFFF64
```

10000000 对 SoftICE 来说太大了,但它还是给出了相同的结果。现在是来看看什么东西躲在 EBP - 9C 那里的时候了,这样输入命令:



```
:d ebp - 9c
```

数据窗口会显示出一大排数字——注册码!但是记住我前面说过的,两种注册方式对应两个注册码……所以你把这些注册码抄下来以后,继续用 F10 单步运行,我们会遇到这些代码:

```
>LEA EAX, [EBP - 68]; EAX = EBP - 68
```

```
LEA ECX, [EBP - 34]; ECX = EBP - 34
```

```
PUSHEAX ; 保存 EAX
```

```
PUSHECX ; 保存 ECX
```

```
>CALL00403DD0; 再次调用子程序
```

```
ADD ESP, 08 ; 删除保存的信息
```

```
TESTEAX, EAX; 检查返回结果
```

```
JNZ 00402BFF; 如果非零跳转
```

你在 EBP - 68 处找到了什么?不错吧…另一个注册码。

```
:d ebp - 68
```

3.7 破解实例三——Command Line 95 (ED!SON 设计制作)

类型:容易的用户名/注册码方式的注册、注册器

1. 检查程序

检查程序以后你知道它是 32 位的应用程序,要求输入名字和注册码。让我们开始!

2. 捕捉代码

我们象拆解 TaskLock 那样设置断点。我们可以在可能性最大的两个函数都设上断点: GetWindowTextA 和 GetDlgItemTextA。按下 Ctrl + D 进入 SoftICE,然后:

```
:bpx getwindowtexta
```

```
:bpx getdlgitemtexta
```

接下来进入注册对话框,输入一个名字和一些数字(多数情况下是一个整数)。

我是这么写的,然后按 OK。

```
Name:ED!SON '96
```

```
Code:12345
```

程序在 GetDlgItemTextA 处停住了,就像 TaskLock 一样。我们按 F11 回到调用它的地方。用 Ctrl + Up 卷动窗口直到看到这些:

```
MOV ESI, [ESP + 0C]
```

```
PUSH1E; 最大长度
```

```
PUSH0040A680; 缓冲地址
```

```
PUSH000003ED; 控制柄
```

```
PUSHESI ; 对话框柄
```



```
CALL[User32! GetDlgItemTextA]
```

数字 40A680 引起了我们的注意,看看那里有什么:

```
:d 40a680
```

如果没有我们输入的名字,数据窗口里有些什么呢?好了,我们来研究下面的一段代码:

```
PUSH00
```

```
PUSH00
```

```
PUSH000003F6; 控制柄
```

```
MOV EDI, 0040A680; 保存缓冲区地址
```

```
PUSHESI ; 对话框
```

```
CALL[User32! GetDlgItemInt]
```

GetDlgItemInt 和 GetDlgItemText 差不多,但它从文字框中返回一个整数。它出在 EAX 中返回来的,所以单步运行通过这些代码,再来看看寄存器窗口,对我而言是:

```
EAX = 00003039
```

十六进制数 3039 是多少?输入:

```
:? 3039
```

我们得到:

```
000030390000012345"09"
```

```
^ 16 进制 ^ 十进制 ^ ASCII
```

正如你看到(和已经猜到)的那样,它是你输入的注册码。OK,下面怎么办?让我们来看下面的代码:

```
MOV [0040A548], EAX ; 返回注册码
```

```
MOV EDX,EAX;同时保存在 DX 中
```

3. 计算注册码

这样:注册码就算出来了

```
MOV ECX, FFFFFFFF; 这几行计算字符长度
```

```
SUB EAX, EAX; .
```

```
REP NZ SCASB ; .
```

```
NOT ECX ; .
```

```
DEC ECX ; ECX ← - 长度
```

```
MOVSXEAX, BYTE PTR [0040A680]; 读入 40A680 处的一字节
```

```
IMULECX, EAX; ECX = ECX * EAX
```

```
SHL ECX, 0A ; 左移 0A 次
```

```
ADD ECX, 0002F8CC; 结果加上 2F8CC
```

```
MOV [0040A664], ECX
```

验证合法性……

```
CMP ECX, EDX; 比较
```



JZ00402DA6; 如果相同就……

当你运行到比较这一步时,就可以得到你真正的注册码:

```
:? ecx
```

对我而言它是:

```
000DC0CC0000901324
```

也就是说我的正确的注册码是 901324。

按 F5 或者 Ctrl + D 让它运行,然后用正确的注册码(十进制)再来一次。这一次成功了!

3.8 Win API 函数与中断点设置技巧

通过前面章节的学习,大家会注意到,使用动态分析跟踪技术破解软件,最常用到的手段就是设置程序中断点找出关键程序段,然后逐行执行命令语句,分析代码直至找到所需要的信息。因此,设置最合理的中断点,便成为破解关键。在 3.5 节中介绍“F12”的应用时,曾经提到过,因为程序的作者用的是高级语言,Windows 又是提倡“透明”,不希望程序员知道底层的操作,而只提供给他们高层的接口,而相当多的高级函数调用某个一定的底层函数,所以我们通常用 SoftICE 在某些底层的 Windows 函数上设中断点。这一小节,我们就重点说说组成 Windows 编程接口的底层函数以及中断点设置技巧。

3.8.1 基本 Win API 函数

API(Application Programming Interface)就是 Windows 应用程序设计接口的意思。API 是一个程序内(或一组相关程序内)的一组函数调用,程序员用它创建其他程序。不必知道函数内部,只要知道函数原型及返回值。将一组函数转入 API 的问题实质是此函数提供每个人可使用的技术规范资料。Windows API 大概是今天世界上最著名的 API 了。现在 API 已发展到了 Win32 API。

API 是一些用 C 语言编写、由操作系统自身调用的函数。Windows API 函数由许多“动态链接库”或 dll 组成。在 32 位 Windows 中,核心的 Windows API .DLL 有如下一些:

gdi32. dll——图形显示界面的 API

kernel32. dll——处理低级任务(比如内存和任务管理)的 API

user32. dll——处理窗口和消息(Visual Basic 程序员能把其中一些当作事件访问)的 API

还不断有新的 API 出现,处理新的操作系统扩展,比如 E-MAIL、联网和新的外设。由于 Windows API 函数不是 Visual Basic 的内部函数,所以在使用它们之前必须显式地加以声明。要想得到正确格式化的函数声明,可以访问 WinAPI 目录下的文件 Win32API. txt。

1. 限制程序功能函数

EnableMenuItem 允许、禁止或变灰指定的菜单条目

EnableWindow 允许或禁止鼠标和键盘控制指定窗口和条目(禁止时菜单变灰)



2. 对话框函数

CreateDialog 从资源模板建立一非模态对话框
CreateDialogParam 从资源模板建立一非模态对话框
CreateDialogIndirect 从内存模板建立一非模态对话框
CreateDialogIndirectParam 从内存模板建立一非模态对话框
DialogBox 从资源模板建立一模态对话框
DialogBoxParam 从资源模板建立一模态对话框
DialogBoxIndirect 从内存模板建立一模态对话框
DialogBoxIndirectParam 从内存模板建立一模态对话框
EndDialog 结束一模态对话框
MessageBox 显示一信息对话框
MessageBoxEx 显示一信息对话框
MessageBoxIndirect 显示一定制信息对话框
GetDlgItemInt 得指定输入框整数值
GetDlgItemText 得指定输入框输入字符串
GetDlgItemTextA 得指定输入框输入字符串
Hmemcpy 内存复制（非应用程序直接调用）

3. 磁盘处理函数

GetDiskFreeSpaceA 获取与一个磁盘的组织有关的信息,以及了解剩余空间的容量
GetDiskFreeSpaceExA 获取与一个磁盘的组织以及剩余空间容量有关的信息
GetDriveTypeA 判断一个磁盘驱动器的类型
GetLogicalDrives 判断系统中存在哪些逻辑驱动器字母
GetFullPathNameA 获取指定文件的详细路径
GetVolumeInformationA 获取与一个磁盘卷有关的信息
GetWindowsDirectoryA 获取 Windows 目录的完整路径名
GetSystemDirectoryA 取得 Windows 系统目录(即 System 目录)的完整路径名

4. 文件处理函数

CreateFileA 打开和创建文件、管道、邮槽、通信服务、设备以及控制台
OpenFile 这个函数能执行大量不同的文件操作
ReadFile 从文件中读出数据
ReadFileEx 与 ReadFile 相似,只是它只能用于异步读操作,并包含了一个完整的回调
WriteFile 将数据写入一个文件
WriteFileEx 与 WriteFile 类似,只是它只能用于异步写操作,并包含了一个完整的回调
SetFilePointer 在一个文件中设置当前的读写位置
SetEndOfFile 针对一个打开的文件,将当前文件位置设为文件末尾



CloseHandle 关闭一个内核对象。其中包括文件、文件映射、进程、线程、安全和同步对象等

_lcreat 创建一个文件

_lopen 以二进制模式打开指定的文件

_lread 将文件中的数据读入内存缓冲区

_lwrite 将数据从内存缓冲区写入一个文件

_llseek 设置文件中进行读写的当前位置

_lclose 关闭指定的文件

_hread 将文件中的数据读入内存缓冲区

_hwrite 将数据从内存缓冲区写入一个文件

OpenFileMappingA 打开一个现成的文件映射对象

CreateFileMappingA 创建一个新的文件映射对象

MapViewOfFile 将一个文件映射对象映射到当前应用程序的地址空间

MapViewOfFileEx(内容同上)

CreateDirectoryA 创建一个新目录

CreateDirectoryExA 创建一个新目录

RemoveDirectoryA 删除指定目录

SetCurrentDirectoryA 设置当前目录

MoveFileA 移动文件

DeleteFileA 删除指定文件

CopyFileA 复制文件

CompareFileTime 对比两个文件的时间

SetFileAttributesA 设置文件属性

SetFileTime 设置文件的创建、访问及上次修改时间

FindFirstFileA 根据文件名查找文件

FindNextFileA 根据调用 FindFirstFile 函数时指定的一个文件名查找下一个文件

FindClose 关闭由 FindFirstFile 函数创建的一个搜索句柄

SearchPathA 查找指定文件

GetBinaryTypeA 判断文件是否可以执行

GetFileAttributesA 判断指定文件的属性

GetFileSize 判断文件长度

GetFileTime 取得指定文件的时间信息

GetFileType 在给出文件句柄的前提下,判断文件类型

5. 注册表处理函数

RegOpenKeyA 打开一个现有的注册表项

RegOpenKeyExA 打开一个现有的注册表项

RegCreateKeyA 在指定的项下创建或打开一个项



RegCreateKeyExA 在指定项下创建新项的更复杂的方式

RegDeleteKeyA 删除现有项下方一个指定的子项

RegDeleteValueA 删除指定项下方的一个值

RegQueryValueA 获取一个项的设置值

RegQueryValueExA 获取一个项的设置值

RegSetValueA 设置指定项或子项的值

RegSetValueExA 设置指定项的值

RegCloseKey 关闭系统注册表中的一个项(或键)

6. 时间处理函数

CompareFileTime 比较两文件时间

GetFileTime 得文件建立,最后访问,修改时间

GetLocalTime 得当前本地时间

GetSystemTime 得当前系统时间

GetTickCount 得 Windows 启动至现时毫秒

SetFileTime 设置文件时间

SetLocalTime 设置本地时间

SetSystemTime 设置系统时间

7. 进程函数

CreateProcessA 创建一个新进程

ExitProcess 以干净的方式关闭一个进程

FindExecutableA 查找与一个指定文件关联在一起的程序的文件名

FreeLibrary 释放指定的动态链接库

GetCurrentProcess 获取当前进程的一个伪句柄

GetCurrentProcessId 获取当前进程一个唯一的标识符

GetCurrentThread 获取当前线程的一个伪句柄

GetExitCodeProcess 获取一个已结束进程的退出代码

GetExitCodeThread 获取一个已结束线程的退出代码

GetModuleHandleA 获取一个应用程序或动态链接库的模块句柄

GetPriorityClassA 获取特定进程的优先级别

LoadLibraryA 载入指定的动态链接库,并将它映射到当前进程使用的地址空间

LoadLibraryExA 装载指定的动态链接库,并为当前进程把它映射到地址空间

LoadModule 载入一个 Windows 应用程序,并在指定的环境中运行

TerminateProcess 结束一个进程



3.8.2 中断点设置技巧

设置正确的 SoftICE 的断点,无论是 CRACK 软件还是调试软件都是非常重要的。虽然一些 CRACK 教学文件里有教,但往往不够全面,用的时候无从找起。现在整理出这篇断点集合,分门别类,方便大家查阅。

一般处理 bpx hmemcpy

bpx MessageBox

bpx MessageBoxExA

bpx MessageBeep

bpx SendMessage

bpx GetDlgItemText

bpx GetDlgItemInt

bpx GetWindowText

bpx GetWindowWord

bpx GetWindowInt

bpx DialogBoxParamA

bpx CreateWindow

bpx CreateWindowEx

bpx ShowWindow

bpx UpdateWindow

bmsg xxxx wm_move

bmsg xxxx wm_gettext

bmsg xxxx wm_command

bmsg xxxx wm_activate

时间相关 bpint 21 if ah == 2A (DOS)

bpx GetLocalTime

bpx GetFileTime

bpx GetSystemtime

CD-ROM 或 磁盘相关 bpint 13 if ah == 2 (DOS)

bpint 13 if ah == 3 (DOS)

bpint 13 if ah == 4 (DOS)

bpx GetFileAttributesA

bpx GetFileSize

bpx GetDriveType

bpx GetLastError

bpx ReadFile



bpio -h (Your CD-ROM Port Address) R
软件狗相关 bpio -h 278 R
bpio -h 378 R
键盘输入相关 bpint 16 if ah == 0 (DOS)
bpint 21 if ah == 0xA (DOS)
文件访问相关 bpint 21 if ah == 3dh (DOS)
bpint 31 if ah == 3fh (DOS)
bpint 21 if ah == 3dh (DOS)
bpx ReadFile
bpx WriteFile
bpx CreateFile
bpx SetFilePointer
bpx GetSystemDirectory
INI 初始化文件相关 bpx GetPrivateProfileString
bpx GetPrivateProfileInt
bpx WritePrivateProfileString
bpx WritePrivateProfileInt
注册表相关 bpx RegCreateKey
bpx RegDeleteKey
bpx RegQueryValue
bpx RegCloseKey
bpx RegOpenKey
注册标志相关 bpx cs:eip if EAX == 0
内存标准相关 bpmb cs:eip rw if 0x30:0x45AA == 0
显示相关 bpx 0x30:0x45AA do “d 0x30:0x44BB”
bpx CS:0x66CC do “? EAX”



第四章 静态反汇编三剑客—— “W32Dasm”、“HIEW”、“IDA”

前面章节提到过的静态分析是一项十分重要的破解技术,说它的作用不亚于动态跟踪技术一点不过分。所谓静态分析就是从反汇编出来的程序清单上分析。从提示信息入手进行分析,目前大多数软件在设计时,都采用了人机对话方式。所谓人机对话,即在软件运行过程中,需要由用户选择的地方,软件即显示相应的提示信息,并等待用户按键选择。而在执行完某一段程序之后,便显示一串提示信息,以反映该段程序运行后的状态,是正常运行,还是出现错误,或者提示用户进行下一步工作的帮助信息。为此,如果我们对静态反汇编出来的程序清单进行阅读,可了解软件的编程思路,以便顺利破解。常用的静态分析工具是“W32DASM”、“IDA”和“HIEW”。下面我们一一介绍。

4.1 W32Dasm

W32Dasm 是一个强大的反汇编工具,操作简单,使用方便。通常被程序员使用,当然也可被用来 Crack 软件了,很适合 Cracker 使用。我在这里把与 Crack 相关的功能简述如下:

开始

- ▶反汇编文本代码的基本操作
- ▶复制汇编代码文本
- ▶装载 32 位的汇编代码动态调试
- ▶运行,暂停或终止程序
- ▶单步跟踪程序
- ▶设置激活断点
- ▶偏移地址和虚拟地址转换

4.1.1 开始

运行 W32Dasm,在这里以 Windows95 自带的计算器为例:calc.exe。从 Disassembler(反汇编)菜单选择 Disassembler Options(反汇编程序选项)选项,将出现如下对话框图 4-1 所示:

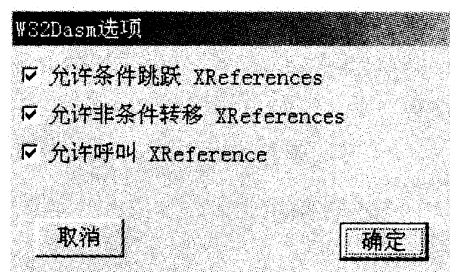



图 4-1




Pc friend ·


在 Disassembler(反汇编)菜单,选择 Open File(打开文件)选项或按工具栏按钮 , 选择你要打开的文件就可。注意:你反汇编文件后,如字符已超过屏幕外,这时你要选择合适的字体(在 Font 字体选项中 Select Font 选择字体),然后设为默认字体(Save Default Font)即可。当然一般以默认值就可。之后保存反汇编文本文件和创建方案文件(Save The Disassembly Text and Create A Project File)。

4.1.2 反汇编源代码的基本操作


1. 转到代码开始(Goto Code Start)

在工具栏按  图标或从菜单的转到(Goto)选项选择转到代码开始(Goto Code Start) 或按 Ctrl + S, 这样光标将来到代码的开始处,用户可通过双击鼠标或用 shift + 上下光标键改变光标的位置。

2. 转到程序入口点(Goto Program Entry Point)

在工具栏按  图标或菜单的转到(Goto)选项选择 转到程序入口点(Goto Program Entry Point)或按 F10,这样光标将来到程序入口点(Entry Point),这里就是程序执行的起始点,一般动态调试时 LOAD 时也就停在此处。

3. 转到页(Goto Page)

在工具栏按  图标或菜单的转到(Goto)选项选择转到页(Goto Page)或按 F11,这时跳出一对话框,如图 4-2 的图标,输入页数可跳转到相关页面去。

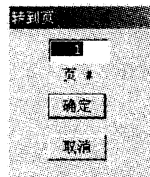



图 4-2

4. 转到代码位置(Goto Code Location)

在工具栏按  图标或菜单的转到(Goto)选项选择转到代码位置(Goto Code Location)或按 F12,一个对话框将出现,如图 4-3 所示,允许用户输入代码偏移地址,以跳转到此位置上去。

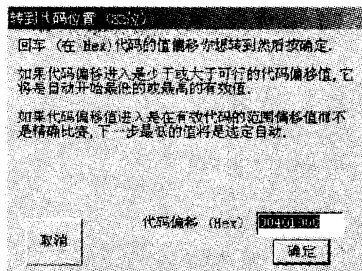



图 4-3

此时工具条 Jump To 按钮 , 也激活,如图 4-4:

此时按如图 4-4 按钮或菜单选项 Execute Jump(执行跳跃)或按右光标键,光条将来到跳转指令所指到的位置。在这例子里,将来到:

5. 执行文本跳转(Execute Text Jump)

这功能是在 Execute Text(执行文本)菜单选项里的,执行跳跃 (Execute Jump)功能激活条件是光标在代码的跳转指令 这行上 (这时光条是高亮度的

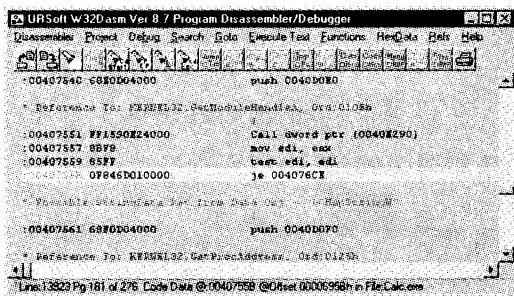


图 4-4



004076CE xor eax,eax 这一行代码处,如图 4-5 所示:

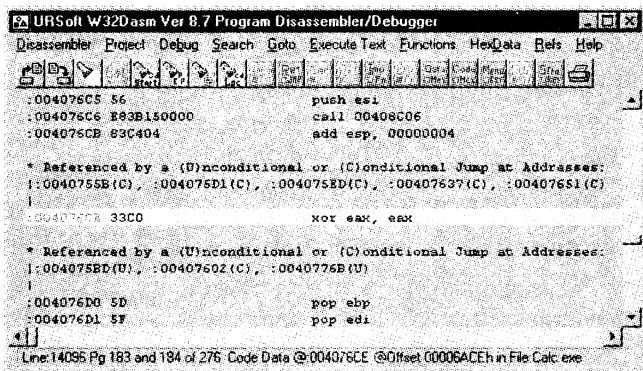


图 4-5

6. 返回到上一次跳跃 Return From Last Jump

这功能是在 Execute Text(执行文本)菜单选项里的,此指令仅仅是在 执行文本跳转功能完成后才激活。当这条件成立时,按钮 将激活。按 按钮或在菜单里选项返回到上一次跳跃(Return From Last Jump)或按左光标键,光条将返回到上一次跳跃位置处。

7. 执行呼叫 Execute Text Call

这功能是在 Execute Text(执行文本)菜单选项里的,此功能激活的条件是光条在 CALL 指令一行。在这一行时光条将发绿,按钮 将激活。执行时光条将会来到 CALL 所指的地址处。如下图 4-6: 光条在 0040751D call 004073D4 一行。

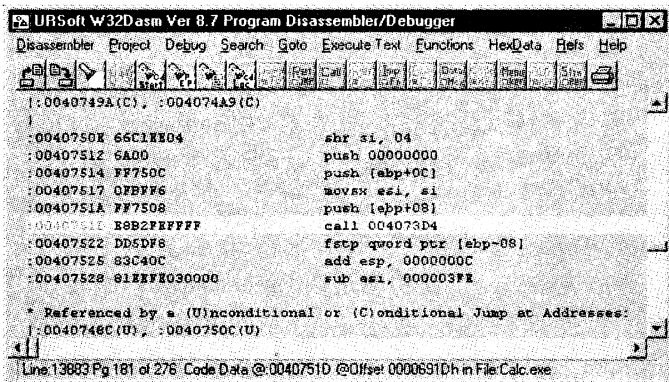


图 4-6

此时 按钮或在菜单的执行呼叫(Execute Text Call)或按右光标键,光条将来到 CALL 所指的地址 004073D4 这一行,如图 4-7 所示。

8. 返回呼叫(Return From Last Call)

这功能是在 Execute Text(执行文本)菜单选项里的,此指令仅仅是在执行呼叫 Execute Text Call 功能完成后才激活。当这条件成立时,按 按钮或在菜单里选项返回呼叫(Return From

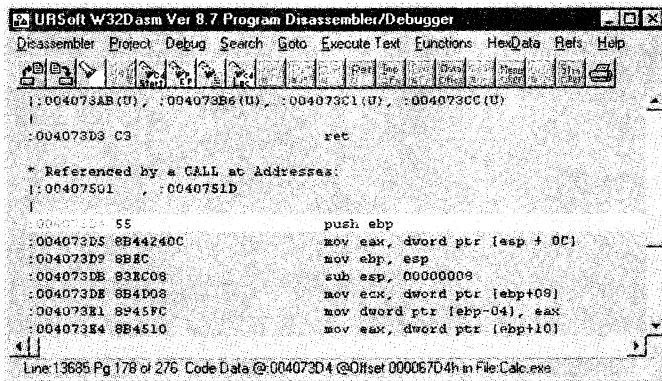



图 4-7

Last Call)或按左光标键,光条将返回到上一次呼叫位置处。

9. 导入功能(Imported)

在菜单功能选项里,其作用主要是查看 import 函数。按  按钮或在菜单功能选项里的导入(Imports)命令,执行后将列出当前文件的 Import 函数。如图 4-8:

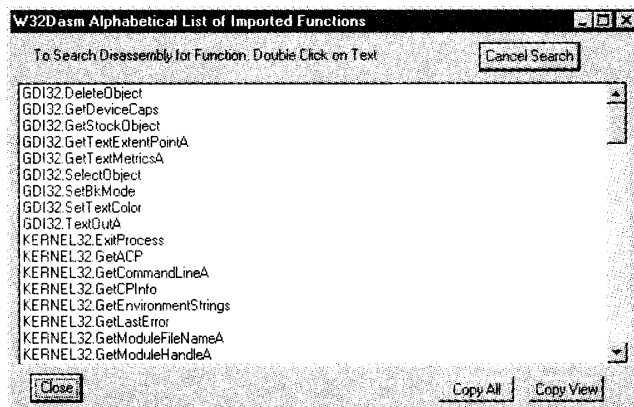


图 4-8

你可双击这些项目,光条将来调用这些函数的代码处。

注意:如果代码多处引用了这些函数,你双击这个项目函数时,光条将在调用了其的几个位置代码处循环。

你也可用 copy all 或 copy view 复制 import 函数。

10. 出口功能(Exported)

在菜单功能选项里,其作用主要是查看 Export 函数。按  按钮或在菜单功能选项里的出口(Exports)命令,执行后将列出当前文件的 Exports 函数。

注意:一般 EXE 文件没有 exported, DLL 文件有 exported 函数。

11. 裁判(References)

在这个菜单选项里有菜单参考(MENU), 对话参考(DIALOG) or (串式数据参考 STRING



DATA), 分别对应按钮: 、、.

注意:其中(串式数据参考 STRING DATA)功能破解时很常用。

4.1.3 复制汇编代码文本

W32dasm 允许打印或复制指定行的汇编代码。首先你将鼠标移到 W32DASM 的最左边单击,将会出现一个小红点,再按住 Shift 键,移到你需要的下一行,再单击鼠标一下,将选中一段,按 CTRL + C 复制或 在菜单选项反汇编里的拷贝指定的行(Copy Lines of Text)功能或按 ,把数据复制到剪贴板里。如图 4-9 所示:

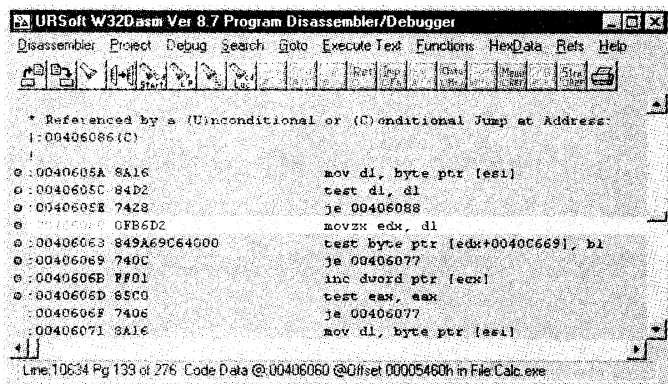


图 4-9

4.1.4 装载 32 位的汇编代码动态调试

反汇编 Windows 自带的计算器程序 calc.exe。选择菜单调试选项中的加载处理(Load Process),或按 Ctrl + L 键出现一个加载对话框,你可输入选项命令。现在你可按装载(load)按钮。Calc.exe 现在被 W32DASM 动态调试,将出现左右两个调试窗口(如下图)。在初始化 calc.exe 程序后,指令将停留在入口点(Entry Point)处。图 4-10 的调试窗口列出各种状态器如:CPU 寄存器,CPU 控制寄存器,断点,活动的 DLL,段寄存器等。

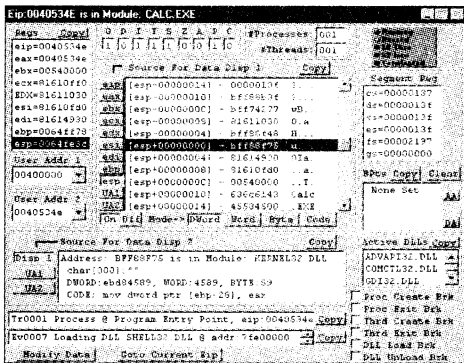


图 4-10

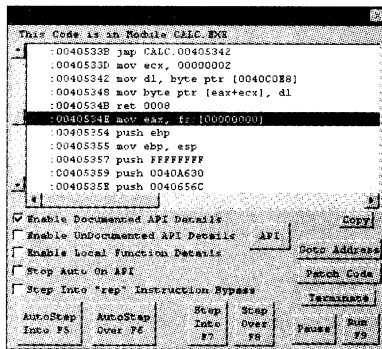


图 4-11



4.1.5 运行,暂停或终止程序

在图 4—11 调试窗口,按运行(Run)按钮或按 F9, calc. exe 将运行起来。按暂停(Pause)按钮或空格键,程序将暂停,这在单步跟踪时经常用到。按终止(Terminat)按钮,程序将停止,退出动态调试环境。

4.1.6 单步跟踪程序

重新加载 calc. exe,在程序加载后,停留在入口点,你可按 F7 或 F8 单步调试程序,这两个键所不同的是 F7 是跟进 CALL 里, F8 是路过。进入自动调试按 (F5) 和结束自动调试按 (F6)。

4.1.7 设置激活断点

重新加载 calc. exe,在 W32DASM 的菜单转到选项转到代码处(goto code)功能,填上 403198,按确定,你将在 W32DASM 的主窗口(此时可能最小化了,把其还原即可)来到 403198 地址一行。光条在这一行明亮绿色,按 F2 或用鼠标左点击最左边(同时按住 Ctrl)设置断点。

这时如断点设置成功,光条最左边有一小段黄条,显示此行为断点。如图(4-12):

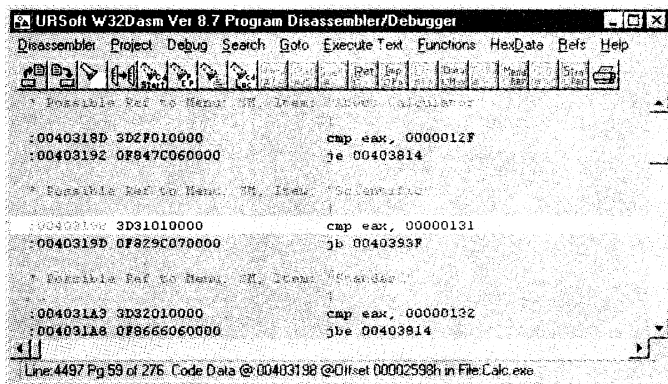


图 4-12

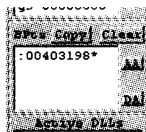


图 4-13

如果断点不在这里,整行光条将是黄色的。当断点设置好后,在左调试窗口中的断点小窗口显示断点情况,如图 4-13(右边有一*):

此时按 F2 或鼠标左键 + Ctrl,断点将取消。此时按 F9 程序将运行到相关断点时停止。

4.1.8 偏移地址和虚拟地址转换

偏移地址(File offset)和虚拟地址的关系是:虚拟地址 = 偏移地址 + 基址(ImageBase),基址



在 Windows NT 中,缺省的值是 10000h;对于 DLL,缺省值为 400000h。在 Windows 95 中,缺省基地址为 400000h。其实你用 W32DASM 打开文件,在开始处就会有一句 Imagebase = 00400000h,这就是基址,有可能部分应用软件的基址不是 00400000h。了解它们的关系后,可利用此公式快速换算偏移地址和虚拟地址。

W32DASM、SOFTICE 和 Hiew(Decode 模式)显示的地址都是虚拟地址,但是在 Hiew(Decode 模式)下,F5 功能键查找的地址是偏移地址,因此必须将虚拟地址转换成偏移地址,才能找到正确的地址。除了上面的公式外,常用的方法是在 W32DASM 下将绿色的光条移到某一行代码上,在窗口底部有一行字指示其偏移地址,如虚拟地址:Code DaTa @ 0040534e 而偏移地址为:@ Offset 0000474Eh。这就是偏移地址。如图 4-14。

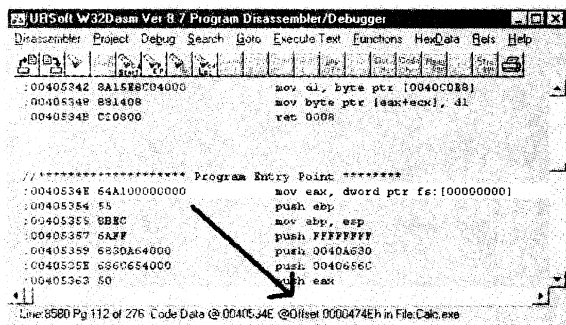


图 4-14

4.2 Hiew 简要说明

1. 运行

在 Hiew 目录找到 Hiew.exe,运行它,这时 Hiew 界面出现的是 Hiew 目录文件,如图 4-15。

此时在屏幕底部的命令行有相关提示,对应的是功能键 F(n),如按 F1 出现的帮助:

F2 - Hidden - 打开或关闭隐藏文件显示

F3 - Name - 按文件排序

F4 - Exten - 按扩展名排序

F5 - Time - 按文件时间排序

F6 - Size - 按文件大小排序

F7 - Unsort - 不排序

F8 - Revers - 反转排序

F9 - Files - 查看曾打开的文件历史

F10 - Filter - 设置过滤

Ctrl\ - 来到驱动器的根目录

CtrlPgUp - 回到上一目录

Insert - 打开/创建文件

[printable char] - fast search filename

* - next fast search

Tab - attempt to perform complete filenameAltF1 - Drive - 选择驱动器

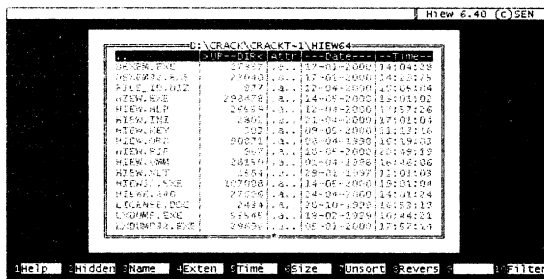


图 4-15



AltF2 - Drive - 选择驱动器
 AltF4 - ReRead - 重新读取目录文件
 CtrlF1 - Store1 - store current path 1
 CtrlF2 - - retrieve stored path 1
 CtrlF3 - Store2 - store current path 2
 CtrlF4 - - retrieve stored path 2
 CtrlF5 - Store3 - store current path 3
 CtrlF6 - - retrieve stored path 3
 CtrlF7 - Store4 - store current path 4
 CtrlF8 - - retrieve stored path 4
 CtrlF9 - Sta__ - toggle save state in next file
 CtrlF10 - Home - go home dir
 回车键 - 可进入子目录或从子目录退出

2. 基本操作

(1)参考上表操作,打开你需要修改的文件。

(2)此时按 F1,屏幕又会出现相关的帮助信息。

(3)打开文件后,观察屏幕底部的 4 (Mode),此时按 F4,将出现一对话框,让你选择 Text(文本), Hex(十六进制)和 Decode(反汇编)模式。

(4)此时你可根据需要选择相关的模式。在这里我们以 Decode(反汇编)模式为例,在此模式下,将出现汇编代码,你可修改这些代码。现在按 F3 (Edit)将进入编辑模式,按 F5 (Goto)将跳到指定的地址(注:是偏移地址,具体请参考上一节 W32DASM 的相关描述),按 F7 (Search)是查找 ASCII 码或十六进制数据。

(5)F3 (Edit)将进入编辑模式后,移动光标到相应的行,按 F2 或回车键,跳出一对话框,可修改汇编代码。修改好后,F9 存盘(按回车后到下一行,再按 Esc 让对话框消失,然后按 F9)。

4.3 关于 IDA 与 W32DASM 的比较

IDA Pro Avanced 是一个极好的反汇编工具,它在某些方面甚至胜过了 w32dasm。对于 w32dasm 来说,通常菜鸟不喜欢,而高手又崇拜它。不喜欢的原因是因为 IDA 相对于 W32DASM 来说有更多的附加功能和作用,有更大的复杂性

当你运行 IDA Pro 时,你所最先注意到的是它的界面比 W32DASM 更加专业,这里比 W32DASM 有更多的选项或更先进的地方。它的优点是可以更好的反汇编和更有深层分析。而缺点是使用 IDA 更困难。

实际上 IDA 同 W32DASM 有很多相同的功能:可以快速到达指定的代码位置;可以看到跳到指定的位置的 jmp 的命令位置;可以看参考字符串;可以保存静态汇编等。



在 IDA 中另一个同 W32DASM 近似的是十分简单的,如:“Goto code location”等同于在 IDA “Jump - Jump to adress”。或者 “Goto entrypoint”等同于在 IDA “Jump - Jump to entry point”。

IDA 优点:

- (1)能够对 W32DASM 无法反汇编的最难的软件进行反汇编(如加壳程序)
- (2)能够以 .asm .sym 和甚至是 .exe 及其它文件形式保存
- (3)压缩的静态汇编,可以节省大量的磁盘空间。
- (4)可以重命名函数
- (5)能够分析巨大的程序

有人会问:如果 IDA 这么好看,为什么我还要使用 W32DASM?”下面就是对于这个疑问的解释:

首先是速度,对于 IDA 来分析一个小程序是非常非常的快,但是如果分析一个大的 exe 它就要花费 3 个小时或更多的时间来全面分析 exe。其次,如果你对于一个指定的搜索,IDA 将很慢的,而在 W32DASM 中在文本方面中搜索是很快的。第三,当分析一个仅有简单的保护的程序时,W32DASM 就为的首选。因为你就不需要 IDA 那些附加的功能了。

4.4 破解实例

对象程序:Crackme

破解工具:W32DASM, HIEW;

1、思路提示:首先试运行要破解的程序,了解一些提示信息,如:文本/NAG 屏(警告窗口)/按钮等等。最重要的就是出错信息,如:“Wrong serial……”记下,因为你在后面要用到它,你需要它来找到 CALL 出错 messagebox 的地方。当 W32DASM 反编译后你会看到一屏幕难懂的汇编码。你还记得刚要你记下的那个 message 么?此时单击在工具栏里的串式数据参考 SDR (=String Data Reference),这个功能可是非常有用的。

在串式数据参考 SDR 中找到那个提示信息(它也许只显示了信息的一部分),此时双击它,来到相关代码处,再分析源代码。

(2)运行 Crackme,输入假的序列号,点击 Check,出现错误提示:“Incorrect try again!!”记下。

(3)将 Crackmer 备份一份,用 W32DASM 反汇编它。

(4)一旦完成反汇编,点串式数据参考(string data reference)按钮,在列出的字符串列表中找到“Incorrect try again!!”并双击它。(注:如代码中有多处有此字串,你再次双击后,光标将出现在下一代码上)

(5)关闭这个窗口回到主窗口,你应该能够看到下面这一行:

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

|:00401595(C)

|



Pc friend ·

:004015AD 6A40push 00000040

* Possible StringData Ref from Data Obj →“CrackMe”//错误提示窗口的标题

|

:004015AF 686C304000push 0040306C

* Possible StringData Ref from Data Obj →“Incorrect try again!”//错误提示处,我们来到这一行

|

:004015B4 6874304000push 00403074

:004015B9 8B4DE0mov ecx, dword ptr [ebp - 20]

(6)现在你必须从这行起向上找,直到找到有这样的命令为止:cmp,jne,je,test 等等。

CMP = 比较(如 CMP EAX, EBX) ← 比较 EAX 和 EBX

JE = 如果相等就跳转

JNE = 如果不相等就跳转

JL = 如果小于就跳转

JLE = 如果小于等于就跳转

JA = 如果大于就跳转

JAE = 如果大于等于就跳转

JMP = 无条件跳转

(7)注意这一行代码:

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

|:00401595(C)

|

:004015AD 6A40push 00000040

:00401595(C) 是代码位置而不是 offset,表示指令由 00401595 一行跳转到此。此时你再利用菜单的转到代码位置功能或按 Shift + F12,在对话框中输入:00401595,你将来到此:

:00401585 8D4DE4lea ecx, dword ptr [ebp - 1C]

:00401588 51push ecx

:00401589 8D55F4lea edx, dword ptr [ebp - 0C]

:0040158C 52push edx

* Reference To: KERNEL32.lstrcmpA, Ord:02FCh

|

:0040158D FF1500204000Call dword ptr [00402000]

:00401593 85C0test eax, eax

:00401595 7516jne 004015AD

(8)上面这段代码和第五课的一样,此时你借助 SOFTICE 动态调试能很快找到序列号,在这里我们今天用暴力法破解,注意:

:0040158D FF1500204000Call dword ptr [00402000]//真假序列号比较核心(调用函数



lsrmpa 比较)

```
:00401593 85C0test eax, eax//用 eax 当旗帜,如相等,则 eax = 0
```

```
:00401595 7516jne 004015AD//如不跳转则注册成功
```

看明白了吗? 要让程序接受任何注册码就只要把 JNE(= 不相等就跳) 改成 JE(= 相等就跳), 或改成空指令 NOP(什么也不执行), 这样前一个改法要注册就只能输入错误的注册码, 后者可任意注册码。

(9)将绿色的光条移到:00401595 7516 jne 004015AD 上,在窗口底部有一行字指示这句命令的偏移地址,此处为@ Offset 00001595h. 这就是应该修改的地方了。

(10)启动 hiew, 打开 crackme. exe, 按 F4, 然后选择 decode mode, 按 F5 输入偏移地址 1595(@ Offset 00001595h)。你应该看到下面这几行:

```
?00401593: 85C0 test eax, eax
```

```
?00401595: 7516 jne .0004015AD
```

(11)这就是修改的地方了,按 F3 进入修正状态,在机器码处直接用 7416 代替 7516,按 F9 存盘。或在这一行按 F2 或回车进入小汇编修改状态,输入正确的指令。

(12)第二种修改方法是用两个 NOP 指令(NOP 指令机器码是 90,是一个字节)代替机器码: 7516,即改为:9090

(13)运行 crackme,随便输入几个字符试试,成功了!(当然这只是对那些简单的程序有效。



第五章 注册表破解技巧浅析

通过反汇编直接跟踪调试程序的方法虽然比较有效,可花费的时间和精力也是最多的。其实有的软件根本就不需要反汇编也可以破解,那就是修改注册表。假如你正准备 Crack 一个软件,那就不妨先试试这个方法,对大多数软件来说,基本上都能将其破解。要掌握这种方法,首先要熟悉注册表的体系结构和基本操作,下面就分类来探讨一下吧。

5.1 注册表的备份

我之所以把注册表的备份放在开头来讲,主要是因为注册表是 Windows 95 及 Windows 98 的核心数据库,表中存放着各种参数,直接控制着 Windows 的启动、硬件驱动程序的装载以及一些 Windows 应用程序运行的正常与否,如果该注册表由于某种原因受到了破坏,轻者使 Windows 的启动过程出现异常,重者可能会导致整个 Windows 系统的完全瘫痪。因此正确地认识、修改、及时地备份以及有问题时恢复注册表,对 Windows 用户来说就显得非常重要了。

这里我郑重地提醒大家,在改动注册表前务必进行备份,以防不测。假如系统因为注册表的改动而不能正常启动时,可在 DOS 方式下运行 Scanreg/Restore,以恢复注册表(其实 Windows 在每次启动成功时都会备份注册表, System.dat 备份为 System.da0, User.dat 备份为 User.da0,文件存放在 Windows 所在文件夹,属性为系统与隐藏)。常用的注册表备份方法和工具很多,大家可以根据个人情况选择一个。如利用注册表编辑器中的“导出注册表文件”即可导出一份扩展名为 .REG 的文件。不过你也可以利用 Windows 光盘上 Other\Misc\ERU\ERU.EXE 紧急事故恢复工具(Emergency Recovery Utility)。该工具小巧,功能却不错,很实用,可以备份 system.ini、win.ini、msodos.sys、System.dat 等所有的系统文件。使用方法很简单,运行 ERU,选择一路径(默认是 A 盘)如:C:\ERD 备份,以后如需恢复,则在 DOS 下进入 C:\erd 目录,运行 ERD,就可完整恢复整个系统配制文件的还原。是不是很简单?这也是我向你推荐的原因。

一般在对付一个软件之前,应该先备份一下注册表,然后才安装该软件。这样做有两个原因,一是:因为你在破解某些软件有这种情况,寻找关键点时,在这时改动某一代码以验证自己的判断(如:reax,0),这时正确注册成功,此时你再想回到那里看究竟,重装该软件都没用,我们在第二章中讲过的,除非你重装系统。此时你只要还原注册表和配制文件,再重装该软件,又可注册了。当然这种情况少见,但还是有的。二是如果跟踪调试不能成功,只好分析注册表了,所以事先备份是很明智的选择。

当然,如果你觉得这样备份还不妥当的话,你可以备份整个 Windows 系统,本文并不提倡这



样做,一是太麻烦,而是一般没必要,这里粗略地讲一下,目的是让你多了解一些方法。系统备份的方法很多,下面介绍两个常用的。

(1)在 Windows 下的 DOS 窗口用 xcopy 命令

`xcopy c:\windows*. * c:\winbak/s/e/h/k/y/c`,各参数意思大家用 `xcopy/?` 理解。这样你的系统就备份在 winbak 目录下了。注意:该命令需在 windows 的 dos 窗口下运行,因为你在纯 dos 下运行,xcopy 或 xcopy32 将不支持长文件名和 h 参数下的拷贝隐含和系统文件。

(2)打开资源管理器,选择菜单的“查看”→“选项”→“查看”,选中“显示所有文件”,也就是说在资源管理器下能查看所有的文件(系统、隐含、只读、等)。好,已完成一半了,然后进入 windows 目录,你会看到所有的文件,然后选定全部所有的文件(Ctrl + A)(是不是有人在笑,这招我早试过,不行)。哈,当然这样你复制系统不到一半就会保护性中断,到底是什么原因导致复制中断呢?我们知道 Windows 系统使用临时文件作为虚拟内存,明白了吧,关键在此,这文件是 WIN386.SWP,刚才复制到这个文件中断了,下面就简单了,在 Windows 下全选中后,找到 WIN386.SWP 文件,按住 Ctrl 键同时,用鼠标点一下,结果是除了这文件外别的都选中。然后复制到事先建好目录下。这样 Windows 系统备份结束,这时你比较两个目录大小不一样,没关系,因为你没复制 WIN386.SWP,所以有差别,这是临时文件,不影响系统完整。下次你要重装系统时只要在纯 DOS 下用 ren 命令改两个目录名称就行了。另外有一点要注意,我们没备份 C 盘根目录下的配制文件,最好备份一下,用 ERU 或手动。别看后罗罗唆唆说了一大堆,做起来,两下就解决。你完成备份后一定要验证一下,不然没有备份完全就死定了。验证方法:在纯 DOS 下用 REN 命令改目录名,如:ren windows win,ren winbak windows 即可,这里假设 winbak 是你刚备份的目录。

5.2 注册表结构分析

完成了注册表的备份,你就不会为你的系统无法启动而担心了。在“开始”菜单中,按“运行”按钮,键入 regedit 就可打开注册表。慢着!如果你还对注册表不熟悉的话,千万不要随便改动它。好,我们就来逐步的认识注册表的各项含义吧。

5.2.1 注册表的六大根键

在注册表中,所有的数据都是通过一种树状结构以键和子键的方式组织起来,十分类似于目录结构。每个键都包含了一组特定的信息,每个键的键名都是 和它所包含的信息相关的。如果这个键包含子键,则在注册表编辑器窗口中代表这个键的文件夹的左边将有“+”符号,以表示在这个文件夹中有更多的内容。如果这个文件夹被用户打开了,那么这个“+”就会变成“-”。

1. HKEY_USERS

该根键保存了存放在本地计算机口令列表中的用户标识和密码列表。每个用户的预配置信息都存储在 HKEY_USERS 根键中。HKEY_USERS 是远程计算机中访问的根键之一。

2. HKEY_CURRENT_USER



该根键包含本地工作站中存放的当前登录的用户信息,包括用户登录用户名和暂存的密码(注:此密码在输入时是隐藏的)。用户登录 Windows 98 时,其信息从 HKEY_USERS 中相应的项拷贝到 HKEY_CURRENT_USER 中。

3. HKEY_CURRENT_CONFIG

该根键存放着定义当前用户桌面配置(如显示器等)的数据,最后使用的文档列表(MRU)和其他有关当前用户的 Windows 98 中文版的安装的信息。

4. HKEY_CLASSES_ROOT

包含注册的所有 ole 信息和文档类型,是从 hkey_local_machine\software\classes 复制的。根据在 Windows 98 中文版中安装的应用程序的扩展名,该根键指明其文件类型的名称。

5. HKEY_LOCAL_MACHINE

该根键存放本地计算机硬件数据,此根键下的子关键字包括在 SYSTEM.DAT 中,用来提供 HKEY_LOCAL_MACHINE 所需的信息,或者在远程计算机中可访问的一组键中。

该根键中的许多子键与 System.ini 文件中设置项类似。

6. HKEY_DYN_DATA

该根键存放了系统在运行时的动态数据,此数据在每次显示时都是变化的,因此,此根键下的信息没有放在注册表中认识键和子键注册表通过键和子键来管理各种信息。但是,注册表中的所有信息是以各种形式的键值项数据保存下来。在注册表编辑器右窗格中,保存的都是键值项数据。这些键值项数据可分为如下三种类型:

(1) 字符串值

在注册表中,字符串值一般用来表示文件的描述、硬件的标识等。通常它由字母和数字组成,最大长度不能超过 255 个字符。通过键值名、键值就可以组成一种键值项数据,这就相当于 Win.ini、Syst - em.ini 文件中小节下的设置行。其实,使用注册表编辑器将这些键值项数据导出后,其形式与 INI 文件中的设置行完全相同。

(2) 二进制值

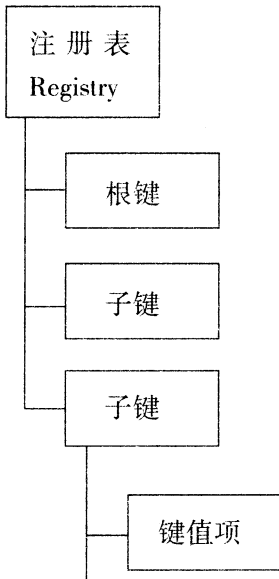
在注册表中,二进制值是没有长度限制的,可以是任意个字节长。在注册表编辑器中,二进制以十六进制的方式显示出来。

(3) DWORD 值

DWORD 值是一个 32 位(4 个字节,即双字)长度的数值。在注册表编辑器中,您将发现系统会以十六进制的方式显示 DWORD 值。在编辑 DWORD 数值时,可以选择用十进制还是 16 进制的方式进行输。

5.2.2 注册表的层次结构

注册表的体系结构呈树状的分层结构,操作起来相当方便。大致可以分成 4 个层次,如下图所示:



接下来对各个层次进行说明。

1. 根键:根键类似于硬盘上的根目录。Registry 有 4 个预定义的根键:

- (1) HKEY_LOCAL_MACHINE
- (2) HKEY_USERS
- (3) HKEY_CURRENT_USER
- (4) HKEY_CLASSES_ROOT

2. 键与子键:键和子键类似于文件管理器中看到的目录结构,在键下面是子键,就像目录可以包含子目录一样。

3. 键值项:键值项类似硬盘上树型目录的末端文件,键和子键可以包括一个或多个键值项。键值项由键值名、数据类型和键值三部分组成,其格式为:“键值名:数据类型:键值”。

4. 键值类型:Registry 中有如下三种键值类型:

DWORD 值:只允许一个键值,并且必须为 1-8 个 16 进制数据(即双字)。

字符串值:只允许一个键值,并且作为要存储的字符串来解释。

二进制值:只允许一个值,是 16 进制数字串,每对作为一个字节值解释。

5.3 注册表的文件组成

注册表 Registry 由 5 个文件组成的。

5.3.1 系统配置注册表文件 System.dat

在 Windows 98 的系统目录中有一个隐含、系统、只读文件 System.dat,它是 Windows 98 注



册表的一部分,该文件具有如下作用:

- 描述单一的 PC 配置。
- 描述安装在一单独的 PC 上的消息。
- 安装即插即用类型的设备硬件配置,如设备的 I/O 地址、IRQ 级和 DM A 通道等。

该文件的作用有点类似 Windows 3. x 中的 System. ini 文件。

该文件在 Windows 98 的网络运行状态时,保存在本地的工作站或本地 PC 机中。

在 Windows 98 安装期间,Setup 将检查您的计算机上已安装的硬件,然后在 System. dat 中建立适当的配置项。若从现有的 Windows 3. x 中安装 Windows 98,则 Setup 将把现有的 System. ini、Reg. dat 文件中的部分设置项拷贝到 System. dat 中,

在您使用“控制面板”的“系统”图标查看硬件配置时,其窗口中所显示的选项都是从 System. dat 中读取的,如图 5-1 所示。

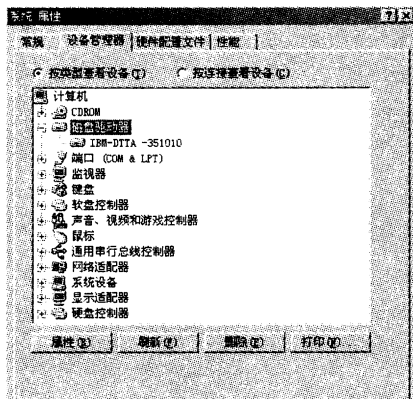


图 5-1

5.3.2 系统配置注册表备份文件 System. da0

Windows 98 注册表的一个主要特点就是可靠性强,不易损坏。这个特点靠的就是注册表有备份文件。

系统配置注册表 System. dat 的备份文件为 System. da0,该文件在 System. dat 文件遭到意外破坏时,将由系统自动拷贝为 System. dat。

5.3.3 用户平台配置注册表文件 User. dat

在 Windows 98 的系统目录中有一个隐含、系统、只读文件 User. dat,它也是 Windows 98 的注册表的一部分,该文件具有如下作用:

- 它定义用户优先权,如用户平台配置等。
- 特定于某一个用户的应用程序的安装信息。

该文件的作为类似于 Windows 3. x Win. ini 文件。

当您在 Windows 98 中使用网络时,User. dat 必须放在网络服务器上。

在您第一次输入用户标识和密码时,安装程序将把这些信息存储在 User. dat 中。您的 Windows 98 的序列号也存储在 USER. DAT 中。

如果用户在“控制面板”的“密码”图标中选择了“用户可自定义首选项及桌面设置登录时,Windows 自动启用个人设置”这个选项后(参见图 5-2),系统就会为每个用户创建他自己的 User. Dat,并且把它保存为 C:\Windows\Profiles\用户名\User. dat。用户每次登录后,他自定的 User. dat 会被调入到系统中。

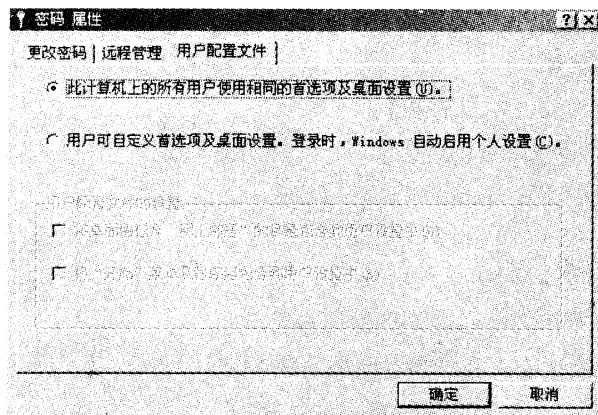


图 5-2

5.3.4 用户平台配置注册表备份文件 User. da0

用户平台配置注册表文件 User. dat 也有一个备份文件 User. da0。当 User. dat 遭到意外破坏时,将由系统将 User. da0 拷贝为 User. dat,从而使 User. dat 得到恢复。

5.3.5 网络管理注册表文件 Config. pol

若您在 Windows 98 安装了“系统策略编辑器”后,则可以使用 Config. pol 文件中的限制来决定系统如修改注册表,也就是说,系统根据 Config. pol 中的设置对网络用户的操作作一些限制,这种限制在 Windows 98 被称为“策略”。Config. pol 文件也是一个隐含、系统、只读文件,它主要用于 Windows 98 的网络用户的管理方面的策略。

5.3.6 网络管理注册表备份文件 Config. po0

同 System. dat、User. dat 有备份文件一样,Config. pol 也有一个备份文件 Config. po0,它是一个隐含、系统、只读文件。它存放在网络服务器中。

5.4 注册表分析工具

通过前面的学习,我们基本了解注册表的一些常识了,那么到底如何判断软件在注册表做过什么手脚呢?这里推荐两个工具给大家,用它什么问题都会迎刃而解:

一是:tianwei 的 RegShot ;

二是:Regsnap 2.6。

这两个工具都不错。它们可以详细地向你报告注册表及其他与系统有关项目的修改变化情



况。RegSnap 对系统的比较报告非常具体,对注册表可报告修改了哪些键,修改前、后的值各是多少;增加和删除了哪些键以及这些键的值。报告结果既可以纯文本的方式,也可以 html 网页的方式显示,非常方便。

RegShot 使用举例

很多软件为了防备 Cracker 们,在反跟踪、反调试方面都做了很多手脚,那我们就:不修改软件的代码,不反汇编它,甚至根本不跟踪它的运行,而只看看它留下什么脚印:)

- RegShot 的原理是这样的:在运行该软件之前作个记录,在运行它之后作个记录。比较二者的差别。很简单吧:)

- 最先前的工具是各类的反安装工具,如 CleanSweep 之类做得非常好,它能记录一个软件安装过程,如果您到了期限还想用,那么就反安装一次,再装一下就可以了。但问题在于,您有可能将有用的设置,辛苦的工作成果都给 Uninstall 了。而实际上您可以只改动很小的地方,就可以达到这样的效果。

- RegShot 的前辈是 RegSnap,一个非常好的软件,功能强。但 RegSnap 本身就是一个共享软件,有非常讨厌的不定时等待窗口,想知道怎么破解它,可以看看我的站台上的 oldnotes. htm 内有介绍。实际上,RegShot 的产生也是我见过 RegSnap 后才想到的:“这么点功能,要搞这么强的防护(指 RegSnap 对自身的效验),我自己写一个吧!”

以下是一个利用 RegShot 来狼吃狼的例子。所谓狼吃狼,是指此次的“样品”是个比较不“正派”的软件,是个跑 NT 密码的软件——LOphtCrack v2.5,但微软说这是个很好的 NT 密码安全性检测工具,而且这个软件现在也是以共享形式出现的,需注册,不注册只有 15 天的时限,而且时间到后,即使自身反安装,再安装一次也无用。

(1)首先,在安装前用 RegShot 做一次 Shot,按下“1stShot”按钮,如果您想附带对 system. ini, win. ini 进行监察的话请在按下按钮前选定“IncludeWin. ini…”复选框;如果您想存盘记录此次 Shot 的话,就选定“StoreKeys&values.”复选框。

(2)运行 LOphtCrack2.5 的安装程序。

(3)安装结束后,用 Regshot 再作一次 Shot,按“2ndShot”。

(4)用 RegShot 的“Compare”按钮,您会看到结果如下:

** Original contents Maybe deleted or modified **

H. L. K\SOFTWARE\Description\Microsoft\Rpc\UuidPersistentData\LastTimeAllocated:
60 2B 52 AF DA A4 D3 01

W. D\SYSTEM. INI:01BF38DB191D3100000009550000020

W. D\WAVEMIX. INI:01BF38DAD3F8FF00000000360000020

W. D\POWERPNT. INI:01BF38DAD3F8FF000000003C0000020

W. D\SYSTEM. DAT:01BF38DB1A4E5E000024A4F40000027

W. D\USER. DAT:01BF38A5FFADC200000542340000020

** Keys&Values Modified | Added in the 2ndShot **

H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\LOphtCrack 2.5



H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\LOphtCrack 2.5\Uninstall-String: "C:\WIN95\uninst.exe -f"C:\Program Files\LOphtCrack 2.5\DeIsL1.isu" -c"C:\Program Files\LOphtCrack 2.5_JSREG32.DLL""

H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\LOphtCrack 2.5\Display-Name: "LOphtCrack 2.5"

H. L. K\SOFTWARE\Description\Microsoft\Rpc\UuidPersistentData
 \LastTimeAllocated: C0 8D 37 8A 11 A5 D3 01

H. L. K\SOFTWARE\LOpht Heavy Industries

H. L. K\SOFTWARE\LOpht Heavy Industries\LOphtCrack 2.5

H. L. K\SOFTWARE\LOpht Heavy Industries\LOphtCrack 2.5\2.5

H. L. K\System\CurrentControlSet\control\Shutdown\

SetupProgramRan: 0x00000002

W. D\SYSTEM.INI:01BF38DB2E925B000000095500000020

W. D\WAVEMIX.INI:01BF38DB2E925B000000003600000020

W. D\POWERPNT.INI:01BF38DB2E925B000000003C00000020

W. D\SYSTEM.DAT:01BF38DB4538B2000024A4F400000027

W. D\USER.DAT:01BF38DB4B2E93000005423400000027

我们看到，安装程序在 Uninstall 处装了键，这很正常，在 HKEY_LOCAL_MACHINE\SOFTWARE\ 处开了个 LOpht Heavy Industries 的入口，这也很正常。

(5)为了确保万一，我们用“Clear”按钮清除历史记录，在未运行 l0phtcra.exe 之前再作一次 Shot，按“1stShot”按钮。

(6)运行 l0phtcra.exe，并结束它。

(7)在 Regshot 中做“2ndShot”，并“compare”，结果如下：

* *Original contents Maybe deleted or modified* *

W. D\USER.DAT:01BF38DB4B2E93000005423400000027

* *Keys&Values Modified | Added in the 2ndShot* *

H. U\. Default\Software\Microsoft\Windows\CurrentVersion\Network

H. U\. Default\Software\Microsoft\Windows\CurrentVersion\Network\Tmp

H. U\. Default\Software\LOpht

H. U\. Default\Software\LOpht\LOphtCrack

H. U\. Default\Software\LOpht\LOphtCrack\AdminGroupName: "Administrators"

H. U\. Default\Software\LOpht\LOphtCrack\WordList:

"C:\Program Files\LOphtCrack 2.5\words - english"

H. U\. Default\Software\LOpht\LOphtCrack\Install: 0x0C4684F2



W. D\USER. DAT:01BF38DB8CBF3E00000542340000027

注意 :这里,我们看到,l0phtcr. exe 在第一次运行时对注册表的改动!!!!!!!!!!!!

(8)您可以多作几次,可以发现 l0phtcr. exe 在以后的运行中都不对注册表作变化!

(9)把时间调过头,果然不能再运行(真小气,只有 15 天),然后再安装,还是不能运行。

(10)如果您够小心,您会在第 9 步时对 uninstall 程序做一次比较,看看到底 l0phtcrack 在注册表中留下什么没有去除,导致它认识您的机器,知道它在这台机器上安装过。

结果如下:

* * Original contents Maybe deleted or modified * *

H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\L0phtCrack 2. 5

H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\L0phtCrack 2. 5\Uninstall-String: "C:\WIN95\uninst. exe -f"C:\Program Files\L0phtCrack 2. 5\DeIsL1. isu" -c"C:\Program Files\L0phtCrack 2. 5_JSREG32. DLL"

H. L. K\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\L0phtCrack 2. 5\Display-Name: "L0phtCrack 2. 5"

H. L. K\SOFTWARE\L0pht Heavy Industries

H. L. K\SOFTWARE\L0pht Heavy Industries\L0phtCrack 2. 5

H. L. K\SOFTWARE\L0pht Heavy Industries\L0phtCrack 2. 5\2. 5

W. D\USER. DAT:01BF38DBB8DABF00000542340000027

* * Keys&Values Modified | Added in the 2ndShot * *

W. D\USER. DAT:01BF38DBD576F700000542340000027

大家可以看到,反安装程序只是去除了安装程序所留下的东西,并没有去除 l0phtcr. exe 第一次运行时创建的键值!我们返回看看那个入口:

H. U\. Default\Software\L0pht

一般情况下,我们如果没有 RegShot 这个工具,也能用 Regedit. exe 来找到这个入口,毕竟名字很好找“L0pht”,于是您会想到,将其删除,以为万事大吉。但如果您此时再装 l0phtcrack 的话,却发现怎么也不让您再试用了,剩余天数总是 0。

再看看当初的记录,有一个键值很不引人注目:

H. U\. Default\Software\Microsoft\Windows\CurrentVersion\Network

H. U\. Default\Software\Microsoft\Windows\CurrentVersion\Network\Tmp

这个 tmp 就是我们想要找的,删除它之后一切都搞定了。



5.5 破解范例

好了,具体分析过程就不重复了,就用上节的方法对付。下面的方法只是延期使用,最彻底的破解还是用以前的调试方法改源程序或找出注册码。

rca max Animated Email Magic

HKEY_CURRENT_USER\Software\Arcamax\EMagic\2.0\Mail Options

Animation Shop 1.0(PSP 附带)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{A9CDFB42 - BD7F -
11D1 - B712 - 00A0C90AE045}\MS iPID50v(dword) 置 0 或删除

CacheX for IE v2.01

HKEY_CLASSES_ROOT\CLSID\{52ABC440 - 34D6 - 11D2 - BD9D - 00400534FC6D}

MiscStatus 置 0 或删除

Cuteftp 2.5

HKEY_CLASSES_ROOT\pfc\CFK20

@ = 0

Cuteftp 3.0

HKEY_CLASSES_ROOT\pfc\CFK25

@ = 0

Desk At Will

HKEY_CURRENT_USER\Software\ldyle Software\Desks At Will

License 、InitFlags 置 0 或删除

MemTurbo 1.0b

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
\DataViewStream - MT01

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
DataViewSettings - MT01

Settings - MT01 置 0 或删除

Microangelo 98

HKEY_CURRENT_USER\Software\Impact\Microangelo 98\Evaluation

Start = 2451385 CheckNum = 535479 LastRan = 2451385 ,重装即可

Paint Shop Pro 5.0

HKEY_CLASSES_ROOT\CLSID\{84124FF1 - 5D04 - 11D1 - A575 - 00A0C96F2B0D}\MS]
iPID50t 、iPID50u 置 0 或删除

Paint Shop Pro 5.01

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{84124FF1 - 5D04 - 11D1 - A575 -



00A0C96F2B0D}\MS
 iPID501t 、iPID501u 置 0 或删除
 PC - cillin 98 试用版
 HKEY_LOCAL_MACHINE\Software\SYSTEMOLEDDDE\KIOPEN\Shell
 ROCKET98 = hex:07,7a,4e,23,fc,29,2c,38,2c,2e,53,59,53,54,45,4d,5c,4f,4c,45,删除
 Snagit 4.2
 HKEY_CLASSES_ROOT\tigans
 @ = 0 置 0 或删除
 The Bat!
 HKEY_CURRENT_USER\Software\RIT\The Bat! \Viewer
 Default_Value(dword) = 00008e2c
 Theme Freak 1.2
 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\MasterInfo
 Enabled = False 、UsageData = 0 置 0 或删除
 Turbo Browser 98
 HKEY_LOCAL_MACHINE\Security
 Tool1. = hex:e0,59,9b,87,fd,d5,be,01 删除
 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
 Q. Status = hex:e0,59,9b,87,fd,d5,be,01 删除
 Virus Scan 4.0
 HKEY_LOCAL_MACHINE\Software\Network Associates\ECare\LM\FDX5 - KAA
 Data(hex) 置 0 或删除
 WebZip 2.3
 HKEY_CURRENT_USER\Software\Microsoft\IFind
 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
 Explorer\Metrics
 @ = 0 置 0 或删除
 WebZip 3.0
 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
 ShellRects
 Settings 置 0 或删除
 Windows Help Design Pro
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\URL
 news(hex) = 00,00,00,00,60,cf,e1,40 删除
 lnews(hex) = 00,00,00,00,60,cb,e1,40 删除
 超级解霸 5.5



HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup
RunTime(dword) = ffffffff
Crystal 3D IMPACT! Pro
HKEY_CLASSES_ROOT\JSMP - R. Manager. 1
RunFlags = EP2PAVTZJW803ICCUXMP
Explor2000
HKEY_CURRENT_USER\Software\CMAufroy\Explor2000
BS(hex) 置 0 或删除
HKEY_CURRENT_USER\Software\CMAufroy\Explor2000\Main
MS(hex) 置 0 或删除
Resplendent Registrar 1.07
HKEY_CURRENT_USER\Software\Resplendence Sp\Resplendent Registrar\Settings
2C8FD321 - C523034A, A4358739 - 43D89234 置 0 或删除



第六章 剥除软件的外衣——脱壳技术

编者语:第五章的第一节引用了脱壳站点 topage. 126. com 站长吴朝相的文章,此君可谓国内“脱壳”技术的元老,如果大家有什么“脱壳”方面的问题,可以通过 wx98@163. net 联系他。

6.1 一切从“壳”开始

首先我想大家应该先明白“壳”的概念。在自然界中,我想大家对壳这东西应该不会陌生的,植物用它来保护种子,动物用它来保护身体等等。同样,在一些计算机软件里也有一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行,拿到控制权,然后完成它们保护软件的任务。就像动植物的壳一般都是在身体外面一样理所当然(但后来也出现了所谓的“壳中带籽”的壳)。由于这段程序和自然界的壳在功能上有很多相同的地方,基于命名的规则,大家就把这样的程序称为“壳”了。就像计算机病毒和自然界的病毒一样,其实都是命名上的方法罢了。

最早提出“壳”这个概念的,据我所知,应该是当年推出脱壳软件 RCOPY 3 的作者熊焰先生。在几年前的 DOS 时代,“壳”一般都是指磁盘加密软件的段加密程序。可能是那时候的加密软件还刚起步不久吧,所以大多数的加密软件(加壳软件)所生成的“成品”在“壳”和需要加密的程序之间总有一条比较明显的“分界线”。有经验的人可以在跟踪软件的运行以后找出这条分界线来,至于这样有什么用这个问题,就不用我多说了。但毕竟在当时,甚至现在这样的人也不是很多,所以当 RCOPY3 这个可以很容易就找出“分界线”,并可以方便地去掉“壳”的软件推出以后,立即就受到了很多人的注意。在当时来说,的确是有很多全新的构思,单内存生成 EXE 可执行文件这项,就应该是世界首创了。但它的思路在程序的表现上我认为还有很多可以改进的地方(虽然后来出现了可以加强其功力的 RO97),这个想法也在后来和作者的面谈中得到了证实。在这以后,同类型的软件像雨后春笋一般冒出来,记得住名字的就有 UNKEY、MSCOPY、UNALL……等等,但很多的软件都把磁盘解密当成了主攻方向,忽略了其它方面,当然这也为以后的“密界克星”“解密机器”等软件打下了基础,这另外的分支就不多谈了,相信机龄大一点的朋友都应该看过当时的广告了。

解密(脱壳)技术的进步促进和推动了当时的加密(加壳)技术的发展。LOCK95 和 BITLOK 等所谓的“壳中带籽”加密程序纷纷出笼,真是各出奇谋,把小小的软盘也折腾的够辛苦的了。正在国内的加壳软件和脱壳软件较量得热闹的时候,国外的“壳”类软件早已经发展到像 LZEXE 之类的压缩壳了。这类软件说穿了其实就是一个标准的加壳软件,它把 EXE 文件压缩了以后,再在文



件上加上一层在软件被执行的时候自动把文件解压缩的“壳”来达到压缩 EXE 文件的目的。接着,这类软件也越来越多,PKEXE、AINEXE、UCEXE 和后来被很多人认识的 WWPACK 都属于这类软件,但奇怪的是,当时我看不到一个国产的同类软件。

过了一段时间,可能是国外淘汰了磁盘加密转向使用软件序列号的加密方法吧,保护 EXE 文件不被动态跟踪和静态反编译就显得非常重要了。所以专门实现这样功能的加壳程序便诞生了。MESS、CRACKSTOP、HACKSTOP、TRAP、UPS 等等都是比较有名气的本类软件代表,当然,还有到现在还是数一数二的,由台湾同胞所写的 FSE。其实以我的观点来看,这样的软件才能算是正宗的加壳软件。

在以上这些加壳软件的不断升级较劲中,很多软件都把比较“极端”的技术用了上去,因为在这个时候 DOS 已经可以说是给众高手们玩弄在股掌之间了,什么保护模式、反 SICE、逆指令等等。相对来说,在那段时间里发表的很多国外脱壳程序,根本就不能对付这么多的加壳大军,什么 UPC、TEU 等等都纷纷成为必防的对象,成绩比较理想的就只有 CUP386 了。反观国内,这段时间里也没了这方面的“矛盾斗争”。加壳软件们挥军直捣各处要岗重地,直到在我国遇到了 TR 这个铜墙铁壁以后,才纷纷败下阵来各谋对策,但这已经是一年多以后的事情了。我常想,如果 TR 能早两年“出生”的话,成就肯定比现在大得多,甚至盖过 SICE 也有可能。TR 发表的时候 Win95 的流行已经成为事实,DOS 还有多少的空间,大家心里都清楚。但话又说回来,TR 的确是个好软件,比起当年的 RCOPY3 有过之而无不及,同时也证明了我们中国的 CRACK 实力(虽然有点过时)。这个时候,前面提到过的 FSE 凭着强劲的实力也渐渐的浮出了水面,独领风骚。其时已经是 1997 年年底了,我也走完了学生“旅程”。工作后在 CFIDO 的 CRACK 区认识了 Ding-Boy,不久 CRACK 区关了,我从此迷上了 Internet,并于 1998 年 6 月建起了一个专门介绍“壳”的站台:<http://topage.126.com>,放上了我所收集的所有“壳”类软件。在这段时间里,各种“壳”类软件也在不断地升级换代,但都没什么太大的进展,差不多就是 TR 和众加壳软件的版本数字之争而已。

1998 年 8 月,一个名为 UNSEC(揭秘)的脱壳软件发表了,它号称可以脱掉 1998 年 8 月以前软件的所有壳。我测试之后,觉得并没传闻中的那么厉害,特别是兼容性更是令我不想再碰它。Ding-Boy 给这个软件的作者提了很多建议,但寄去的 Email 有如泥牛入海。可能是一怒之下吧,不久 Ding-Boy 的 BW(冲击波)就诞生了。这个使用内存一次定位生成 EXE 文件(后来放弃了)的脱壳软件,在我的站台公开后,得到了很多朋友们的肯定。要知道,从 RCOPY 3 开始,绝大部分的脱壳软件都是要两次运行目标程序来确定 EXE 的重定位数据的。BW 的这一特点虽然有兼容性的问题,但也树立了自己的风格和特色。经过几个月的改善,BW 升级到了 2.0 版本,这个版本的推出可以说是 BW 的转折点,因为它已经是一个成熟、稳定的脱壳软件了,它可以对付当时(现在)大多数的壳,包括当时最新的 FSE 0.6 等。更重要的是这个版本把选择壳和软件“分界线”这个最令新手头疼的步骤简化到不能再简化的地步,使更多的朋友接受了它。另外,能加强 BW 功力的 CI 模式也是其他脱壳软件没有的东西。最近,BW 发表了最新的 2.5 BETA2 版本,增强了一些方面的功能,因它竟然可以脱掉号称最厉害的磁盘加密工具 LOCKKING 2.0 的加密壳,因而进一步奠定了它在“脱壳界”的地位。说到最新,就不能不提 GTR、LTR、EDUMP、ADUMP、UPS、UPX、APACK 这几个国外的好软件了,它们每个都有自己的特色,可以说都是当今各类“壳”



中的最新代表了。(这些软件和详细介绍请到我的主页查阅)

由于 Windows 3.1 只是基于 DOS 下的一个图形外壳,所以在这个平台下的“壳”类软件很少,见过的就只有像 PACKWin 等几个有限的压缩工具,终难成气候。

可能是 Microsoft 保留了 Win95 的很多技术上的秘密吧,所以即便是 Win95 已经推出了 3 年多的时间,也没见过在其上面运行的“壳”类软件。直到 98 年的中期,这样的软件才迟迟的出现,而这个时候 Win98 也发表了有一段日子了。应该是有 DOS 下的经验吧,这类的软件不发表由自可,一发表就一大批地的冲了出来。先是加壳类的软件如:BJFNT、PELOCKNT 等,它们的出现,使暴露了 3 年多的 Win95 下的 PE 格式 EXE 文件得到了很好的保护。大家都应该知道现在很多 Win95 下的软件都是用注册码的方法来区分、确定合法与非法用户的吧,有了这类加壳软件,这种注册方法的安全性提高了不少,如果大家也有自己编的 Win95 程序,就一定要多留意一下本类软件了。接着出现的就是压缩软件了,因为 Win95 下运行的 EXE 文件“体积”一般都比较大,所以它的实用价值比起 DOS 下的压缩软件要大很多,这类的软件也很多,早些时候的 VBOX、PEPACK、PETITE 和最近才发表的 ASPACK、UPX 都是其中的佼佼者。在 DOS 下很流行的压缩软件 WWPACK 的作者也推出了对应 Win95 版本的 WWPACK32,由于性能并不是十分的突出,所以用的人也不太多。由于压缩软件其实也是间接给软件加了壳,所以用它们来处理 EXE 也是很多软件作者喜欢做的事情,最近新发表的很多软件里都可以看到这些加壳、加压缩软件的名字了。有加壳就一定会有脱壳的,在 Win95 下当然也不例外,但由于编这类软件比编加壳软件要难得多,所以到目前为止,我认为就只有 PROCDUMP 这个软件能称为通用脱壳软件了,它可以对付现在大多数的加壳、压缩软件所加的壳,的确是一个难得的精品。其它的脱壳软件多是专门针对某某加壳软件而编,虽然针对性强、效果好,但收集麻烦,而且这样的脱壳软件也不多。前些时候 TR 作者也顺应潮流发表了 TR 的 Win95 版本:TRW,由现在的版本来看可以对付的壳还不多,有待改进。

BW 的作者 Ding - Boy 最新发表了一个 Win95 的 EXE 加壳软件 DBPE。虽然它还不太成熟,但它可以为软件加上使用日期限制这个功能其他加壳软件所没有的,或者以后的加壳软件真的会是像他说的那样:可以加壳和压缩并重、并施;随意加使用日期;加上注册码;加软件狗(磁盘)保护;加硬件序列号判别;加……

6.2 手动脱壳

这一节以一实例介绍手动脱壳最简单的情况,我们平时碰到最多的 EXE 压缩工具是 UPX、ASPACK 等,在这里我们用 UPX 来压缩 Windows 自带的记事本程序,然后手动将其脱壳。

UPX 版本:UPX V1.01

原文件:Notepad 34K

用 UPX 压缩后:Notepad - upx 16K

先来分析一下用 UPX 压缩后的记事本程序运行情况。UPX 压缩时在记事本程序前加了一段自解压代码,记事本程序运行时,首先就运行这段自解压代码,这段代码按一定算法,将压缩过的



记事本程序在内存解压,直到将记事本程序完全解压,跳到记事本程序代码处(这个地方就是入口点),然后从这里开始正确运行记事本程序。此时解压后的记事本程序代码全部完整存在内存里,我们可用相关工具将其全部复制保存到一文件,再将这文件运行的入口点修正,程序就可完全运行了。这就是手动脱壳最基本的情况。

因此手动脱壳关键是找到入口点,不然就不能得到完整的解压程序代码。找入口点可依据如下原则:决大多数 PE 加壳程序在被加密的程序中加上 1 个或多个段。所以看到一个跨段的 JMP 就有可能了。UPX 用了一次跨段的 JMP,ASPACK 用了两次跨段的 JMP。就是你一步步跟踪时会看到代码有一突跃,一般再根据领空文件名的变化,就能确定入口点了。

说了这么多了,我们开始工作:

1. 分析是用何软件压缩(假设开始我们不知是用什么软件压缩的)

一般拿到这软件后,可用工具 gtw、TYP32、FileInfo 等侦测文件类型的工具来看看是何种软件压缩的,在这我们以 FileInfo 为例,把 Notepad - upx 复制到工具软件目录下,在资源管理器下双击 FileInfo,再按回车,你将看到报告出来:告诉你这是 UPX1.01 压缩的软件。

或者你用 Procdump 工具,运行 Procdump 后,点击 P EEditor 按钮,选上 Notepad - upx 文件,再点击 Sections 按钮,你会看到 Sections informations 对话框里,Name 那项有 UPX0、UPX1,这表明是用 UPX 压缩的。

2. 用 TRW2000 来脱壳

(1) 手动找入口点

运行 TRW2000 装载 Notepad - upx,然后 LOAD,你将中断在主程序入口处:此时按 F10、F7 键(程序执行到光标行,用来走出循环)一直向前走,注意此时领空会是:NOTUPX! UPX1 + 2xxx,. 直到你来到:

```
0137:40ddbe popa
```

```
0137:40ddf jmp 00401000←此行已完全解压结束,将要跳到记事本程序入口点执行程序。
```

```
0137:401000 push ebp←完全解压后的记事本程序第一行
```

好了,基本大功告成。在 0137:401000 一行,执行命令 makepe 文件名或 pedump 文件名。就这样脱壳成功。

makepe 命令含义:从内存中整理出一个指令名称的 PE 格式的 exe 文件,当前的 EIP 将成为新的程序入口,生成文件的 Import table 已经重新生成过了。生成的 PE 文件可运行任何平台和微机上。

pedump 命令含义:将 PE 文件的内存映像直接映像到指定的文件里。生成的文件只能在本机运行,不能在其他系统平台或微机运行。

你也可用 Procdump 来配合脱壳,在 137:401000 一行,执行 suspend 命令挂起程序。然后就回到 Windows 下,运行 Procdump 文件,在 Procdump 的左上窗口中,在 Task 一列找到 Notepad - upx. exe,然后在此行点击右键,选择 DUMP(FULL),将内存中的记事本程序以另一文件名存盘。然后点击 PE Editor 按钮,选上你刚脱壳的文件,会出现一窗口,在 Entry Point(入口点)一项填上程序入口点,这里是 00401000,然后点击 OK 存盘即可。注意:在此例 DUMP(FULL)的入口点刚好是 00401000,在大多数情况下,均要手动修正。这样处理后,程序脱壳成功。此时你可在 Proc



dump 选上刚才的记事本程序,点击右键,用 Kill Task 命令关闭记事本程序。

(2)用 PNEWSEC 命令找入口点

运行 TRW2000 装载 Notepad - upx, 然后 LOAD, 你将中断在主程序入口处: 执行命令 PNEWSEC, 稍等就会停在入口点, 剩下的和上面一样, 但有时用这命令对一些程序无效, 就不得不用手动来找入口点了。

PNEWSEC: 运行直到进入一个 PE 程序内存的新的 section 时产生断点。

3. 用 SOFTICE 来脱壳

(1)用 SOFTICE 找入口点, 只有靠手动来找了, 方法同 TRW2000 一样, 来到:

```
0137:40ddf jmp 00401000
```

现在这一行, 键入以下命令:

```
a eip(然后按回车)
```

```
jmp eip(然后按回车)
```

按下 F5

这样将改变 0137:40ddf 行的代码。你会注意到在键入“jmp eip”并按下回车后, 40ddf 的指令现在是一个 jmp。这将有效地使程序“暂停”(有点类似 TRW2000 的 suspend 命令)。按下 F5 使你回到 Windows, 你就可以 dump 已经脱壳的程序到你的硬盘了。剩下的就和上面 TRW2000 操作一样了。

(2)用 Icedump 来配合 SOFTICE 和 Procdump

装载 SOFTICE 后, 在 Icedump 的目录里执行你相应版本的 Icedump(这里我的 SOFTICE 是 4.05 版, 我选上 win9x 目录下 405 目录, 运行 icedump.exe)。

再运行 Procdump32, 从主菜单中选择“Option”, 选中“Rebuild new import table”重建 import 表, 这样生成的 PE 文件就会重建, 类似于 TRW2000 的 makepe 命令。在上一节用 Procdump 自动脱壳时, 也要选上这一项。

再点击 Procdump 其中的“Bhrama Server”, OK, 就别管它了。(注意: AutoFixPE 要选上)再用 SOFTICE 的 Symbol Loader 装载 Notepad - upx 来到:

```
0137:401000 push ebp ← 你停在这, 下命令“PAGEIN B PROCDUMP32 - DUMPER SERVER”脱壳。
```

下命令后, 来到 Windows 环境下在 Procdump 里会跳出一对话框, 以另一文件存盘, 至此脱壳成功。

你每次下“PAGEIN B PROCDUMP32 - DUMPER SERVER”这命令也麻烦了, 你可在 SOFTICE 目录下的 winice.dat 里加上一行: F3 = “PAGEIN B ProcDump32 - Dumper Server;” 以后按 F3 就可执行这命令。

(注: 这是 icedump 6.015 的命令, 在 6.16 版本后命令完全不同, 而是 F3 = “/BHRAMA ProcDump32 - Dumper Server;”)

4. 小结

(1)你会发现脱壳后的软件比压缩前的大了, 这没关系, 只要程序能正常运行即可。判断脱壳成功的依据是什么呢? 我个人的观点是: 你在调试工具下(SOFTICE 或 TRW2000)看到程序任何



一处的机器码同用 W32DASM 反汇编出来看到的机器码一样,那么即是脱壳成功。

(2)问:有些程序脱壳后用 W32DASM 不能反汇编?

你可用 ProcDump 的 PE Editor 把脱壳后的文件的 text 或 code section 的 Characteristics 改为 E0000020,再反汇编就可以了。

(3)问:部分脱壳后的 exe 文件如何再压缩?用 UPX,PELITE,PECOMPACT 等都说错。

不能被压缩多是无效的 Relocations,Relocations 存放程序重定位信息。Win9x 下一般不需要用到重定位,但 NT 下就一定要用到,这是使脱壳的程序在 NT 下不能运行的原因。用 Procdump 修改脱壳程序 Relocations rav/size 为 0 就可压缩。需要在 NT 下运行就把对应的 .reloc 段的 rav/size 填上即可。



第七章 实例

本章所涉及内容大多为破解高手破解软件时的笔录,发布在网上,只可为教学所用。通过这些方法破解的软件(教学专用软件除外)不可用于任何商业活动或自由发布,否则后果自负。

7.1 FlashGet(JetCar Ver0.77) 破解实录

这个软件是完全免费的,根本没有破解的必要,因为注册前与注册后的主要区别在于注册后“广告栏会自动移除”。而且这个软件也是取用目前较流行的防破解手法:即在输入完注册码后并不立即进行比对(先把注册码存放在①文件中②注册表中③内存中),而是在下一次软件启动的时候才作比对,所以我们将这篇文章介绍给大家,它应该是一篇很好的破解教材!希望大家能够喜欢。

该软件是取用第二种手法,即把注册码存放在注册表中:\HKEY_CURRENT_USER\SoftWare\JetCar\JetCar\General的RegName和RegPass,所以第一时间应想到的方法就是用拦注册表的API函数:bpx RegOpenKeyA或bpx RegQueryValueExA,想在它进行注册码比对时再把其一网打尽。但是,这个软件在启动的时候有数十处地方调用这两个函数,这又给破解带来了一些麻烦,因为不可能一个一个地去筛选,这样做太愚蠢了。这时你应该想到破解利器W32DASM,因为它常常是SoftIce的好助手。

破解工具:W32DASM 8.9X

SoftIce for Win9X 4.X

首先用W32DASM把JetCar反编译,然后查找字符串:RegName(此处非常关键),一会就搜索到了:

```
* StringData →“RegName”
|
:00410356 push 0049BC60
* StringData →“General”
|
:0041035B push 0049B430
:00410360 mov ecx, esi
; 此处请填入你的注册名
:00410362 call 00469650
```



```
; \HKEY_CURRENT_USER\SoftWare\JetCar\JetCar\General 的 RegName
:00410367 mov edx, dword ptr [esp + 0000012C]
:0041036E mov ecx, esi
:00410370 push edx
* Possible StringData Ref from Data Obj →“RegPass”
|
:00410371 push 0049BC58
* Possible StringData Ref from Data Obj →“General”
|
:00410376 push 0049B430
; 此处请输入的你填写的注册码
:0041037B call 00469650
; \HKEY_CURRENT_USER\SoftWare\JetCar\JetCar\General 的 RegPass
:00410380 push FFFFFFFF
:00410382 push 00000030
*** “Thank you for registering FlashGet. Please restart the progr”
|
:00410384 push 0000EF82
:00410389 call 004116D0
; 就是那个提示重新启动的窗口
既然上面的代码是把你输入的名字和注册码写入注册表中,那么它肯定还有一段代码是把
你的名字和注册码从注册表中读出来的,于是再次往下查找 RegName,这次又会找到:
* StringData →“RegName”
|
:004104BF push 0049BC60
:004104C4 lea eax, dword ptr [esp + 14]
* StringData →“General”
|
:004104C8 push 0049B430
:004104CD mov esi, ecx
:004104CF push eax
:004104D0 call 00472783
; 从注册表中读出你刚才输入的名字
:004104D5 push 0049FC40
* StringData →“RegPass”
|
:004104DA push 0049BC58
```



```
:004104DF lea ecx, dword ptr [esp + 10]
```

```
* StringData →“General”
```

```
|
```

```
:004104E3 push 0049B430
```

```
:004104E8 push ecx
```

```
:004104E9 mov ecx, esi
```

```
:004104EB mov [esp + 34], 00000000
```

```
:004104F3 call 00472783
```

```
; 从注册表中读出你刚才输入的注册码
```

```
:004104F8 mov edx, dword ptr [esp + 0C]
```

那么正确的注册码是什么?它们又是在哪里进行比对的?呵呵,先不要急嘛,继续往下看吧。

```
:0041057B push ecx
```

```
; 你输入的名字
```

```
:0041057C push edx
```

```
; edx, 程序生成的
```

```
:0041057D mov ecx, esi
```

```
:0041057F call 00410620
```

```
; 生成注册码的 Call
```

```
; 有兴趣的朋友可以跟进去研究研究
```

```
:00410584 mov eax, dword ptr [esp + 0C]
```

```
; 你输入的注册码
```

```
:00410588 mov ecx, dword ptr [esp + 14]
```

```
; 正确的注册码
```

```
:0041058C push eax
```

```
:0041058D push ecx
```

```
:0041058E call 00449F6E
```

```
; 注册码进行比对
```

```
:00410593 add esp, 00000008
```

```
:00410596 mov byte ptr [esp + 28], bl
```

```
:0041059A test eax, eax
```

```
; 成功 eax = 0, 不成功 eax = FFFFFFFF
```

```
:0041059C pop edi
```

```
:0041059D lea ecx, dword ptr [esp + 10]
```

```
:004105A1 jne 004105DA
```

```
; 注册失败
```

```
; 也可直接把其改成 9090
```

现在大家应该一目了然嘛。如果还不明白,那就快学学前面的基础知识吧。



最后整理一下：

- (1) 先运行 JetCar 0.77,然后在菜单上选“帮助→移掉广告横幅”,用户名称:000ye,注册码:78787878,按“确认”键,最后退出 JetCar;
- (2)用 SoftIce 的 Symbol Loader 载入 JetCar;
- (3)按 F8;
- (4)下断点; bpx 0041058C;
- (5)按 F5;
- (6)程序中断: D ecx;
- (7)赶快抄下来正确的注册码:05914NB7R3

7.2 ACDSec V3.0 破解

ACDSec 是一个快速、功能完整,兼具影像浏览、查看、数据库、档案管理和图像处理的工具。这个第一手的软件支持了超过 40 种不同的档案格式,让使用者可以查看、管理、打印影像,或是制作图像的缩图。最新的 ACDSec 可以增加图像,包括切割、变更大小并改变色平衡。ACDSec 也可以让你把图档送出去和其他朋友分享,或是直接观看存放在 ZIP 或是 LZH 档案中的图像。但是由于是共享软件,没注册时,有许多不便。下面我们就用 Trw2000 来对其进行破解。

启动 TRW2000,点击 OK,按下 Ctrl - N,下 PMODULE 指令,运行 ACDSec,弹出过期画面,按下 Ctrl - N,关闭过期画面,马上被 TRW 拦下,如下所示:

```
xxx: 004045A8 CALL 00433830 关键 CALL1  
XXX: 004045AD ADD ESP, BYTE +04
```

光标停在这里,按下 F6,把光标移动到 004045A8 处,按下 F9 设断点,接着是按 F5。再次运行 ACDSec,在 004045A8 处拦下,按 F8 进入 CALL,一直按 F10 直到:

```
xxx: 00433ABB CALL 00433FE0 关键 CALL2
```

按 F8 进入关键 CALL2,如下:

```
xxx: 00433FE0 MOV EAX, [ESP + 04]  
XXX: 00433FE4 MOV ECX, [004E8FE8]  
      PUSH BYTE +00  
      PUSH DWORD 00434010  
      PUSH EAX  
      PUSH DWORD 0407  
      PUSH ECX  
XXX: 00433FF8 CALL USER32! DialogBoxPa 关键 CALL3  
xxx: 00433FFE DEC EAX  
      NEG EAX  
      SBB EAX, EAX
```



XXX: 00434003 INC EAX

看见关键 CALL3 没有?只要我们在它前面插入一个 JMP 跳过它便可以避开过期画面。但 JMP 不能乱插,看看前面的 5 条 PUSH 指令,我们要记下光标走到每一条 PUSH 指令上时的 ESP 的值,然后记下光标走到 xxx: 00433FFE 上时 ESP 的值,光标在哪一条 PUSH 指令上时 ESP 的值和在 xxx: 00433FFE 上时 ESP 的值一样,便在哪一条 PUSH 指令那里加入 JMP 指令。答案是:将第一条 PUSH 指令改成 JMP 00434003。下 CODE ON 指令记下机器码,以后有用。

由于 ACDSec 用 ASPACK 压缩过,所以不能直接修改它的 16 进制代码,下面还要用 TRW 脱壳。运行 TRW,将 ACDSec 的图标拖到 TRW 中,点击 LOAD,拦下后一直按 F10 直到 TRW 中的“ACDSec!. ASPACK + ????”变成“ACDSec!. TEXT + ????”(很长时间的,你也可以先按 F10,到一个反复跳动的地方后,按一下 F12 后,再点击一下 LOAD,再按 F10,反复约 2-3 次便可以了),就可以脱壳了,下 PEDUMP 指令后生成一个 DUMP1. EXE 的程序。找到 DUMP1. EXE,它在 TRW 的工作目录(c:\ 或 trw 的安装目录 或 桌面)。用 UEDIT32 打开 DUMP1. EXE 修改机器码(前面记录过),答案是:

6A00681040430050

EB17 - - - - -

将改过的 DUMP1. EXE 复制到 ACDSec 所在目录并改名为 ACDSec. exe 即可。

7.3 美萍网管大师 v5.2 破解及注册机制作

美萍安全卫士 v5.2 可以防 TRW2000 和 SoftICE,而且极为凶悍,有些程序检测到这类跟踪调试软件只不过是显示一个 nag 然后终止程序运行,而美萍网管大师 v5.2 (包括安全卫士的最新版本)发现此类程序,就关机,所以这次使用 W32DASM 超级 中文版来破解它!

(1) scon. exe 这个文件是用 aspack 1.07 加的壳,直接使用 unaspack 就可以搞定了!

(2) 启动 W32dasm 反汇编 scon. exe,那么我们从何入手呢,看看说明,哦,有时间限制,还有那个注册框上显示的未注册一句话作为入手!如果在 W32dasm 中找不到,那么我们可以通过注册表,因为它通过阅读注册表的信息,然后判断是否注册,很高兴,我们找到了这么一句话“软件试用期还剩”,我们就从这里入手!双击它,然后来到如下程序段:

* Possible StringData Ref from Code Obj →“软件试用期还剩”

```

|
: 004846DA 6808494800      push 00484908
: 004846DF 8D55DC           lea edx, dword ptr [ebp - 24]
: 004846E2 A1F48D4800      mov eax, dword ptr [00488DF4]
: 004846E7 40              inc eax
: 004846E8 2B0544DE4A00   sub eax, dword ptr [004ADE44]
: 004846EE E8392EF8FF     call 0040752C
: 004846F3 FF75DC           push [ebp - 24]

```



:004846F6 6820494800 push 00484920

/* 当然这里没有我们需要的信息,我们需要往上找 */

往上来到如下:

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

|:00484476(C)

|

:004846A3 E8EC55FEFF call 00469C94→判断什么的?

:004846A8 85C0 test eax, eax

:004846AA 7577 jne 00484723 →这个 jnz 有可疑!双击此处,让光标来到此处!

:004846AC A1F48D4800 mov eax, dword ptr [00488DF4]

:004846B1 83E80F sub eax, 0000000F

:004846B4 3B0544DE4A00 cmp eax, dword ptr [004ADE44]

:004846BA 7D67 jge 00484723

:004846BC 6A40 push 00000040

:004846BE 8D45E8 lea eax, dword ptr [ebp - 18]

让光标停留在 4846AA 处,然后用 jump to 看它跳到哪里去.....

* Possible StringData Ref from Code Obj →“,请赶快向作者注册(0371 - 8982414)”

|

:004846FB 682C494800 push 0048492C

:00484700 8D45E4 lea eax, dword ptr [ebp - 1C]

:00484703 BA04000000 mov edx, 00000004

:00484708 E88FF5F7FF call 00403C9C

:0048470D 8B45E4 mov eax, dword ptr [ebp - 1C]

:00484710 E88BF6F7FF call 00403DA0

:00484715 50 push eax

:00484716 8BC3 mov eax, ebx

:00484718 E82719FAFF call 00426044

:0048471D 50 push eax

* Reference To: user32. MessageBoxA, Ord: 0000h

|

:0048471E E8DD1BF8FF Call 00406300 →call 出那个讨厌对话框的地方!

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:

|:004846AA(C), :004846BA(C)

|

:00484723 B201 mov dl, 01 →4846AA 的跳跃就是来到这里的,到了这里,也就是跳过了那个窗口!



```
:00484725 8B8314020000      mov eax, dword ptr [ebx + 00000214]
:0048472B E85408FDFE      call 00454F84
/* 那么 4846A3 的那个 call 不是判断时间就是判断注册码的,我们进那个 call 看看 */
4846A3 那个 call 的内容如下:
```

* Referenced by a CALL at Addresses:

! :0048305F , :004846A3

|

```
:00469C94 53                push ebx
:00469C95 A13C8F4800      mov eax, dword ptr [00488F3C]
:00469C9A 8B00          mov eax, dword ptr [eax]
:00469C9C E827A5FFFF      call 004641C8 →计算注册码的 call! 写注册机就要仔细看这个 call 它的算法不是很复杂!

:00469CA1 8BD8          mov ebx, eax
```

* Possible StringData Ref from Code Obj →“RegNum” →看见了吗?这个 call 就是判断注册码的! 算出注册码也不难了吧!

```
! :00469CA3 B8C49C4600      mov eax, 00469CC4
:00469CA8 E8B3A6FFFF      call 00464360
:00469CAD 3BD8          cmp ebx, eax →哈哈,我们可以用 trw2000 来下断点! 下断点 469C94 很快来到这里,看 ebx 的值,把它转成十进制就是注册码

:00469CAF 7507          jne 00469CB8→这里不跳就 OK! 改破解版,就改这里好了,把 7507 改成 9090

:00469CB1 B801000000      mov eax, 00000001
:00469CB6 5B                pop ebx
:00469CB7 C3                ret
```

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

! :00469CAF(C)

|

```
:00469CB8 33C0          xor eax, eax →不能来到这里,让他把 eax 清 0 就完了!

:00469CBA 5B          pop ebx
:00469CBB C3          ret
```

下面我们用 Crackcode2000 来制作注册机,因为这次的注册码不是直接用 ASCII 码形式放在内存中的,

而是用数值的形式放在寄存器处的,所以这时就要用模式 1 了。下面是 Crackcode.ini 的信息:

[Options]



CommandLine = scon. exe

Mode = 1

First_Break_Address = 469CAD

First_Break_Address_Code = 3B

First_Break_Address_Code_Lenth = 2

Save_Code_Address = EBX

我的序列号是 183894, 计算出的注册码是 30806! crackcode2000 注册机就写好了! 很简单吧!

破解版制作:

(1)用 UnAspack 解压 scon. exe 文件

(2)查找:E8 B3 A6 FF FF 3B D8 75 07

替换: -- -- -- -- -- -- -- -- 90 90

7.4 WinZIP8.0 牛刀小试

如果你是一个电脑用户,却诚恳地告诉我你不知道什么是 Winzip。我晕!那我没什么可说的,这篇文章也不用看了,幸好这样的人不算太多,又给了我写下去的勇气。

本文的目的不是单单为破解此软件,意义在于抛砖引玉,让初学者理解破解的基本思路。本文具有一定的普遍性,过程讲解尽可能详细,即使是未接触过破解的人也能按步骤找出注册码,掌握一套普遍适用的方法。

废话少说,还是让我们来看看破解的方法吧。

详细过程:

一、运行 TRW2000 程序

二、运行 Winzip8.0

三、粗跟踪

(1)点 HELP→about winzip...→register...。

(2)输入 Name: cccc Reg Key: 88888888 (8个8)。

(3)Ctrl + N 呼出 TRW,下断点:BPX HMEMCPY 按 F5 返回。

(4)点 OK,被拦截。

(5)bd * , 作废所有断点。

(6)pmodule,直接到达 Winzip 领空,下代码:

0137: 00407F6D CALL \USER32! GetDlgItemTextA\

0137: 00407F73 PUSH EDI ←来到此行,是 Winzip 的代码,细跟踪可以直接中断到这行[A]

0137: 00407F74 CALL 0043F89A

0137: 00407F79 PUSH EDI

0137: 00407F7A CALL 0043F8C3



```

0137:00407F7F POP     ECX
0137:00407F80 MOV     ESI,0048CDA4
0137:00407F85 POP     ECX
0137:00407F86 PUSH    BYTE +0B

```

(7)按 F12,在 1 次后出现非法注册码错误对话框,点 OK 退出

(8)分析:按 1 次后即出现非法注册码错误框,说明验证注册码就在这段代码中(F12 运行到遇到 RET, RETF, IRET 指令时停下来)。接下来应找出具体哪个 CALL 产生错误框,并记录下大致跳转的过程,以便可找出在哪个跳转位置可以跳过产生错误框的 CALL。进一步找出验证注册码、计算注册码的位置。

四、细跟踪

(1)同前,输入注册码,呼出 TRW,设断点:BPX 004077F73 ←是上面[A]行

(2)点 OK,被拦截,代码如下面[步骤 7 后面]

(3)bc * ,清除所有断点

(4)现在要找出产生误注册码框的哪个 CALL:按 F10,即单步跟踪。一直按 F10,一直按,注意记下的次数,直到出现错误框,假设使用次数为 X 次。

(5)从步骤 1 开始重来,做到步骤 4 时按 F10(X-1)次,即找出了产生错误的 CALL,是下面代码后部的 0137:00408018 CALL 00430025,就是这条指令产生错误框。

(6)着重分析如何跳过 0137:00408018 CALL 00430025 这条产生错误框指令。读者可从下面代码由后面向前读,看懂本人的分析过程。另外也可以首先在离 0137:00408018 CALL 00430025 这条产生错误框指令不远代码处开始,记录一份程序执行到 0137:00408018 CALL 的跳转过程,这样便于直接找出那个重要的跳转点,即如本程序中的 00407FBC JZ 00408005。

(7)现在已基本找出验证注册码的地方了 0137:00407FB5 CALL 004079D5 这个 CALL 中验证注册码,所以要深入跟踪进这个 CALL。(深入跟踪步骤在代码后面)

```

0137:00407F6D CALL    `USER32! GetDlgItemTextA`
0137:00407F73 PUSH    EDI        ←中断于此行,从这行起开始细跟踪,即按 F10 键。
0137:00407F74 CALL    0043F89A
0137:00407F79 PUSH    EDI
0137:00407F7A CALL    0043F8C3
0137:00407F7F POP     ECX
0137:00407F80 MOV     ESI,0048CDA4
0137:00407F85 POP     ECX
0137:00407F86 PUSH    BYTE +0B
0137:00407F88 PUSH    ESI
.
.
.
0137:00407F96 CALL    0043F89A

```



```

0137: 00407F9B PUSH     ESI
0137: 00407F9C CALL     0043F8C3
0137: 00407FA1 CMP      BYTE [0048CD78], 00
0137: 00407FA8 POP      ECX
0137: 00407FA9 POP      ECX
0137: 00407FAA JZ       00408005
0137: 00407FAC CMP      BYTE [0048CDA4], 00
0137: 00407FB3 JZ       00408005
0137: 00407FB5 CALL     004079D5 ← 就是这个 CALL 中验证注册码,所以深入跟踪
                        进入这个 CALL
0137: 00407FBA TEST     EAX, EAX ←就是这个测试(TEST),至关重要,EAX 的值
                        由上面的 CALL 决定,就是说上面这个
                        CALL 验证注册码,并相应置 EAX 的值,决定
                        是否跳转.应深入到这个 CALL 中,找出验证
                        的地方。
0137: 00407FBC JZ       00408005 ←这里如跳转则到 00408005 CALL,接下去执行
                        00408018 CALL,出错

0137: 00407FBE PUSH     EDI
0137: 00407FBF MOV      EDI, 0047FFA4
0137: 00407FC4 PUSH     DWORD 0047DB24
0137: 00407FC9 PUSH     EDI
0137: 00407FCA CALL     0043B5DA
0137: 00407FCF PUSH     ESI
0137: 00407FD0 PUSH     DWORD 0047E66C
0137: 00407FD5 PUSH     EDI
0137: 00407FD6 CALL     0043B5DA
0137: 00407FDB PUSH     DWORD 0047FFC4
0137: 00407FE0 PUSH     BYTE  +00
0137: 00407FE2 PUSH     BYTE  +00
0137: 00407FE4 PUSH     DWORD 0047DB30
0137: 00407FE9 CALL     0043B5C1
0137: 00407FEE MOV      EAX, [00487AF4]
0137: 00407FF3 ADD      ESP, BYTE +28
0137: 00407FF6 TEST     EAX, EAX
0137: 00407FF8 JZ       00408001
0137: 00407FFA PUSH     EAX
0137: 00407FFB CALL     `GDI32! DeleteObject`

```



```

0137: 00408001 PUSH    BYTE + 01
0137: 00408003 JMP     SHORT 00408035
0137: 00408005 CALL    004082A6 ←上面 00407FBC 行跳到此行,如执行到此行,则
                    会执行 00408018 CALL
0137: 0040800A PUSH    DWORD 028E 说明上一跳转已判别出输入的是错误注册
                    码。继续向后分析
0137: 0040800F CALL    0043F5ED
0137: 00408014 PUSH    EAX
0137: 00408015 PUSH    EBX
0137: 00408016 PUSH    BYTE + 3D
0137: 00408018 CALL    00430025 ←执行此行 CALL 则出现错误框,须找出如何才
                    能跳过此行
0137: 0040801D ADD     ESP, BYTE + 10
0137: 00408020 INC     DWORD [00487AF8]

```

四、深入跟踪

- 1 重复细跟踪步骤中的 1-3 步;
- 2 按 F10, 小心不要走过头呵, 一直执行 00407FB5 CALL 004079D5 这行;
- 3 按 F8, 追入此 CALL, 来到下面代码(代码在步骤 4 后面);
- 4 按 F10, 边按边分析, 值得怀疑的地方可查看各寄存器的内容(用 D EAX、EDI 等命令), 你会找到下面的代码, 本程序就在这里计算和验证注册码。按 F10 键 53 次到达 0137: 00407A97 PUSH EAX(见代码), 这里就是……

```

0137: 00407905 POP     ESI ← 追入上叙 CALL 后, 来到此行
0137: 00407906 POP     EBP
0137: 00407907 RET     04
0137: 0040790A PUSH    ESI
0137: 0040790B MOV     ESI, ECX

```

```

0137: 00407A5E PUSH    EAX
0137: 00407A5F CALL    00467C10
0137: 00407A64 PUSH    DWORD C8
0137: 00407A69 LEA    EAX, [EBP + FFFFFFF8]
0137: 00407A6F PUSH    BYTE + 00
0137: 00407A71 PUSH    EAX
0137: 00407A72 CALL    00467C10
0137: 00407A77 ADD     ESP, BYTE + 18

```



0137: 00407A7A	TEST	ESI, ESI	
0137: 00407A7C	JZ	00407A91	
0137: 00407A7E	CALL	004082A6	
0137: 00407A83	AND	DWORD [00489FDC], BYTE +00	
0137: 00407A8A	XOR	EAX, EAX	
0137: 00407A8C	JMP	00407B42	
0137: 00407A91	LEA	EAX, [EBP + FFFFFFFE0]	
0137: 00407A97	PUSH	EAX	←按 F10 键 53 次到这行
0137: 00407A98	PUSH	EDI	←执行此行为后,下令 D EDI,显示‘cccc’,即输入的注册名
0137: 00407A99	CALL	00407B47	←呼叫计算注册码子程序(新版本)
0137: 00407A9E	MOV	ESI, 0048CDA4	←传送输入的注册码,执行此行后下令 D ESI,显示‘8 个 8’
0137: 00407AA3	LEA	EAX, [EBP + FFFFFFFE0]	
0137: 00407AA9	PUSH	ESI	←将输入的假码‘8 个 8’压入堆栈,下令 DESI,显示‘8 个 8’
0137: 00407AAA	PUSH	EAX	←计算出的注册码压入堆栈,下令 D EAX 显示正确注册码:02EC0252
0137: 00407AAB	CALL	004692D0	←呼叫验证注册码子程序,看看输入的是否为新版注册码。
0137: 00407AB0	ADD	ESP, BYTE + 10	
0137: 00407AB3	NEG	EAX	
0137: 00407AB5	SBB	EAX, EAX	
0137: 00407AB7	INC	EAX	
0137: 00407AB8	MOV	[00489FDC], EAX	
0137: 00407ABD	JNZ	00407B27	←如输入的注册码正确,这里跳转,可返回呼叫程序,可跳过 00408018 CALL,完成程序注册。
0137: 00407ABF	LEA	EAX, [EBP + FFFFFFFE0]	
0137: 00407AC5	PUSH	EAX	
0137: 00407AC6	PUSH	EDI	←执行此行为后,下令 D EDI,显示‘cccc’,即输入的注册名
0137: 00407AC7	CALL	00407BE4	←呼叫计算注册码子程序(老版本)
0137: 00407ACC	LEA	EAX, [EBP + FFFFFFFE0]	
0137: 00407AD2	PUSH	ESI	←将输入的假码‘8 个 8’压入堆栈,下令 DESI,显示‘8 个 8’
0137: 00407AD3	PUSH	EAX	←计算出的注册码压入堆栈,下令 D EAX 显



示正确注册码:07480594

```

0137: 00407AD4 CALL    004692D0    ←呼叫验证注册码子程序,看看输入的是否为
                                新版本注册码。
0137: 00407AD9 ADD     ESP, BYTE + 10
0137: 00407ADC NEG     EAX
0137: 00407ADE SBB    EAX, EAX
0137: 00407AE0 INC     EAX
0137: 00407AE1 MOV    [00489FDC], EAX
0137: 00407AE6 JNZ    00407B27
0137: 00407AE8 LEA    EAX, [EBP + FFFFFFFEC4]
0137: 00407AEE PUSH   BYTE + 04
0137: 00407AF0 PUSH   EAX
0137: 00407AF1 PUSH   ESI
0137: 00407AF2 CALL   004696C0
0137: 00407AF7 ADD     ESP, BYTE + 0C
0137: 00407AFA TEST   EAX, EAX
0137: 00407AFC JNZ    00407B20          (JUMP)
0137: 00407AFE LEA    EAX, [EBP + FFFFFFFEC0]
0137: 00407B04 PUSH   BYTE + 04
0137: 00407B06 PUSH   EAX
0137: 00407B07 PUSH   DWORD 0048CDA8
0137: 00407B0C CALL   004696C0
0137: 00407B11 ADD     ESP, BYTE + 0C
0137: 00407B14 TEST   EAX, EAX
0137: 00407B16 JNZ    00407B20
0137: 00407B18 MOV    [00489FDC], EBX
0137: 00407B1E JMP    SHORT 00407B27
0137: 00407B20 AND    DWORD [00489FDC], BYTE + 00
0137: 00407B27 PUSH   DWORD 012C
0137: 00407B2C LEA    EAX, [EBP + FFFFFFFEC0]
0137: 00407B32 PUSH   BYTE + 00
0137: 00407B34 PUSH   EAX
0137: 00407B35 CALL   00467C10
0137: 00407B3A MOV    EAX, [00489FDC]
0137: 00407B3F ADD     ESP, BYTE + 0C
0137: 00407B42 POP    EDI
0137: 00407B43 POP    ESI

```



```
0137: 00407B44 POP      EBX
0137: 00407B45 LEAVE
0137: 00407B46 RET      ←执行此行返回呼叫程序
至此,找出注册码!
```

7.5 呼吸小秘书(javagirl)的破解

这是一个做主页特效的小软件,内容包括:窗口特效,鼠标特效,文字特效,菜单特效,还有一些常用特效(如计数器)等。软件不注册有功能限制,其注册检测部分同人物生物节律有点相像,不提示出错信息。

这个软件用 aspack1.06 版压过,可以用 prodump 脱壳。软件将注册信息写入注册表 HKEY_USER / SOFTWARE / BREATHSOFT / 注册 / javagirl 下,每次启动时都做比较。注册码与注册名无关,但必须是 13 位,而且只要前 8 位是 BSJG08SN,后 5 位就可以任意填写啦。

破解工具选 TRW2000。

破解过程:

(1)用 trw2000 载入脱壳后的 javagirl.exe;

(2)填写注册信息:name: yubing
code: 78787878

(3)按下 ctrl - n,进入 trw,下断点:

: bpx hmemcpy

: g

(4)按“注册键”,程序立即被拦截,下清除断点指令:

: bc *

: pmodule

(5)按 F10,直到如下程式:

```
0167: 0049A329 MOV EAX, [EBP - 04] &下 d eax 可看到你输入的注册码 78787878
```

```
0167: 0049A32C CALL 00403C00
```

```
0167: 0049A331 CMP EAX, BYTE + 0D &此时 eax 中为注册码个数(8 个),是否为 13 位。
JNZ NEAR 0049A4AF &如果不相等,则出错。
```

```
LEA EAX, [EBP - 04]
```

```
PUSH EAX
```

```
.....
```

```
0167: 0049A36C MOV EAX, [EAX + 0508]
```

```
0167: 0049A372 CALL 0043BAA8
```

```
0167: 0049A377 MOV EDX, [EBP - 08] &下 d edx 可见到注册码 BSJG08SN
```

```
POP EAX &下 d eax 可见到输入注册码的前 8 位。
```




```
CALL 00403D10    &比较注册码的核心, F8 追入
JNZ NEAR 0049A4AF  &不相等则出错。
```

.....

(6)看注册码比较的部分 call 00403D10

```
0167:00403D10  PUSH EBX
                PUSH ESI
                PUSH EDI
                MOV  ESI, EAX    &下 d eax 为你输入的注册码
                MOV  EDI, EDX   &下 d edx 为正确的注册码
                CMP  EAX, EDX   &比较注册码.
0167:00403d19  JZ  NEAR 00403DAE  &相等, 则一定要跳转
```

.....

(7)至此,程序追踪完成,由于注册码必须是 13 位,所以我们前 8 位输入 BSJG08SN 之后,还必须要任意填 5 位。

7.6 最流行的离线浏览器 Teleport Pro 的破解

Teleport Pro 是威力最强大的离线浏览、站台复制以及档案抓取的工具。它是一个能全自动链接追踪以及具有多执行任务的资讯网离线浏览工具。它能让您从网际网络上抓取所有您所需要的档案,并且刚好就只有那些您所要的。不论规模多大的网站,只要你设置妥当,无论网站目录、内容、图片影像、背景音乐,甚至 Java Applet 都能够完整地复制一份在你的硬盘中。Teleport Pro 所能做的,不仅仅是离线浏览某个网页,它还可以从 Internet 的任何地方抓回你想要的任何文件(例如某个站点的全部 MIDI 文件或 MP3 文件),它可以在你指定的时间自动登录到你指定的网站下载你指定的内容,另外它还可以随意设定下载的深度。等到这些文件全部传回来之后,你只要用你常用的浏览器浏览自己硬盘中的文件就可以了,从此不必再忍受在屏幕前发呆的窘境了。

现在我们开始,从“开始”→“程序”→“Teleport Pro”→“Teleport Pro”弹出操作界面,跟着“Help”→“About Teleport Pro”,弹出注册窗口。

Username: 填入 YanHuaQi (因为此处要求 6 个字母以上)

Company: CSMC

注册码: 87654321 (先乱填一通)

开始吧!先按下 Ctrl - D 切入到 SoftICE 下,设断点: bpx hmemcpy。紧跟着按 F5 键,切回到 Teleport Pro,然後按下 OK 键,SoftICE 会拦下 Teleport Pro,把拦截中断的功能关掉: BD *。按几次 F12,跳回到 Teleport Pro 领空下,然後一直按 F10 键一直到下面:

```
XXX: 0040E3C6 JZ 0040E48B
```

```
XXX: 0040E3CC LEA EDI, [ESI + 000000D5]
```



XXX: 0040E3D2 MOV EAX, [EDI]

XXX: 0040E3D4 PUSH EAX

XXX: 0040E3D5 CALL 0041BAD0

这是算注册码的 CALL

XXX: 0040E3DA ADD ESP, 04

XXX: 0040E3DD CMP EAX, EBP

这里非常重要,是核心部分。

XXX: 0040E3DF JNZ 0040E497

若 EAX 和 EBP 不相同,就跳到 0040E497,那就 GAME OVER 啦,所以执行到 XXX: 40E3DD 那行时,应看一下 EAX 和 EBP。

EBP: 05397FB1

呵呵,这不就是 87654321 的 16 进位值...

EAX: 50CCD6BA

这可是真正的注册码,赶快换算成 10 进位,答案就是: 1355601594。

整理一遍:

username: YanHuaQi

company: CSMC

password: 1355601594

下面再用 SoftICE4.05 结合 W32DASM 来破解它。

(1)用 W32dasm 打开执行文件,默认的安装目录 c:\progra~1\teleport pro\pro.exe,将其反汇编,查找字符串“Thank you! Your copy of Teleport Pro is now registered.”

你会找到如下代码:

* Possible Reference to

String Resource ID = 07028: “Thank you! Your copy of Teleport Pro is now registered. Al”

```

:00425F78 68741B0000      push 00001B74
:00425F7D 8D4DF0          lea ecx, dword ptr [ebp - 10]
:00425F80 895DFC          mov dword ptr [ebp - 04], ebx
    
```

.....

(2)向上看,有如下的代码(分析见右边注释)

```

:00425F29 8B87DD000000    mov eax, dword ptr [edi + 000000DD]
:00425F2F 33DB            xor ebx, ebx
:00425F31 6A0A            push 0000000A
:00425F33 53              push ebx
:00425F34 50              push eax
:00425F35 E85B690000      call 0042C895
:00425F3A 8B0D68F04700    mov ecx, dword ptr [0047F068]
    
```



Pc friend

```

: 00425F40 83C40C          add esp, 0000000C
: 00425F43 8945E8          mov dword ptr [ebp - 18], eax
: 00425F46 3899DB040000    cmp byte ptr [ecx + 000004DB], bl
: 00425F4C 0F8412020000    je 00426164
: 00425F52 3BC3           cmp eax, ebx
* Possible StringData Ref from Data Obj →“User”

```

```

: 00425F54 BEB8C94700      mov esi, 0047C9B8
: 00425F59 0F8406010000    je 00426065
: 00425F5F FFB7D5000000    push dword ptr [edi + 000000D5]
: 00425F65 E896090000      call 00426900

```

;F8 追入。

```

: 00425F6A 3945E8          cmp dword ptr [ebp - 18], eax
;比较什么?

```

```

: 00425F6D 59             pop ecx
: 00425F6E 753A          jne 00425FAA

```

;此处不跳转,则胜利在望,如跳转则死路一条。

```

: 00425F70 A114D44700      mov eax, dword ptr [0047D414]
: 00425F75 8945F0          mov dword ptr [ebp - 10], eax

```

(3)用 ICE 载入 pro. exe。

: bpx 00425f5f29

: g

回到程序填入注册信息:

name: yubing

company: [CCG]

registration: 78787878 (随便)

按“OK”程序被拦如下:

```

: 00425F29 8B87DD000000    mov eax, dword ptr [edi + 000000DD]←78787878 送 eax

```

```

: 00425F2F 33DB           xor ebx, ebx

```

```

: 00425F31 6A0A          push 0000000A

```

```

: 00425F33 53           push ebx

```

```

: 00425F34 50           push eax

```

;可知 eax 中存放 78787878 的十六制 4b23526

```

: 00425F35 E85B690000      call 0042C895

```

```

: 00425F3A 8B0D68F04700    mov ecx, dword ptr [0047F068]

```

```

: 00425F40 83C40C          add esp, 0000000C

```

```

: 00425F43 8945E8          mov dword ptr [ebp - 18], eax

```



```
;将 4b23526 送[ebp - 18]
:00425F46 3899DB040000      cmp byte ptr [ecx + 000004DB], bl
:00425F4C 0F8412020000      je 00426164
:00425F52 3BC3              cmp eax, ebx
:00425F54 BEB8C94700        mov esi, 0047C9B8
:00425F59 0F8406010000      je 00426065
:00425F5F FFB7D5000000      push dword ptr [edi + 000000D5]
:00425F65 E896090000        call 00426900

;F8 追入。
:00425F6A 3945E8           cmp dword ptr [ebp - 18], eax
;用什么和 4b23526 比较。
:00425F6D 59              pop ecx
:00425F6E 753A           jne 00425FAA

;此处不跳转,否则就该结束了。
:00425F70 A114D44700      mov eax, dword ptr [0047D414]
:00425F75 8945F0         mov dword ptr [ebp - 10], eax
(4)在 call 00426900 追入分析,按 F10 继续,直到
|
:00426914 83F805         cmp eax, 00000005
;比较输入注册名的个数是否大于 5
:00426917 7304           jnb 0042691D
;不于 5,则提示错误。
:00426919 33C0           xor eax, eax
:0042691B 5F            pop edi
:0042691C C3            ret
:0042691D 53            push ebx
:0042691E 56            push esi
;下面的留意。
:0042691F BEA4E4FE5D     mov esi, 5DFEE4A4
:00426924 33DB           xor ebx, ebx
:00426926 85FF           test edi, edi
:00426928 7409           je 00426933
:0042692A 57            push edi
:0042692B E8F0560000     call 0042C020
:00426930 59            pop ecx
:00426931 EB02           jmp 00426935
:00426933 33C0           xor eax, eax
```



```

:00426935 83C0FC          add eax, FFFFFFFC
:00426938 3BD8             cmp ebx, eax
:0042693A 730C             jnb 00426948
:0042693C 33343B          xor esi, dword ptr [ebx + edi]
:0042693F F6C340          test bl, 40
:00426942 7401             je 00426945
:00426944 43              inc ebx
:00426945 43              inc ebx
:00426946 EBDE             jmp 00426926
;将输入的姓名变换得到正确的注册码,进一步可以得到注册机。
:00426948 8BC6             mov eax, esi
;将得到的正确的注册码送至 eax 中
:0042694A 5E              pop esi
:0042694B 5B              pop ebx
:0042694C 5F              pop edi
:0042694D C3              ret

```

5、开始整理正确的注册码,在

```

:00425F6A cmp dword ptr [ebp - 18], eax
? eax 就可看见正确的注册码,赶快拿笔记下十进制的数,去注册吧。

```

7.7 Explor2000 V1.51 强迫注册法

对于 Explor2000 的注册要用到下面的工具:TRW2K V1.03、UltraEdit - 32。由于 Explor2000 用 Aspack 压缩过,所以先要脱壳,然后再进行破解。首先用 TRW2K 脱壳,启动 TRW2K,将 Explor2000 的图标拖入 TRW2K,点击 LOAD;拦下后按 F10,直到来到一个反复跳跃的地方,按 F12,马上再按一下 LOAD,应在 006E6501 处拦下,按一下 F10 来到 0059D178(注意 TRW2K 的 DEBUG 窗口中的变化,从 EXPLOR2000!. Aspack + ???变成 EXPLOR2000! Code + ???),下 PEDUMP 指令脱壳。找到 PEDUMP1.EXE 后改名成 EXPLOR2000.EXE 并复制到 Explor2000 的目录即可。(请不要下 G 0059D178 指令,否则脱壳时会当机)

现在我们开始破解软件,还是用 TRW2K 载入 Explor2000,点击 LOAD,在 59D178 处拦下,TRW2K 中出现很多问号,不要管它,按一下 F10 便正常,一直按 F10 来到:

```

59D218 CALL 0045262C    &按 F8 进入按 F10 来到:      4526A5 CALL 0044C4FC
&光标经过此 CALL 弹出 E2K 的主画面
4526AA MOV  EAX, [EBP - 04]
4526AD CALL 00452498    &光标第 4 次经过次 CALL 弹出干扰画面
MOV  EAX, [EBP - 04]

```



```
CMP Byte Ptr [EAX + 00000084], 00
```

```
4526BC JZ 004526AA &程序在这里反复跳跃
```

由于光标第 4 次经过 4526AD 时会弹出干扰画面,于是当光标第 4 次走到 4526AD 上时按 F8 进入此 CALL,进入后按 F10 来到:

```
4524A2 CALL 004523E8
```

光标经过此 CALL 会弹出干扰画面,按 F8 进入(由于相同的原因,下面有 6 个 CALL 都要按 F8 进入,就不一一说明了,仅把它们列出来:

```
1:56E39F CALL 0058120C
```

```
2:581343 CALL 0058195C
```

```
3:58196E CALL 005106E0
```

```
4:510755 CALL 00511934
```

```
5:511949 CALL Near [EBX + 000000A0]
```

```
6:581C0E CALL 00581ACC )
```

按 F8 进入 581C0E CALL 00581ACC 后一直按 F10 直到出现干扰画面,点击一下 OK 后又被拦下,如下:

```
581B29 CMP Byte Ptr [EDX + 74], 00 令[EDX + 74]的值为 1
```

```
JNZ 00581B3F 跳过关键 CALL1
```

```
PUSH ESI
```

```
PUSH 005814F4
```

```
PUSH EAX
```

```
MOV ECX,EBX
```

```
MOV EAX,ESI
```

```
581B3A CALL 005815C0 &关键 CALL1
```

```
DEC EBX &光标停在这
```

只要令[EDX + 74]的值为 1 便可以避开关键 CALL1,于是我们再来一次,用 TRW2K 载入后下 G 581B29 指令(有时会没有反应,多试几次)拦下后下 E 012F8EDC 1 指令可令[EDX + 74]的值为 1,按 F10,成功跳过关键 CALL1。别高兴太早,下面还有陷阱,一直按 F10 直到弹出干扰画面,点击 OK 又被拦下,如下:

```
581388 CALL 005815C0 &关键 CALL2
```

```
LEA EDX,[EBP - 08] &光标停在这
```

按 F6,移动光标向上看看哪可以避开关键 CALL2,如下:

```
58135E CALL 005816AC
```

```
581363 TEST AL,AL &令 AL 的值为 1
```

```
581365 JNZ 0058138D &跳过关键 CALL2
```

现在知道怎么改程序了吗?答案是:

CMP Byte Ptr [EDX + 74], 00 → INC Byte Ptr [EDX + 74] 由于少 1 个 Byte,所以加一个 NOP。



TEST AL, AL → MOV AL, 01

下 CODE ON,记下机器码。用 Uedit32 打开 Explor2000.exe

查找: 84C075268B45FCE82506

修改为:B001 - - - - -

查找: 807A74007510

修改为:FE427490 - - - -

存盘后试运行 Explor2000,没有了干扰画面。查看 About 项,窗口写着“User license granted to”,因为是强迫注册的,所以没有名字,而是空白。



附录 softice&trw2000 指令详解

附录包括每个命令的语法、解释及范例。所有的数字均以 16 进位表示。使用到 + - * / 或暂存器的数字均可视为运算式。所有的命令都不区分大小写。命令语法叙述中的斜体字需以真实的值代替而不是打入斜体字。

以下是附录中所使用的代号：

[]——语法中非必用的部分

< >——可选用的部分

X|Y——使用 X 或 Y(X Y 择一使用)

count——count 指定断点条件要成立几次才会真正引发中断。如果没有设定,内定值是 1。每次引发中断而叫出 Soft - ICE 的视窗后,记数器自动回复为原先指定值。

verb——指定在什么状况下断点会做用。R 代表读取;W 代表写入;RW 代表读取及写入;X 代表执行。

address——地址。由两个 16 位元的字以冒号分隔而组成。第一个字代表区段地址,第二个字代表差距地址。地址可以由符号或暂存器构成,也可以包括\$、.、@等特殊符号。参阅 3.8 以取得更多资讯。

break - number ——断点号码是在你修改断点(即编辑、删除、重新启动、暂停作用)时使用的。它是用来代表各断点的代码。断点号码是由 0 到 F。

list——一串由逗号或空白分隔的断点号码。

mask——由 1、0、X 所构成的位元屏蔽。X 代表不处理的位元。

例如: BPIO 21W EQ M 1XXX XXXX

如果 21 端口被写入且造成其高位元被设定则会引发中断。

一、设置断点命令

命令:

BPM BPMB BPMW BPMD——在内存地址被存取或执行时引发中断

BPR——对内存范围设置断点

BPIO——对 I/O 端口存取时触发中断

BPINT——呼叫中断时触发中断

BPX——设置 / 清除 执行断点

CSIP——CS:IP 范围的检定判断



Pc friend ·

BPAND——等待复合断点的发生

BPM BPMB BPMW BPMD——在内存地址被存取或执行时引发中断

语法: BPM [size] address [verb] [qualifier value] [C = count]

size —— B、W、D

B —— byte 字节 W —— word 字 D —— Double word 双字

size 是指断点所涵盖的范围。举例来说,如果使用的是双字,而其第三个字节被改变了,就会引发中断。如果有指定判断资格(qualifier),size 也是很重要的。

verb —— R、W、RW 或 X

qualifier —— EQ、NE、GT、LT、M

EQ —— 相等 NE —— 不等 GT —— 大于

LT —— 小于 M —— 屏蔽

qualifier 只有在读写断点才有用到。

value —— 由断点大小决定是字节、字或双字的值

解说:

BPM 命令会在内存读、写或执行时引发中断。

verb 内定值为 RW; size 内定值为 byte。

除了 X 外的 verb 值会使程序执行引发中断的那段程序码。CS:IP 所指的是引发中断的最后一行程序码。如果 verb 值是 X,CS:IP 所指的是断点设置的位置。

如果设定的是 R,当内存地址被读取或做没有改变的写入时,将引发中断。如果设定的是 R、W、RW 时,指定的地址被执行时并不会引发中断。

[注]如果使用 BPMW,指定的地址必须由字边界开始。如果使用 BPMD,指定的地址必须指向一个双字边界。

[例] BPM 1234:SI W EQ 10 C = 3

这道命令设定一个字节的内存存取断点。当 10H 第三次写入 1234:SI 时将启动断点。

[例] BPM CS:1235 X

这道命令设定一个执行断点。当 CS:1235 的程序码被执行时将引发中断。此时 CS:IP 所指的就是断点设定地址。

[例] BPMW DS:F00 W EQ M 0XXX XXXX XXXX XXX1

这道命令设定一个字的内存写入断点。当 DS:F00 被写入一个高位元为 0,低位元为 1(其他位元不考虑)的资料时,将引发中断。

[例] BPM DS:1000 W GT 5

这道命令设定一个字节的内存写入断点。当 DS:1000 被写入一个大于 5 的值时,将引发中断。

BPR——对内存范围设置断点

语法: BPR start - address end - address [verb] [C = count]

start - address、end - address —— 界定范围的开始及结束地址



verb —— R、W、RW、T 或 TW

解说:

BPM 命令让你对一段内存范围设断点。

除了 T 和 TW 外的 verb 值均会执行引发中断的程序码。CS:IP 将指向引发中断的下一段程序码。

你不能设定执行的范围断点。如果想做到执行的范围断点必须使用 R。

程序码的引出被视为是对范围断点的读取。

如果未指定 verb, 内定值是 W。

在某些状况下, 设置范围断点会降低系统的性能。Soft-ICE 将会分析所有对包括范围断点的 4K 内存的读写动作。性能的降低通常无法察觉, 但也可能有严重降低的例外。

verb 值使用 T 或 TW 将在指定范围内可以做回溯跟踪 (back trace)。它们并不会真正引发中断而只是记录下程序码的资料。这个资料可以用 SHOW 或 TRACE 命令显示出来。参阅第九章以取得更多有关回溯跟踪的资讯。

〔例〕 BPR B000:0 B000:1000 W

这道命令定义一个内存范围的断点。任何对单色影像内存的写入均会引发中断。

BPIO——对 I/O 端口存取时触发中断

语法: BPIO port [verb] [qualifier value] [C = count]

port —— 一个字节或字形态的值

verb —— R、W 或 RW。R —— read (IN) W —— write (OUT)

qualifier —— EQ、NE、GT、LT、M

EQ —— 相等 NE —— 不等 GT —— 大于

LT —— 小于 M —— 屏蔽

value —— 一个字节或字形态的值

解说:

BPIO 命令会在 I/O 端口读写时引发中断。

如果有指定 value 值, 它将被拿来和引发中断的 IN、OUT 程序码所读/写的真正资料值做比较。value 可以是一个字节或字。如果是对一个字节的端口做 I/O, 则是使用较低的 8 位元来做比较。

CS:IP 将会指向引发中断的程序码的后一段程序码。

如未指定 verb, 内定值是 RW。

〔例〕 BPIO 21 W NE FF

这道命令定义一个 I/O 端口存取断点。如果一号中断控制器的屏蔽暂存器被写入除了 FFh 的外的值, 将会引发中断。

〔例〕 BPIO 3FE R EQ M 11XX XXXX

这道命令定义一个字节的 I/O 端口读取断点。如果 3FEh I/O 端口被读取, 且这个值的二高位元是 1 时, 将会引发中断。其他位元可以是任意值。

**BPINT —— 呼叫中断时触发中断**

语法: BPINT INT - NUMBER [< AL | AH | AX > = value] [C = count]

int - number —— 由 0 到 FFh 的中断号码

value —— 一个字节或字的值

解说:

BPINT 命令可以在呼叫硬件中断或软件中断时引发中断。藉由指定 AX 暂存器的值可以轻易分离指定的 DOS 或 BIOS 呼叫。

如果没有指定 value 值,在呼叫指定的中断向量时将引发中断。这个中断可以是硬件中断、软件中断或内部中断。

选定的 value 值当中断发生时将与指定的暂存器比较 (AH、AL 或 AX)。如果其值和指定的暂存器值相同时,将引发中断。断点引发时,如果是硬件中断,CS:IP 将指向此中断程序的第一段程序码。使用 INT? 命令可以得知此中断呼叫发生时执行到哪里。如果是软件中断,则 CS:IP 将指向呼叫此中断的程序码。

〔例〕BPINT 21 AH = 4C

这道命令定义一个 21h 中断的断点。当 DOS 4Ch 函式(结束程序)被呼叫时将引发中断。

BPX —— 设置 / 清除 执行断点

语法: BPX [address] [C = count]

解说:

BPX 命令让你在原始程序中 设置/清除 执行断点。如果游标在程序码窗中,则不需要输入地址,执行断点将设置在目前游标所在地址。如果目前游标所在地址已经设置一个执行断点,则将清除此断点。

如果程序码窗是不可见的或游标未在其中,则必! 指定地址。如果只有指定差距地址,目前的 CS 值会被当做节段地址。

〔注〕除非断点的位置在 ROM 中,不然 BPX 均使用 INT 3 的方式设置断点。用这样来取代断点暂存器是为了能设置更多的断点。如果你的处境因某些原因必须使用断点暂存器(例如说程序码未载入),你可以用 BPM 命令设置执行断点。

〔例〕BPX .1234

这道命令将在原始程序第 1234 行设置断点。

CSIP —— CS:IP 范围的检定判断

语法: CSIP [OFF | [NOT] start - address end - address]

NOT —— 如果使用 NOT,只有当 CS:IP 所指超出范围,才会引发中断。

OFF —— 停止对 CS:IP 的检定。

解说:

CSIP 命令会使断点的成立条件由命令指标所指地址而定。这个功能在你怀疑程序会突然修改其范围的外的程序码时特别有用。



当断点条件成立时,CS:IP 暂存器会被拿来和指定的范围做比较。当其在范围内时会引发中断。要在 CS:IP 指在范围外时引发中断,则需要用 NOT 参数。

如果没有加参数则会显示目前 CS:IP 的范围。

〔例〕CSIP NOT F000:0 FFFF:0

这个命令只有在断点条件成立且 CS:IP 并未指向 ROM BIOS 时才会引发中断。

BPAND——等待复合断点的发生

语法: BPAND list | * | OFF

list —— 一串由逗号或空白分开的断点号码。

* —— 复合所有的断点。

解说:

BPAND 命令会对二或多个断点做逻辑的 AND 运算。只有当所有的断点条件均成立时才会真正引发中断。

有些情况下你会希望在许多不同条件均成立下才引发中断。BPAND 命令让你指定二或多个在断点发生前必须成立的断点。这个功能让你可以设置更复杂的断点条件。

每次使用 BPAND 命令均会把指定的断点号码加入名单中,直到使用 BPAND OFF 命令为止。

你可以用 BL 命令列出断点以察看哪些断点号码被复合在一起。被复合在一起的断点其断点号码后会有个 & 。

一旦断点被复合后,除非此断点被清除或 BPAND 被关闭才会中止。

〔例〕BPAND 0,2,3

这道命令将复合 0 号、2 号、3 号断点。只有当三个的条件均成立时才会引发中断。例如:如果 2 号和 3 号的条件均成立一次以上,但 0 号的条件尚未成立,则只有当 0 号的条件成立时才会引发中断。

二、处理断点

Soft-ICE 提供许多命令来处理断点。处理类的命令可以用来列出、修改、删除、启动和中止断点。断点是以由 0h 到 Fh 的断点号码来识别的。处理中断点的命令有:

BD——中止断点

BE——启动断点

BL——列出断点

BPE——编辑断点

BPT——把断点当样板

BC——清除断点

BD——中止断点

语法: BD list | *



Pc friend ·

list —— 一串由逗号或空白分开的断点号码。

* —— 中止所有断点。

解说:

BD 命令是用来暂时中止断点的活动的。断点可用 BE 命令(启动断点)重新启动。

你可以用 BL 命令列出断点以查看哪些断点被中止了。被中止的断点其断点号码后会有一个 * 。

〔例〕 BD 1,3

这道命令会暂时中止 1 号和 3 号断点。

BE——启动断点

语法: BE list | *

list —— 一串由逗号或空白分开的断点号码。

* —— 启动所有断点。

解说:

BE 命令是用来重新启动被 BD 命令中止的断点。当断点第一次定义时将会自动启动。

〔例〕 BE 3

这道命令会启动 3 号断点。

BL——列出断点

语法: BL

解说:

BL 命令会显示所有目前设定的断点。BL 命令会列出每个断点的断点号码、断点条件、断点状态和计数。

断点的状态分为启动和中止。中止的断点其断点号码后面会有个 *。在 BPAND 命令中使用的启动的断点其断点号码后面会有个 &。最后一个引发中断的断点会以高亮度显示。

BL 命令没有参数。

〔例〕 BL

这道命令会显示所有定义的断点。以下列出一个 4 个断点的例子:

0) BPMB 1234:0000 W EQ 0010 C = 03

1) BPR B000:0000 B000:1000 W C = 01

2) BPIO 00021 W NE OOFF C = 01

3) BPINT 21 AH = 4C C = 01

BPE——编辑断点

语法: BPE break - number

解说:

BPE 命令会把断点的叙述放到编辑行以供修改。然后你可以用编辑键重新编辑,按 Enter 重新输入。这个命令让你可以快速修改原有断点的参数。



〔例〕 BPE 1

这道命令会把 1 号断点的叙述搬到编辑行并清除原 1 号断点。按 Enter 可以把这个断点重新输入。

BPT——把断点当样板

语法: BPT break - number

解说:

BPT 命令会把已存在的断点叙述拿来当新断点的样板。

原存在的断点叙述会被放到编辑行去。断点号码所指的断点并没有任何改变。这个命令让你可以快速的设置和原断点相似的新断点。

〔例〕 BPT 3

这道命令会把 3 号断点的样板放入编辑行。当你按下 Enter 后会增加一个新断点。

BC——清除中断

语法: BC list | *

list —— 一串由逗号或空白分开的断点号码。

* —— 启动所有断点。

解说:

BC 命令是用来永远清除一个或多个断点的。

〔例〕 BC *

这道命令会清除所有的断点。

三、显示及编辑类命令

命令:

U——反编译或显示原程序码

R——显示或更改暂存器

MAP——显示系统内存分布图

D——用最后一次指定的形式显示内存

DB——以字节的形式显示内存

DW——以字的形式显示内存

DD——以双字的形式显示内存

E——用最后一次指定的形式编辑内存

EB——以字节的形式编辑内存

EW——以字的形式编辑内存

ED——以双字的形式编辑内存

INT?——显示最后一次呼叫的中断号码

? 或 H——显示辅助信息



Pc friend

VER——显示 Soft - ICE 的版本号码

U——反编译或显示原程序码

语法: U [address] [L [=] length]

length —— 要反编译的程序码长度

解说:

U 这个命令会显示正在调试的程序的程序码。

如果没有指定 length ,内定值是 8 行或屏幕长度减一。

如果未指定 address ,这个命令会从最后一次反编译的后一字节开始反组译。如果从未使用过反编译命令,则从目前 CS:IP 开始。

如果程序码窗是可见的,则程序码会显示在其中。

如果指定的地址范围的原始程序码有载入,由目前的原始码模式来决定是否显示原始码。

〔例〕 U \$ - 10

这道命令从目前地址的前 10h 字节开始反编译。

〔例〕 u .499

这道命令会从 499 行开始显示 原始码。程序码窗必须是可见的且必须在原始码模式。

R——显示或更改暂存器

语法: R register - name [[=] value]

register - name —— 为下列任一:

AL 、AH 、AX 、BL 、BH 、BX 、CL 、CH 、CX 、DL

DH 、DX 、DI 、SI 、BP 、SP 、IP 、CS 、DS 、ES

SS 、或 FL

value —— 如果 register - name 不是 FL ,value 是个 16 进位值或运算式。若 register - name 为 FL,value 下列旗号符号一或多个的组合。旗号符号可视需要在前面加上 + 或 - 。

O —— Overflow flag 溢位旗号

D —— Direcrion flag 方向旗号

I —— Interrupt flag 中断旗号

S —— Sign flag 正负号旗号

Z —— Zero flag 零值旗号

A —— Auxiliary carry flag 辅助进位旗号

P —— Parity flag 极性旗号

C —— Carry flag 进位旗号

解说:

R 命令是用来显示或更改暂存器的值的。

如果没有指定参数会显示所有暂存器和旗号的值及目前 CS:IP 的程序码。

如果仅指定 register - name 而未加 value ,则 Soft - ICE 会显示指定暂存器现在的值并提示你输入新值。如果 register - name 是 FL ,目前设置的旗号会以高亮度大写显示;未设置的旗



号则用普通小写显示。要维持现在暂存器的值,直接按 Enter。

如果 register - name 和 value 均有指定,则指定的暂存器的值将被改成 value。

想要改变旗号的值,把 FL 当 register - name,后接你想切换的旗号符号。

如果要设置某旗号,在旗号符号前加上 +。要关闭某旗号,则在旗号符号前加上一个 -。旗号可以按任何顺序排列。

[例] R AH 5

这道命令会把 AH 暂存器的值改成 5。

[例] R FL = O Z P

这道命令会切换 O、Z、P 旗号的值。

[例] R FL

这道命令会显示目前旗号的值并让你可以修改其值。

[例] R FL O + A - C

这道命令会切换 O 旗号,设置 A 旗号并关闭 C 旗号。

MAP——显示系统内存分布图

语法: MAP

解说:

MAP 命令显示各内存部分的名称、位置和大小。大小是以页来计算的。一页等于 10h byte。

CS:IP 所指的部分会以高亮度显示。

使用 MAP 命令的时机:

* 断点发生时指向未知的内存区段。

* 你想控制常驻程序或系统程序。你可以根据 MAP 命令所显示的开始地址大小来设置范围断点。

* 你怀疑程序或系统在其内存空间的外写码。MAP 命令可用来找出此区段的内存地址以便在 CSIP 中使用。

* 你必须找出哪个常驻程序拥有目前的中断向量。

[例] MAP

以下是这道命令显示的范例:

.....

若 DOS 的版本低于 3.1,将显示程序的地址而非其程序名称。

D DB DW DD——显示内存

语法: D [size] [address] [L [=] length]

size ——B —— byte W —— word D —— double word

length —— 要显示几字节。

解说:

D 这个命令会显示指定地址的内存内容。



内存内容是以指定的 size 的形式显示。如果没有指定 size ,会以最后一次使用的 size 来显示。所有的形式均会显示 ASCII 码。

如果未指定 address ,则由前一次显示的最后一字节的后一字节开始显示。

如果没有指定 length ,内定值是 8 行或因视窗较小而少一些。

若资料窗是可见的,则资料会显示在资料窗且 length 会被忽略。

〔例〕 DW DS:00 L=8

这道命令会以字和 ASCII 的形式显示目前资料节段的前 8 字节。

E EB EW ED——以字节的形式编辑内存

语法: E [size] address [data - list]

size ——B —— byte W —— word D —— double word

data - list —— 一串指定的 size 的资料,(字节、字或双字)或以逗号、空白分隔的加引号字符串。加引号的字符串可以使用单引号或双引号。

解说:

E 命令显示指定地址的内存内容并让你编辑其值。

这个命令以 ASCII 的形态显示内存内容,并且是以指定的 size 形态。

内存编辑器让你可以快速地更新内存。你可以键入 ASCII 字元或打入位元组、字、双字的值以编辑内存。如果没有指定 size,以最后一次使用的 size 为准。以下是内存编辑的按键:

- 游标上移
- 游标下移
- 游标右移
- 游标左移

SPACE —— 游标移至下一个元素上

TAB —— 在数字区和 ASCII 区间切换

ESC 或 Enter —— 离开内存编辑器

在你输入资料的时候,真正内存上的值也随之更新。所有的数字值都是以 16 进位表示。按 Tab 键可以在数字区和 ASCII 区间切换。

如果资料窗是可见的,则在其中修改资料;否则在命令窗中修改。

资料显示的长度,在命令窗中内定为 8 行。如果资料窗是可见的,则和资料窗同大小。

如果未加参数且资料窗是可见的,则游标会移到资料窗中。若资料窗是不可见的,则在命令窗中由最后一次显示或编辑的地址开始进行编辑。

〔例〕 EB 1000:0

这道命令由 1000:0000 开始,以字节的形态,用数字和 ASCII 字元显示资料的值。你可以编辑这些显示出来的值。

〔例〕 EB 8000:0 "HELLO",0D

这道命令把从 8000:0000 开始的值以 HELLO 字符串和一个归位字元代替。

INT?——显示最后一次呼叫的中断号码



语法: INT?

解说:

INT? 命令显示最后一次发生的中断号码及其地址。

[例] INT?

以下是 INT? 显示结果的例子:

Last Interrupt: 16

At: 0070:0255

这个例子显示在 Soft-ICE 视窗被叫出的前,系统最后一次呼叫的是 16h 中断,地址在 0070:0255。如果最后一次中断是个软件中断,从 0070:0255 做反编译会显示此中断的程序码。若是个硬件中断,反编译则会显示中断发生时所执行的程序码。

? 或 H——显示辅助信息

语法: < ? | H > [command | expression]

解说:

? 和 H 命令两者均会显示辅助信息。

如果未指定参数将会一次一个屏幕的显示所有命令和运算子的简单解说。按任意键以继续显示或按 ESC 键离开辅助说明。

若有指定参数则会显示包括命令语法及范例的详尽说明。

如果加上运算式,则会计算并以 16 进位、10 进位及 ASCII 字元显示其结果。

[例] ? ALTKEY

这道命令会显示包括 ALTKEY 命令的语法及范例的资料。

[例] H 10 + 14 * 2

这道命令会显示: 0038 00056 “8”。这是 10 + 14 * 2 的 16 进位、10 进位值及 ASCII 字元。

VER——显示 Soft-ICE 的版本号码

语法: VER

[例] VER

这道命令会显示 Soft-ICE 的版本及 Nu-Mega 的版权信息。

四、I/O 端口命令

命令:

I、IB——由字节 I/O 端口输入

IW——由字 I/O 端口输入

O、OB——由字节 I/O 端口输出

OW——由字 I/O 端口输出

I、IB、IW——由 I/O 端口输入

语法: I [size] port



Pc friend ·

size —— B —— byte W —— word D —— double word

port —— 一个字节或字的值

解说:

这个由端口输入的命令是用来读取及显示硬件端口的值的。你可以从字节或字组端口输入。如果没有指定 size, 内定值是字节。

[例] I 21

这道命令是显示一号中断控制器的屏蔽寄存器的值。

O、OB、OW——由字 I/O 端口输出

语法: O [size] port value

size —— B —— byte W —— word D —— double word

port —— 一个字节或字的值

value —— 位元端口为一字节值; 字端口为一字值

解说:

对端口输出的命令是用来对硬件端口写值的。你可以对字节端口或字端口做输出, 如果没有指定 size, 内定值是字节。

[例] O 21 FF

这道命令会屏蔽住一号中断控制器的所有中断。

五、转换控制命令

命令:

X——离开 Soft - ICE 的视窗

G——执行到某地址

T——跟踪一道程序码

P——单步执行程序

HERE——执行到目前游标那行

GENINT——强制某一中断

EXIT——强制离开目前的 DOS 程序

BOOT——载入系统 (保留 Soft - ICE)

HBOOT——硬件系统载入 (完全重设)

X——离开 Soft - ICE 的视窗

语法: X

解说: X 命令会离开 Soft - ICE 视窗并恢复因叫出 Soft - ICE 而中断的程序的控制权。Soft - ICE 视窗会消失。如果有设置任何断点, 它将被启动。

G——执行到某地址

j



语法: G [= start - address] [break - address]

解说:

G 命令会离开 Soft - ICE 视窗并设置一个只用一次的执行断点。除此的外,所有的 sticky 断点也会被启动。

若有指定 start - address 参数,将从 start - address 开始执行;否则会从目前的 CS:IP 开始执行。程序将一直执行,直到达到 break - address、使用了叫出视窗的热键或 sticky 断点发生才会停止。

break - address 必须是一道程序码的第一字节。

当达到指定的 break - address 时,CS:IP 将指向设置断点的位置。

未加参数的 G 命令和 X 命令有相同的作用。

除非所有的断点暂存器都被 sticky 断点占满了,不然 non - sticky 中断点会使用 80386 断点暂存器。在这种状况下,断点将会使用 INT 3 方式。这种情形下,在 ROM 中 G 或 P 命令将无法正常工作。如果你尝试这样做将会显示出错误信息。

[例] G CS:1234

这道命令将在 CS:1234 设置一个只用一次的执行断点。

T——跟踪一道程序码

语法:T [= start - address] [count]

解说:

T 命令使用单步旗号以单步执行一道程序码。

如果没有指定 start - address,将从目前的 CS:IP 开始执行。若有指定 start - address,则 CS:IP 将指向 start - address 以进行单步执行。

如果有指定 count,Soft - ICE 将单步执行 count 次。TRACE 命令将持续执行直到 count 为零或按了 ESC 键,而不管是否有断点发生。

若是在原始码模式,T 命令会单步到下一道原始码叙述。如果目前的叙述是个程序或呼叫函数且呼叫的程序的原始码存在,T 命令会单步执行进入这个呼叫。如果没有呼叫的程序或函数的原始码,T 命令会单步执行完整个程序。

[例] T = 1284 3

这道命令会单步执行在内存地址 1284 的 3 道程序码。

P——单步执行程序

语法: P

解说:

P 命令是个逻辑的程序单步执行。除非目前 CS:IP 的程序码是呼叫、中断、回圈或反复字符串,不然将执行此程序码。若为呼叫、中断等程序码,将会执行完整个程序或反复动作才会回到 Soft - ICE。

P 命令会设置一个只用一次的执行断点。除非所有的断点暂存器都被 sticky 断点占满了,不然 non - sticky 断点会使用 80386 断点暂存器。



Pc friend ·

在这种状况下,断点将会使用 INT 3 方式。这种情形下,在 ROM 中 G 或 P 命令将无法正常工作。如果你尝试这样做将会显示出错误信息。

若是在原始码模式,P 命令会单步到下一道原始码叙述。如果目前的叙述是个程序或呼叫函数,P 命令会把它整个执行完。

〔例〕 P

这道命令会单步执行程序。

HERE——执行到目前游标那行

语法: HERE

解说:

HERE 命令会一直执行到目前游标所在那行。只有当游标在程序码窗中才能使用 HERE 命令。如果程序码窗不可见或游标不在其中,用 G 命令代替。

HERE 命令会离开 Soft - ICE 视窗并设置一个只用一次的执行断点。此外,所有的 sticky 断点也会被启动。

程序将由目前的 CS:IP 开始执行,直到执行到游标所在位置的程序码、使用了叫出视窗的热键或某 sticky 断点发生为止。

除非所有的断点暂存器都被 sticky 断点占满了,不然 non - sticky 中断点会使用 80386 断点暂存器。在这种状况下,断点将会使用 INT 3 方式。这种情形下,在 ROM 中 G 或 P 命令将无法正常工作。如果你尝试这样做将会显示出错误信息。

〔例〕 HERE

这个例子在目前游标所在设置一个执行断点,然后离开 Soft - ICE 并从目前的 CS:IP 开始执行。

GENINT——强制某一中断

语法: GENINT INT1 | INT3 | NMI | interrupt - number

interrupt - number —— 00 到 FF 中的一个数字

解说:

GENINT 命令会强制发生某一中断。当 Soft - ICE 和另一个软件调试器共用时,这个功能可以用来把控制权交给另一个调试器。这也可以用来测试中断程序。GENINT 命令会模拟执行一道硬件中断或 INT 程序码。它将把 *flag*、CS、IP 的值推入堆叠,并把 CS、IP 的值改成中断向量表中指定的 interrupt - number 相对的进入点。

〔例〕 GENINT NMI

这道命令会强制发生一个无法屏蔽的中断。如果 Soft - ICE 和 CodeView 一起使用,这将把控制权交回 CodeView。

EXIT——强制离开目前的 DOS 程序

语法: EXIT [R] [D]

R —— 恢复中断向量表



D —— 清除所有断点

解说:

EXIT 命令藉强制执行 INT 21h 的 4Ch 功能来中止目前程序。这个命令只有在 DOS 处于可以接受此函数呼叫的状态下才能使用。如果此呼叫是由目前的中断函式呼叫或是在 DOS 尚未备妥时,系统的行为将无法预期。

使用 R 参数时,除了中断向量表外,不会做任何系统重设的动作。这意味著 BIOS 变数、视讯模式及其他系统层次的资料并不会被还原。使用 R 参数会把中断向量还原成它们最后一次储存的状态。Soft - ICE 会在其载入时、程序以 LDR.EXE 载入时及使用 VECS S 命令时储存中断向量。

〔注〕依照下列步骤来重新启动由 LDR.EXE 载入的程序:

EXIT R

LDR prog.EXE

EXIT 命令会把中断向量表还原成程序载入前的值,然后回到命令处理器。由执行 LDR 并加上.EXE 的尾巴可以把程序重新载入而不需重载符号及原始码。符号和原始码会保持在内存中。

〔注意〕EXIT 命令必须小心使用。因为 Soft - ICE 可以在任何时候叫出,可能会有 DOS 不能接受中止函数呼叫的情形发生。而且 EXIT 命令也不会重置程序的状况。举例来说,EXIT 命令不会重设视讯模式。如果你的程序把 BIOS 和硬件放在特别的视讯模式中,使用 EXIT 命令后仍会留在此模式中。

〔例〕EXIT R

还原中断向量表并跳出目前的程序。如果程序是用 LDR.EXE 载入的,则要加 R 参数。

BOOT——载入系统 (保留 Soft - ICE)

语法:BOOT

解说:

BOOT 命令会重置系统并保留 Soft - ICE 。BOOT 可以用来对载入程序、DOS 驱动程序及非 DOS 的作业系统做调试。

BOOT 是以 ROM BIOS 的 19h 中断呼叫的方法。有时候 19h 中断可能无法工作。如果发生这种状况,叫出 Soft - ICE 并使用 HBOOT 命令。

为了让 BOOT 正确的工作,Soft - ICE 必须由 CONFIG.SYS 中做第一个驱动程式载入。这样 Soft - ICE 才能尽可能的还原系统原始状态。

〔例〕BOOT

这道命令会重新载入系统。Soft - ICE 依然保留。

HBOOT——硬件系统载入 (完全重设)

语法: HBOOT

解说:

HBOOT 命令会重置整个系统。在重置的过程中 Soft - ICE 不会保留。除非介面卡需要重开



电源才能重置否则 HBOOT 就够用了。在这种罕有的状况中,你必须关掉电源再重新打开。

[例] HBOOT

这道命令会重新载入系统。Soft - ICE 必须要重新载入。

六、调试模式命令

命令:

ACTION——设定断点发生后的动作

WARN——设定 DOS/ROM BIOS 重入 (re - entrancy) 警告模式

BREAK——在任何时候中断

13HERE——把 INT 3 指向 Soft - ICE

ACTION——设定断点发生后的动作

语法: ACTION [INT1 | INT3 | NMI | HERE | int - number]

int - number —— 任何可用的中断号码 (0 - FFh)。只有当自己的断点处理程序已取代原中断向量时才可使用。(参阅 11.2)

解说:

ACTION 命令用来决定当断点条件成立时要把控制权交给谁。大部分的状况都是 INT3 或 HERE。INT3 是在 Soft - ICE 和其他调试器一起使用时使用;HERE 则是用来使断点条件成立时回到 Soft - ICE。INT1 和 NMI 则是两者择一用在无法使用 INT3 的调试器时。例如:使用 CodeView 时,ACTION 设为 NMI 最好。

• 只有当自己的断点处理程序已取代原中断向量时才可使用 int - number。

如果没有断点处理程序而使用 int - number 将会发生错误。参阅 11.2 以取得更多资讯。

如果没有加任何参数将会显示目前的设定。

ACTION 的内定值是 HERE。

[例] ACTION HERE

这道命令设定当断点条件成立时将返回 Soft - ICE。

WARN——设定 DOS/ROM BIOS 重入 (re - entrancy) 警告模式

语法: WARN [ON | OFF]

解说:

WARN 命令是用来让 Soft - ICE 和会使用 DOS 或 ROM BIOS 的调试器一起使用。许多调试器使用 DOS 和 ROM BIOS 来做屏幕输出和读取按键。因为 DOS 和 ROM BIOS 不完全能重入,若断点发生在 DOS 或 ROM BIOS 在执行时,调试器可能无法正常工作。

如果设定 WARN ON 而且 ACTION 不是 HERE,在真正动作发生前会先把控制权交给 Soft - ICE。系统会显示目前 CS:IP 并让你决定是要继续或是回到 Soft - ICE。一般而言,你应该选择回到 Soft - ICE 以继续调试。只有在你确定不会造成 DOS 或 ROM BIOS 重入时才可选择继续。

在 Soft - ICE 和 DEBUG、SYMDEB 及 CodeView 一起使用时应该把 WARN 设为 ON。



如果未加参数将会显示目前 WARN 的状态。

WARN 的内定值是 OFF。

[例] WARN ON

这道命令会打开 DOS/ROM BIOS 重入警告模式。

BREAK——在什么时候中断

语法: BREAK [ON | OFF]

解说:

BREAK 命令让你即使在关闭中断的状况下也能从当掉的系统叫出 Soft - ICE。你可以在整个调试过程中使用 BREAK 模式或在需要时开关它。

BREAK 模式会些微的降低系统的效率。系统的效率虽会降低,但却可以跳出当掉的程序。即使效率会降低,若是程序随时可能会当掉,使用者还是可能会一直使用 BREAK 模式。不像其他也可以随时叫出的调试器,Soft - ICE 不需要外加的开关。当 BREAK 为 ON 时,只要按热键即可叫出 Soft - ICE。

如果没有加参数将会显示目前 BREAK 的状态。

BREAK 的内定值是 OFF。

[例] BREAK ON

这道命令会打开 BREAK 模式。这意味著即使关闭中断,Soft - ICE 也可随时叫出。

13HERE——把 INT 3 指向 Soft - ICE

语法: 13HERE [ON | OFF]

解说:

13HERE 命令让你指定所有的 INT 3h 均会叫出 Soft - ICE 的视窗。这项功能在你想让程序停在某特定位置时很有用。要使用这项功能,在你的程序码中你想停下来的位置加上 INT 3 命令。当 INT 3 发生时叫出 Soft - ICE 视窗。这时候,你可以使用 R IP 命令来改变指令指标指向 INT 3 的下一个程序码;然后你可以继续进行调试。如果没有加参数将会显示目前 13HERE 的状态。

13HERE 的内定值是 OFF。

[例] 13HERE ON

这道命令会打开 13HERE 模式。在这的后的所有 INT 3 均会叫出 Soft - ICE 视窗。

七、公用命令

命令:

A——编译程序码

S——搜寻资料

F——将资料填入内存

M——搬移资料



Pc friend ·

C——比较两记忆区块

A——编译程序码

语法: A [address]

解说:

Soft - ICE 的编译器允许你把程序码直接编译进内存中。这个编译器支持基本的 8086 程序码及 80186、80286 真实定址模式的扩充。但是运算辅助器及 80386 的特殊程序码、暂存器定址模式等无法编译。

A 命令会进入 Soft - ICE 内建的编译器。每行前会显示地址当提示符号。当组合语言的程序码打入并按下 Enter 后,此程序码会编译进指定地址的内存中。程序码必须符合标准的 Intel 模式。在地址提示符号下按 Enter 会离开编译模式。

如果你正编译的内存范围在程序码窗中是可见的,在你编译时程序码会交互变化。

Soft - ICE 的编译器支援标准的 8086 族命令,不过有些加强:

* DB 命令用来直接定义内存中的字节资料。DB 命令后接一串字节资料或 / 和由空白、逗号分隔的字符串。

* RETF 代表一个 far return 。

* WORD PTR 和 BYTE PTR 用来决定资料的大小。如:

```
MOV BYTE PTR ES:[1234],1
```

* 使用 FAR 和 NEAR 以明确的指定远程或近程的跳跃或呼叫。如果未指定 FAR、NEAR,一律视为 NEAR。

* 参考到内存位置的运算域必须放在方括号中。如: MOV AX,[1234]。

[例] A CS:1234

这道命令会提示你输入组合语言码并从 CS:1234 开始编译的。输入最后一道程序码后在地址提示符号后按 Enter。

S——搜寻资料

语法: S address L length data - list

data - list —— 一串字节资料或以逗号、空白分隔的加引号字符串。加引号的字符串可以使用单引号或双引号。

length —— 字节长度。

解说:

S 命令会在内存中搜寻和 data - list 相同的字节或字元。搜寻的动作由指定的 address 开始,持续搜寻 length 字节。每个发现的地址都会显示出来。

[例] S DS:SI + 10 L CX 'Hello',12,34

这道命令会从目前的资料节段中差距地址为 SI + 10 处开始搜寻 Hello 字串后接 12h、13h 的资料。搜寻会持续 CX 字节才停止。

F——将资料填入内存



语法: F address L length data - list

data - list —— 一串字节资料或以逗号、空白分隔的加引号字符串。加引号的字符串可以使用单引号或双引号。

length —— 字节长度。

解说:

F 命令会用指定的 data - list 来填满内存。填入的动作会从指定的 address 开始并持续 length 字节。如果有需要会重复 data - list 。

〔例〕 F 8000:0 l 100 'Test'

这道命令会从 8000:0000 开始填入 100h 字节的 Test。Test 字符串会一直重复直到填满指定的长度。

M——搬移资料

语法: M start - address L length end - address

length —— 字节长度。

解说:

M 命令会从指定的 start - address 搬移 length 字节的资料到 end - address 。

〔例〕 M 1000:0 L 200 2000:0

这道命令会从内存地址 1000:0000 处搬移 200h 字节的资料到 2000:0000 处。

C——比较两记忆区块

语法: C address1 L length address2

length —— 字节长度。

解说:

C 命令会拿 address1 处 length 字节大小的内存区块和 address2 处的资料做比较。如果第一块区块的值和第二块的值不同时显示两者各自的值及其内存地址。

〔例〕 C 5000:100 L 10 6000:100

这道命令会比较从内存地址 5000:100 开始 10h 字节的内存区块和从 6000:100 开始 10h 字节的内存区块的值。

八、特别的调试命令

命令:

SHOW——显示在 history buffer 中的程序码

TRACE——进入模拟跟踪模式 (trace simulation)

XT——在模拟跟踪模式中进行单步执行

XP——在模拟跟踪模式中进行程序单步



XG——在模拟跟踪模式中执行到某地址

XRSET——重设回溯跟踪缓冲区 (back trace buffer)

VECS——储存/还原/比较中断向量

SNAP——拍下内存区段的快照

EMMMAP——显示 EMM 分配图

SHOW——显示在 history buffer 中的程序码

语法: SHOW [B | start]

B —— 这会使 SHOW 命令从缓冲区中最早的程序码开始显示。

start —— 从缓冲区中最后一个程序码(最后抓入的程序码)的前多少程序码开始显示。

解说:

SHOW 命令会显示在回溯跟踪缓冲区中的程序码。如果有程序码的原始码,会以混合的方式显示;否则只显示程序码。

SHOW 命令可以用上、下、PageUp、PageDown 等键来卷动。按 Esc 键以离开 SHOW 命令。在每道程序码地址的前有个缓冲区记入号码。这个号码表示你多深入显示缓冲区。号码越高表示你在缓冲区中更深的地方。

[注]在使用 SHOW 命令的前必须先用范围回溯跟踪记录程序码。参阅第九章以取得更多有关范围回溯跟踪的资讯。

[建议]把程序码窗设为可见并在其中显示目前回溯跟踪缓冲区的真正程序码区段是很有用的。以此比较程序码和真正的流程时较不会为跳跃和呼叫困扰。

在 TRACE 命令后接著使用 SHOW 命令可以让你用两种不同的观点来看在回溯跟踪缓冲区中的程序码。

[例] SHOW 40

这道命令会从回溯跟踪缓冲区倒数第 40 个程序码开始显示。

TRACE——进入模拟跟踪模式 (trace simulation)

语法: TRACE [start] | [OFF]

start——从缓冲区中最后一个程序码(最后抓入的程序码)的前多少程序码开始模拟跟踪。

OFF——离开模拟跟踪模式。

解说:

TRACE 命令让你可以把回溯跟踪缓冲区中的程序码以宛如第一次执行的情形再重播一次。你必须把程序码窗设为可见才能使用模拟跟踪模式。进入模拟跟踪模式后,你可以使用 XT、XP 和 XG 命令来跟踪缓冲区中的程序码。

输入 TRACE OFF 以离开模拟跟踪模式。

未加参数的 TRACE 命令会显示目前模拟跟踪模式是 ON 或 OFF。

[注]在使用 TRACE 命令的前必须先用范围回溯跟踪记录程序码。参阅第九章以取得更多有关范围回溯跟踪的资讯。

[建议]在程序码窗设为可见的状态下模拟跟踪模式可发挥最大功能。把 TRACE 命令和



SHOW 命令连接使用是很有用的。这会同时以两种不同的型式显示回溯跟踪缓冲区中的程序码。

〔例〕TRACE 40

这道命令会从回溯跟踪缓冲区倒数第 40 个程序码开始进入模拟跟踪模式。在输入 TRACE OFF 命令的前会一直留在模拟跟踪模式。

XT——在模拟跟踪模式中进行单步执行

语法：XT [R]

R —— 反向进行单步执行。

解说：

XT 命令会单步执行在回溯跟踪缓冲区中的程序码。这个命令的行为类似普通调试中的 T。要注意的是在模拟跟踪模式中单步执行不会改变除了 CS、IP 外的暂存器的值。

XT 命令让你可以重播回溯跟踪缓冲区中的程序码。

〔注〕在使用 XT 命令的前必须先进入模拟跟踪模式。参阅第九章及 TRACE 命令以取得更多有关范围回溯跟踪的资讯。

〔建议〕如果你常常使用 XT 命令，它可以像其他命令一样设个功能键代替。

〔例〕XT

这道命令会在模拟跟踪模式中单步执行一道程序码。

XP——在模拟跟踪模式中进行程序单步

语法：XP

解说：

XP 命令会在回溯跟踪缓冲区中进行一程序单步。这个命令的行为类似普通除错中的 T。要注意的是除了 CS、IP 外的暂存器的值均不会改变。

XP 命令让你可以重播回溯跟踪缓冲区中的程序码。

〔注〕在使用 XP 命令的前必须先进入模拟跟踪模式。参阅第九章及 TRACE 命令以取得更多有关范围回溯跟踪的资讯。

〔建议〕如果你常常使用 XP 命令，它可以像其他命令一样设个功能键代替。

〔例〕XP

这道命令会在模拟跟踪模式中程序单步一道程序码。

XG——在模拟跟踪模式中执行到某地址

语法：XG [R] address

R —— 反向搜寻地址。

address —— 回溯跟踪缓冲区中欲执行到的地址。

解说：

XG 命令会把程序码指标移到回溯跟踪缓冲区中指定的地址的下一道程序码。

如果在地址的前有加 R 的话会把程序码指标移到指定地址的前一道程序码。



address 必须是一道程序码叙述的第一字节。

XG 命令的行为类似普通调试中的 G 。

〔注〕在使用 XG 命令的前必须先进入模拟跟踪模式。参阅第九章及 TRACE 命令以取得更多有关范围回溯跟踪的资讯。

〔例〕XG 273:1030

这道命令会把程序码指标移到地址 273:1030 的后一道命令。

XRSET——重设回溯跟踪缓冲区 (back trace buffer)

语法: XRSET

解说:

XRSET 命令会重设回溯跟踪缓冲区。如果在回溯跟踪缓冲区中有你不想要的程序码时,在设定回溯范围时要先执行这个命令。

〔例〕SRSET

这道命令会重设回溯跟踪缓冲区。

VECS——储存/还原/比较中断向量

语法: VECS [C|S|R]

C —— 比较目前的中断向量表和储存起来的表。

S —— 储存目前中断向量表。

R —— 由缓冲区中还原中断向量表。

解说:

VECS 命令允许你把中断向量表储存到 Soft-ICE 中的内建缓冲区或还原的。你也可以比较真正的中断向量表和储存起来的表并显示出两者间不同的处使用 C 命令比较目前的中断向量表和储存的向量表时,会以下列格式显示:

address old - vector new - vector

每个有改变的中断向量均会显示出来。

载入 Soft-ICE 时的中断向量表会被储存起来。当程序以 LDR.EXE 载入时也会自动储存向量表。只有一份中断向量表会被储存,所以每次执行 VECS S 时上一份备份的中断向量表会被覆写掉。

如果没有加参数则会显示整个中断向量表。

〔例〕VECS C

这道命令会比较真正的中断向量表和上次储存在 Soft-ICE 内建缓冲区中的中断向量表。

SNAP——拍下内存区段的快照

语法: SNAP [C | S | R] address1 address2

C —— 比较缓冲区和内存范围。

S —— 把内存范围存到缓冲区中。

R —— 从缓冲区还原内存范围。



解说:

SNAP 命令会拍下内存区段的快照以供稍后的比较用。用 S 参数会把一记忆体范围备份到延伸内存中的缓冲区里。使用 C 参数会显示延伸内存中缓冲区和指定的地址范围的真实内存间不同的处。加上 R 参数则会把延伸内存中的缓冲区拷贝到主内存中的地址范围。

如果使用 C 参数来比较缓冲区和地址范围,则会以下列格式输出:

```
address old - data new - data
```

每一改变的字节都会显示出来。

使用 C 和 R 命令时通常不需加 address。如果没有指定 address,则会使用最后一次有加 address 的 SNAP 命令的 address。

[注]要使用 SNAP 命令你必须在 CONFIG.SYS 中 S-ICE.EXE 那行加上 /TRA XXXX 参数。SNAP 命令会把资料储存到回溯跟踪缓冲区中。如果你正在使用回溯跟踪则会和 SNAP 起冲突。如果你在回溯跟踪缓冲区中有程序码资料时使用 SNAP S 命令会把回溯跟踪资讯覆写掉。反过来说,如果你用 SNAP 命令储存一区段然后又打开范围回溯跟踪则会覆写掉 SNAP 的缓冲区。

[例] SNAP S 2000:0 4000:0

这道命令会把从 2000:0 到 4000:0 的资料区段存到 Soft-ICE 的回溯追踪缓冲区。

EMMMAP——显示 EMM 分配图

语法: EMMAP

解说:

EMMMAP 命令会显示 EMM 内存中每一个可取得的 page 及目前映射到的 page。

[注]你必须启动 Soft-ICE 的 EMM 特性才能使用这个功能。参阅第八章以取得更多有关启动 EMM 能力的资讯。

[例] EMMAP

这会以下列的格式显示目前 EMM 的分配情形:

```
Phy PageSeg addressHandle/Page
```

```
00D000FFFF
```

```
01D4000001/0000
```

```
02D8000001/0001
```

```
03DC000001/0002
```

在这个范例中,page 0 是在 D000 且没有映射。page 1 是在 D400,handle 是 1 且 page 0 映射到此。page 2 是在 D800,handle 是 1 且 page 1 映射到此。page 3 是在 DC00,handle 是 1 且 page 2 映射到此。

九、视窗命令

Soft-ICE 有三种视窗:暂存器窗、资料窗和程序码窗。这些视窗都可以随时切换出来或关

**Pc friend** ·

闭。资料 and 程序码窗可以改变其大小；暂存器窗的大小是固定的。视窗的顺序总是固定不变。从屏幕顶端由上而下依次是暂存器窗、资料窗、程序码窗。

命令：

WR——切换暂存器窗

WC——切换/设定程序码窗的大小

WD——切换/设定资料窗的大小

EC——进入/离开程序码窗

。——定位目前的程序码

WR——切换暂存器窗

语法：WR

解说：

如果暂存器窗目前是看不见的则这个命令会把它切为可见。若暂存器窗目前是可见的，WR 命令会关闭暂存器窗。

暂存器窗会显示 8086 暂存器及各旗号的值。

内定的功能键：F2

WC——切换/设定程序码窗的大小

语法：WC [window - size]

window - size —— 1 到 21 间的十进位数。

解说：

如果没有指定 window - size，这个命令会切换程序码窗。如果程序码窗是看不见的会把它切为可见；若是可见的则会关闭的。

如果有指定 window - size，则程序码窗会重设大小。如果程序码窗本来是看不见的则会以指定的大小显示。

〔注〕如果你想把游标移到程序码窗中要使用 EC 命令。参阅 EC 命令的解说以取得更多资讯。

〔例〕WC 12

如果程序码窗是看不见的则会显示一个 12 行大小的程序码窗。如果程序码窗目前在屏幕上，它的大小会重设为 12 行。

WD——切换/设定资料窗的大小

语法：WD [window - size]

window - size —— 1 到 21 间的十进位数。

解说：

如果没有指定 window - size，这个命令会切换资料窗。如果资料窗是看不见的会把它切为可见；若是可见的则会关闭的。

如果有指定 window - size，则资料窗会重设大小。如果资料窗本来是看不见的则会以指定



的大小显示。

〔例〕WD 1

如果资料窗是不可见的则会显示一个 1 行大小的资料窗。如果资料窗目前在屏幕上,它的大小会重设为 12 行。

EC——进入/离开程序码窗

语法: EC

解说:

EC 命令会使游标在程序码窗和命令窗中切换。如果游标在命令窗中,它会被移到程序码窗中。如果游标在程序码窗中,它会被移到命令窗中。

当游标在程序码窗时,会有更多可用的功能,这使得调试更为容易。这些功能是:

* Point - and - shoot break points

Point - and - shoot break points 是用 BPX 命令设置的。如果没有加参数,会在目前游标所在位置设置断点。游标所在那行必须包含程序码。(如果你不确定,把程序码窗以混合的模式开著) 内定 BPX 的功能键是 F9。

* Go to cursor line

你可以在游标所在位置设个暂时断点,用 HERE 命令执行到那里。游标所在那行必须包含程序码。(如果你不确定,把程序码窗以混合的模式开著) 内定 BPX 的功能键是 F7。

* Scrolling the code window

只有当游标在程序码窗中时才能卷动程序码窗。卷动的按键在程序码窗中有不同的定义。

UP —— 把程序码窗向上卷一行。

DOWN —— 把程序码窗向下卷一行。

PageUp —— 把程序码窗向上卷一页。

PageDown —— 把程序码窗向下卷一页。

〔注〕程序码窗必须是可见的 EC 命令才能使用。

. ——定位目前的程序码

语法: 。

解说:

当程序码窗是可见的时候,“。”命令会显示目前的程序码。

十、调试器设定命令

命令:

PAUSE —— 显示满一个屏幕后暂停

ALTKEY —— 设定 Soft - ICE 的启动热键

FKEY —— 显示、修改功能键

BASE —— 设定/显示目前的基数

CTRL - P —— 把 LOG 送到打印机

Print - Screen —— 印出目前屏幕



PRN —— 设定打印机的输出端口

PAUSE —— 显示满一个屏幕后暂停

语法: PAUSE [ON | OFF]

解说:

PAUSE 命令会在每一页的结束时暂停屏幕。如果 PAUSE 设为 ON, Soft-ICE 会提示你按任意键以继续滚动视窗, 提示信息会显示在屏幕底部的状态行里。

如果没有指定任何参数则会显示目前 PAUSE 的状态。

PAUSE 的内定值是 ON。

[例] PAUSE ON

这个命令指定接下来屏幕上的显示会等你输入任意键后才继续滚动。

ALTKEY —— 设定 Soft-ICE 的启动热键

语法: ALTKEY [ALTletter] | [CTRLletter] | [SYSREQ]

letter —— 任何一字母 (A - Z)

解说:

ALTKEY 命令可以让你改变用来叫出 Soft-ICE 的热键。你可以把热键改成 CTRL + 字母、ALT + 字母或是 SysRq (即 PrtScr) 键。

有时候你或许会使用会和 Soft-ICE 的 Ctrl-D 热键相冲突的程序, 避免这种冲突的方法的一是使用 ALTKEY 命令改变叫出 Soft-ICE 的热键。另一个方法则是在热键组合中多按个 SHIFT 键, Soft-ICE 对这样的组合不会有反应, 所以能把热键传到你的程序去。举例来说, 如果你使用的常驻程序是以 Ctrl-D 叫出来的, 试著用 Ctrl-Shift-D 来叫出你的程序。有些键盘上你必须按 Alt-PrtScr 来模拟发出个 System Request。小心不要意外的把屏幕上的东西印了出来。

如果没有指定参数则会显示目前的热键。

内定的热键是 Ctrl-D。

[例] ALTKEY ALT Z

这道命令指定 Ctrl-Z 是叫出 Soft-ICE 的热键。

FKEY —— 显示、修改功能键

语法: FKEY [function-key-name string]

function-key-name —— F1, F2……F12

string —— string 包含任何 Soft-ICE 的命令和特殊字元: ^ 及 ;。^ 是用来让命令不显示出来, ; 则代表按下 Enter。

解说:

FKEY 命令是用来指定某功能键所代表的命令字符串, 功能键可设定来代表任何 Soft-ICE 中的命令。

如果没有指定参数则会显示目前各功能键代表的命令。

要取消某个功能键可以用这样的方法: FKEY 加 function-key-name, 然后接上一个空白字符串。



你也可以在设定档 S-ICE.DAT 中预先指定功能键的功能。参阅 6.4 以取得更多有关在设定档中设定功能键的资讯。

在功能键设定字符串中加上归位键的符号可以让一个功能键代表一系列的命令。归位键是用 ; 来表示。

如果你在功能键的设定前面加上 ^ (Shift - 6), 则接下来的命令将不会显示出来。命令的作用还是一样没变, 但是显示在命令窗中的所有信息 (包括错误讯息) 都不会再出现。这个模式在命令会改变视窗中资料而你又不想因此造成命令窗中的混乱时特别有用。

当功能键有加上 ^ 设定时, 你可以在键入其他命令的途中使用这个功能键而不会对输入中的命令造成任何影响。例如, 如果你使用的是 F2 的内定值, 你可以在输入下一个命令的时候按 F2 来切换暂存器窗。

[注] Soft-ICE 有个 S-ICE.DAT 的设定档, 你可以把功能键的设定写在这个档案中, 这样在载入 Soft-ICE 的时候会自动设定功能键。在设定档中设定功能键的语法是: function - key - name = "string"。在设定档中设定功能键的时候要用双引号把字符串括起来。

[例] FKEY F2 ^WR; (command line)

这道命令用来设定 F2 代表切换暂存器窗的命令, ^ 代表这个命令不会显示出来, ; 代表按下 Enter。如此 F2 键就可以用来切换暂存器窗的 on 或 off, 而且即使是在输入其他命令的时候也可以随时使用。

[例] FKEY F1 "G CS:120; R; G CS:" (command line)

这个例子显示你可以用一个功能键代表许多命令, 也可以代表一个命令的一部分, 等待使用者的输入来完成它。输入这道命令后, 按下 F1 键会执行到 CS:120 处, 显示目前的暂存器的值, 然后显示 G 命令等待使用者的输入。

[例] FKEY F1 WD 3; D DS:100; (command line)

这个例子会设定 F1 键代表一串命令。这个按键是可见的, 而且以 Enter 结束。它会把资料窗设为三行的大小并显示从 DS:100 处起的资料。

[例] F1 = "WR; WD 2; WC 10;" (S-ICE.DAT)

如果这一行是放在 S-ICE.DAT 中, 当载入 Soft-ICE 时会自动设定 F1 键。当在 Soft-ICE 中按下 F1 键时, 它会切换暂存器窗, 打开一个 2 行的资料窗, 及一个 10 行的程序码窗。

BASE —— 设定/显示目前的基数

语法: BASE [10 | 16]

解说:

BASE 命令是用来设定基数是以 10 或 16 为底。以 10 为底在小视窗模式中会受到限制, 这是受到视窗宽度的影响。即使是在大视窗模式中, 有些命令显示的资料数目也会受限制。

当基数为 10 的时候, 所有输入和显示的数字和地址都是以十进位表示。如果基数是 16 的话, 则是除了原始码行号, WIN 命令中的屏幕座标、大小以 10 进位表示外, 均为 16 进位。

基数的内定值是 16。

[例] BASE 16

这道命令会把基数设为 16。

Ctrl - P —— 把 LOG 送到打印机



Pc friend ·

语法: Ctrl - P

解说:

在你按下 Ctrl - P 后,所有显示在命令窗中的的信息也会被送到打印机去。要停止把 LOG 送到打印机的动作只要再按一次 Ctrl - P 即可。

当你用 Ctrl - P 送许多资料到打印机时,也许你会想把 PAUSE 设为 OFF,这样资料才可以一直卷动下去而不需要去按键。

Print - Screen —— 印出目前屏幕

语法: Print - Screen

解说:

按下 Print - Screen 键后会整个屏幕上的东西全部输送到打印机中去。

如果你只是想印出内存内容或是某个命令的辅助资料,使用 Ctrl - P 会比用 Print - Screen 快得多,这是因为 Print - Screen 会把屏幕上包括边界的每个字元都送到打印机去。

PRN —— 设定打印机的输出端口

语法: PRN [LPTx | COMx]

x —— 介于 1 到 4 的数字

解说:

PRN 命令允许你把 Ctrl - P 和 Print - Screen 的资料送到不同的打印机去。

如果没有指定参数则会显示目前指定的打印机。

〔例〕PRN COM 1

这道命令会把 Ctrl - P 和 Print - Screen 的输出送到 COM 1 端口去。

十一、屏幕控制命令

命令:

FLASH —— 执行 P 或 T 命令时还原屏幕

FLICK —— 减轻屏幕的闪烁

WATCHV —— 设定监控显示模式

RS —— 显示程序屏幕

CLS —— 清除视窗

ALTSCR —— 转换到替换屏幕

WIN —— 改变 Soft - ICE 的视窗大小

FLASH —— 执行 P 或 T 命令时还原屏幕

语法: FLASH [ON | OFF]

解说:

FLASH 命令让你指定在 T 或 P 命令执行时是否要还原屏幕。如果你指定要还原屏幕,则在 T 或 P 命令执行的时候会短暂的还原一下。在对会存取 VIDEO MEMORY 的程序片段时你会需要用到这个功能。

如果 P 命令用来执行一个 CALL 或中断,则一定会有屏幕还原的动作,因为执行的函式中可能会对屏幕写入。

如果没有指定参数则会显示目前 FLASH 的状态。



FLASH 的内定值是 OFF。

〔例〕FLASH ON

这道命令会把 FLASH 的状态设为 ON。执行任何 P 或 T 命令时会还原屏幕。

FLICK —— 减轻屏幕的闪烁

语法：FLICK [ON | OFF]

解说：

有些显示卡在输出字元之前要先等垂直、水平扫描完成才行。如果任意的输出，在显示字元时将会发生闪烁的现象。如果你使用 Soft-ICE 时屏幕会有闪烁的现象，你应该把 FLICK 设为 ON。有些 EGA 卡上你离开 Soft-ICE 时颜色可能没有还原的很正确，这是模拟的 EGA 显示的问题。3DA 端口是个有两个功能的显示端口。第一种是一些老旧的 CGA 软件靠 3DA 来做 hsync 和 vsync，这样可以避免在一些老旧的 CGA 控制卡上造成闪烁的现象。第二个功能则是用来重新设定 EGA 卡的调色盘。Soft-ICE 有个演算法可以不用一直监控这个端口，一直监控会减慢一些认为自己在 CGA 卡上执行的老旧程序的速度。但是在某些状况下，这套演算法可能无法使用。如果你是在 EGA 上使用 Soft-ICE 而且发现颜色并没有正确的还原的话，把 FLICK 设为 ON，这样 Soft-ICE 会监控 3DA 端口从而解决这个问题。

当 FLICK 设为 ON 时，屏幕更新的速度会变慢。

如果没有指定参数则会显示目前 FLICK 的状态。

FLICK 的内定值是 OFF。

〔例〕FLICK ON

这道命令会把 FLICK 模式设为 ON。Soft-ICE 会等水平、垂直扫描完成后再输出字元。

WATCHV —— 设定监控显示模式

语法：WATCHV [ON | OFF]

解说：

WATCHV 命令让你指定 Soft-ICE 要如何监控显示端口。通常 Soft-ICE 只有在执行 INT 10 切换到非文字模式后才监控显示端口。但是有些程序不用 INT 10 来切换显示模式，这种状况下，如果 WATCHV 设为 OFF，则 Soft-ICE 在储存或还原屏幕时可能会发生问题。把 WATCHV 设为 ON 则会让 Soft-ICE 随时监控显示端口。

如果你发现 Soft-ICE 并未正确的处理你的屏幕，或不能正确的还原游标的位置，把 WATCHV 设为 ON。把 WATCHV 设为 ON 可能会影响目前显示模式的效率。

如果没有指定参数则会显示目前 WATCHV 的状态。

WATCHV 的内定值是 OFF。

〔例〕WATCHV ON

这道命令会把 WATCHV 设为 ON。

RS —— 显示程序屏幕

语法：RS

解说：

RS 命令让你暂时还原程序屏幕，Soft-ICE 视窗将消失直到你按任一键为止。



这个功能在对经常更新屏幕的程序做调试时很有用。当 Soft - ICE 叫出来时会回到文字模式,使用 RS 命令可以暂时回到绘图模式屏幕。

CLS —— 清除视窗

语法: CLS

解说:

CLS 命令会清除 Soft - ICE 的视窗,并把提示符号及游标移到视窗的左上角。

〔例〕 CLS

ALTSCR —— 转换到替换屏幕

语法: ALTSCR [ON | OFF]

解说:

ALTSCR 命令允许你把屏幕的输出从原定屏幕重新导向到替换屏幕去。这个功能在你对绘图模式程序调试时非常有用,这样你就不用再在绘图模式和 Soft - ICE 间切换来切换去。

ALTSCR 要求系统连接两台显示器。替换屏幕必须处于文字模式,这是显示器的内定模式。

WATCHV 的内定值是 OFF。

〔例〕 ALTSCR ON

这道命令会把屏幕的输出重新导向到替换显示器上。

WIN —— 改变 Soft - ICE 的视窗大小

语法: WIN [N | W] [start - row length [start - column]]

N —— 当指定 N 时,视窗会被设为较小的模式:46 字元宽。

W —— 当指定 W 时,视窗会被设为整个屏幕的宽度。

start - row —— 0 到 17 的数字。指定视窗从哪一列开始。

length —— 8 到 25 的数字。指定视窗有几列。

start - column —— 在小视窗模式中指定视窗位置为从左边算过来第几行。

start - row 和 start - column 指定小视窗模式中视窗左上角的位置。在大视窗模式中, start - column 会被忽略。

解说:

WIN 命令可以让你修改 Soft - ICE 视窗的宽度和高度。

如果没有指定参数,这个命令会在小视窗模式和大视窗模式中切换。

如果 WIN 命令只有加上 N 或 W 参数时,则视窗的宽度会变换成指定的大小,但高度不变。

如果视窗的行数加上 start - row 大于 25,则视窗的 length 到屏幕底端为止。WIN 的内定值是小视窗模式。

〔例〕 WIN N 4 9 30

这个命令会把视窗设定为从第 4 列、第 30 行处开始显示,并且是 9 列高、46 个字元宽。

〔例〕 WIN

这道命令会在大视窗和小视窗模式间切换。

〔例〕 WIN W 10 8

这个命令会把视窗设定为从第 10 列处开始显示,并且是 8 列高、整个屏幕的宽度。



编读互动

经过上期的尝试,本刊的“编读互动”在读者群中引起了强烈的反响,来信差点把信箱给撑破了!这多少鼓舞了小编我!也更加坚定了把它办好的决心。为了解决大家的每一个问题,小编可是动员了编辑部的全体同仁,忙得焦头烂额,不亦乐乎(众读者芸:小编辛苦了……什么?应该的!),看来大家的评价还是蛮合理的(小编:心里美滋滋的!),小编可从来不敢有丝毫懈怠和怨言!对我的上帝们我可是抱着十万分的忠诚噢!呵呵……好了,废话少说,还是来看看这一次读者都有哪些问题吧!

1. 众位编辑好,我是《黑客防线》的忠实读者,有一个问题想请教一下,我如何才能从 ICQ 中得到对方的 IP?

最初级的方法:可以在 INFO 里看到对方的 IP 地址,但较新的 ICQ 都有一个选项可以隐藏自己的 IP(在 Security&Privacy 里有个 IP HIDING),所以在 INFO 里你看到的是 N/A。较简单的方法是下载 ICQ IP Sniffer,以前有一个是要在 13 秒内输入密码的,我这里的不需要,用法很简单,输入对方的 ICQ 号即可;其他的方法:先给对方发个信息,等他回复后,开个 DOS 窗口,输入 NETSTAT(或 NETSTST -N)即可。最好先关掉其他的 Internet 程序。本方法除了 ICQ,也适用于其他的地方,只要对方给你发信息你就可以知道他的 IP。

2. 各位编辑好,我想问你们一个问题,就是怎样才能登录远程的 NT 服务器?

我们将做如下简单事情就有可能成功,假设目标 NT 的 IP 地址为 111.111.111.111,做法如下:

```
net use \\111.111.111.111\ipc$ "" /user: ""
```

net.exe 是 NT 的工具文件,该命令将和目标服务器建立 Null Session,如果成功,你可以查看该服务器上的共享目录:

```
net view \\111.111.111.111
```

当然,如果你有该 NT 管理员密码,就更好办了,假设其管理员 Admin 密码为 fuck:

```
net use \\111.111.111.111\ipc$ "fuck" /user: "Admin"
```

命令成功后,几乎所有目标 NT 上的配制、资源,你都可以你本地 NT 上直接使用。

3. 各位编辑救救我,要不然我死定了!我的机器一不小心中了 diskboom,硬盘报废了!请问还有没有办法恢复。

首先小编非常理解你现在的心情,收到信后请教了数个高手,苍天不负有心人,终于找到了解决的办法。为了让更多的人不再出现这种情况,我这里把中了 diskboom 之后的特征说一说。如果你的屏幕无端出现一个 dos 框,并有一行英文 “your system is now locked by diskboom, please reset”



那就证明你中了最无耻的 diskboom 了!这时候你千万不要听它的去重起计算机,因为那样的话,你就再也找不到你的硬盘了,就算光盘引导、软盘引导都无效!

你应该去一些网络安全网站下载一个 diskboom 修复程序(如果不幸重启了,那么去朋友家或者网吧下一个,千万不要扔掉硬盘哦~);然后把压缩包里面的恢复程序 copy 到一张系统盘,在盘上建立一个 autoexec. bat 文件,内容第一行为“恢复程序.exe”,也就是说自动执行恢复程序,呵呵,这一点是最关键的,Readme 里面没有说明。最后,拿这张盘引导后,出现 unlocked 提示,就好啦~~~)。

4. 你好,能介绍一下对付妖之吻黑客软件的办法吗?

如果你的屏幕无端出现一个黄色的框,有“给你一个死亡之吻”字样,并出现倒计时,那么你就是中了妖之吻了,重起后你遇到一个提示框“系统破坏,必须重装 Windows”,千万不要听他的,马上退到 DOS 状态,并修改 c:\windows\system. ini,把 shell = yzw 改成 shell = explorer 就没事了。

5. 各位编辑好,怎样才能解决 Kmodem 的断线攻击?

Kmodem 的原理是向目标的 modem 发送一个 + + + ATH0 信息,这个信息的含义为告诉猫:我要断线了,呵呵!解决方法:只要你的机器上安装一个个人防火墙能截住 ICMP 包就行了。

6. 你好,我的机器经常被黑,我想找到黑我的人,可如何进行端口监听呢?

网络监听的软件很多,这里只介绍两个软件,首先是 NukeNabber,它是端口监视器,你告诉 NukeNabber 需要监视 7306 端口,如果有人接触这个端口,就马上报警。在别人看来,你的电脑的 7306 端口是开放的,但是 7306 不是由 netspy 控制了,当 NukeNabber 发现有人接触 7306 端口或者试图进入你的 7306 端口,马上报警,你可以在 NukeNabber 上面看到黑客对你做了些什么,黑客的 IP 地址是哪,然后,你就可以反过来攻击黑客了。当 NukeNabber 监视 139 的时候,你就可以知道谁在用 IP 炸弹炸你。另外提一下,如果 NukeNabber 告诉你不能监视 7306 端口,说这个端口已经被占用了,那么说明你的电脑中存在 netspy 了。第二个软件就是 Tcpview. exe,这个软件是线程监视器,你可以用它来查看有多少端口是开放的,谁在和你通讯,对方的 IP 地址和端口分别是什么。

7. 大家好,现在 OICQ2000 已经出来了,以前的很多查 OICQip 的工具现在好像不灵了,我想知道有没有办法查 OICQ2000 的好友的 IP?

这个问题你算问对了,小编整天也在不停地琢磨,终于找到了一款工具,那就是刚出品的新的 ip 探测软件 oicqsniffer113,它可以显示所有和你建立连接的对方的 ip 地址和端口。这个软件在本期的附赠光盘中。

8. 各位编辑辛苦了!听说大名鼎鼎的微软公司就栽在了木马 Qaz trojan 的脚下,我想对该软件了解一下,希望不吝赐教。

Qaz trojan 就是前一段时间黑客用来攻击微软公司所使用的木马!大名鼎鼎的微软公司就栽在了这个软件手里!它感染 notepad. exe,并且可以自动感染其他共享机器,它会开放被感染机的 7597 端口,以便日后黑客进入被感染机!假如你的机器不幸中了该木马,你可以手动删除了 Notepad 的注册键值(点击“开始→运行”,键入“Regedit”,按“确定”后找到:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\StartIE = XXXX\Notepad. exe
```



点右面的 StartIE = XXXX\Notepad. exe 后按“编辑→删除”。其中 XXXX 一般为 \Windows, 即 QAZ 蠕虫程序所在的目录)。重新启动计算机之后, 运行杀毒软件把所有受感染的文件清除掉, 然后在资源管理器中把 Windows 下的 NOTE 改为 NOTEPAD。

用资源管理器找到 NOTEPAD, 点击属性, 发现 NOTEPAD 的扩展名是 .COM。好了, 进入 DOS 状态, 执行: Rename notepad. com notepad. exe。返回 Windows, 可随意点击打开文本文件了。到此为止, QAZ 蠕虫的后遗症统统治好了。

9. 各位老编好, 我想问一下, 如果不幸运行了“克林顿”, 是不是硬盘会全被格式化?

呵呵, 你这次问对了, 我不久前还深受其害。这款软件应叫“恶作剧之王”, 是“藏鲸阁”(http://lovejingtao. 126. com) 编的一个恶性硬盘格式化软件(主程序为 SEX. EXE, 大小 215K, 图标为一个女人头像), 其破坏过程如下: 运行主程序后, 屏幕中心出现一个克林顿头像, 右眼被黑眼罩蒙住(克林顿是海盗), 旁边有两行字: “不要摸我的左眼, 否则你会后悔的!” 当鼠标移动到它的左眼上时, 你的厄运开始了: 鼠标活动范围被限制, 系统会锁死, 然后程序在后台修改 C:\MSDOS. SYS, 禁止启动时按 F5、F8 等键, 还将 C:\AUTOEXEC. BAT 内加入格式化命令(从 Z 盘开始至 C 盘只需几秒钟)。最后弹出来一个窗口, 说“你一定想按回车键吧。”按了回车键后, 系统将会重新启动, 格式化所有的硬盘。只要你在线上, 此程序就会从远程随时传送到你的硬盘上(%TEMP%\VBE\SEX. EXE) 并运行。一旦发现了海盗头像, 什么都不要做, 按机箱上的 RESET 键重新启动, 删除 %TEMP%\VBE\SEX. EXE 即可。万一中招, 你将会在重启时听到硬盘“嘎达嘎达……”的声音, 你应该以最快的速度按下 RESET 键, 再自检使关机, 找一张启动盘重新启动, 并检查 C 盘是否被格掉, 如果没有被格掉, 那还算幸运, 你可以删除: \AUTOEXEC. BAT、%TEMP%\VBE\SEX. EXE, 然后进入 Win98, 使用 RecoverNT 恢复后面的分区。如果你的动作太慢, 那硬盘就肯定被全部格掉了。此时可以试一下 UNFORMAT(只能恢复 FAT16 的硬盘), 否则就只能重装系统, 并使用 RecoverNT 恢复后面的分区。

10. 近期掌上电脑受到自由特洛伊(Liberty Trojan)病毒侵袭, 请问这种自由特洛伊病毒还会再度攻击吗?

Liberty Crack 程序攻击特定的目标, 秘密地在隐藏在一个名为 Liberty (自由) 的程序里, 掌上电脑用户可用这个程序在他们的掌上电脑上玩任天堂的游戏。这个病毒的代码是由瑞典的软件开发商 Ardiri 开发的。其目的是想让掌上设备乱作一团, 并以此来测试他准备推出的另一款程序。

这个程序是 Ardiri 故意支使他人释放的, 在该程序释放后 10 分钟后, Ardiri 后悔了, 于是他让人们删除这个程序, 但此病毒可能是一个 PDA(个人数字助理)设备染上恶意代码的预兆。幸运的是这名为“Liberty Crack 1. 1”(自由爆裂)的程序只影响了为数不多的一些人, 而且人们很容易发现并删除它。

现在安全专家正不遗余力地小心对付网络的攻击者, 而接受任务的公司也在不停地追踪网络破坏者。这似乎在向人们证明: 一些不顾道德的人正在不停地对网络进行攻击, 而正义者也在不停地开发新的程序来扼制这些不良程序。

因此, 在病毒、漏洞及特洛伊木马等千万病毒中, 这种自由特洛伊最终会因其弱小的影响力而销声匿迹的。



11、请问各位大虾有没有什么软件可以查出并删掉电脑里的后门?我自己给自己的电脑里装上了后门,却不知道怎样关上它。我的操作系统是 windows98。

试试 cleaner3. exe 吧,最好是监视端口,有不明端口开放就仔细检查一下了,另外了解一下国内常见的木马端口,在《黑客防线 3》的编读互动中我们已经介绍了不少的木马清除方法。

12、如何在下 windows 2000 下关闭 smtp 功能?

选择控制面板 ->管理 ->Internet 服务器器管理,逐一打开,看到 SMTP 服务,点工具栏中的停止按钮。还可以关闭其他服务。

13、我的计算机运行 WIN98,有时关机时会提示“有 1 用户已连接到你的计算机,是否继续?”此时运行网络监视器会发现有用户(与我在同一个局域网)连接到我计算机的“IPC\$”目录中,但实际上我的计算机上是没有这个目录的,请问是不是有什么问题?是不是有可能有黑客程序呢?

那个是共享,局域网下通过 win9x 的一个漏洞,可以远程共享到你的机器上而且可以通过口令验证(如果你没有加 path 的话)。

14、在 win2000 和 winnt 里,日志文件存在泄密问题,可以清除它们吗?怎样清除?

可以清除,但是有些文件需要有权限。路径:

\winnt\system32\logfiles*. *

\winnt\ssystem32\config*. evt(要 administrator 权限)

\winnt*. txt

\winnt*. log

\winnt\system32\dtclog*. *(要 administrator 权限)

\winnt\system32*. log

\winnt\system32*. txt

然后再用 dir *.log /s 搜索 log 文件,删除他们。

15、请问那里可以找到反汇编的工具?

呵呵,这个不用再说了吧!本期配套光盘里就有好多哟。

16、请教各位大虾,我经常被踢,能帮帮我吗?

刚才在编辑部讨论这个问题,有的说:隐藏你的 ip 就行;有的说:装一个防火墙,再把 JAVA 关上。其实,只隐藏 IP 是不行的,至少现在不行,有一些隐藏 IP 的软件现在都没用了,不信你可以试试,和 JAVA 的关系也不是很大。

你被踢有两种可能:一是你有可能中了木马;二是有人用了一些黑客软件,利用操作系统存在的一些漏洞干的。你可以下载一个放火墙,像天网之类的。至于报复我就不多嘴了,嘿嘿。不过这样一来至少你不会再被攻击了。

17、如何限制启动进程?

许多个人计算机可以启动多种不同的操作系统。例如,即使您通常从 C: 驱动器启动 Windows NT,其他人也可以选择其他驱动器(如软驱或光驱)启动其他版本的 Windows。如果发生这种情况,您在 Windows NT 的正常版本中所做的安全防范措施可能会被绕过。

一般情况下,您应只安装希望在您设置的计算机上使用的那些操作系统。对于高级安全系统



,这可能意味着只安装 Windows NT 的一个版本。但是,您必须在物理上保护 CPU 以保证其他人不能装载其他操作系统。根据您的现实情况,可选择卸掉软盘驱动器。在某些计算机中可以通过在 CPU 内设置开关或跳线禁用从软盘驱动器启动。如果使用硬件设置防止从软盘驱动器的启动,您可以锁住计算机机箱(如果可能)或将计算机锁在机柜中,在前面留下一个孔,以便人仍可以使用软盘驱动器。如果 CPU 位于一个上锁的位置且远离键盘和监视器,就无法添加驱动器或更改硬件设置以达到从另一个操作系统启动的目的。另一个简单的设置是编辑 boot. ini 文件,将启动超时设置为 0 秒;这样,如果有一个操作系统存在,用户就很难启动另一个系统。

在最新的硬件中也可以使用其他硬件配置(如固件安装、启动密码、电源密码)来控制启动进程,因此应适当研究和它们。

18. 编辑同志好,我是一个初学者,经常听别人谈论扫描工具如何重要,可我不明白扫描器是什么,用扫描器扫描到的端口有什么用呢?

这个问题对很多初学者比较迷茫,在 INTERNET 安全领域,扫描器可以说是黑客的基本武器,一个好的 TCP 端口扫描器相当与几百个合法用户的口令及密码是等同的,这样说一点也不过分。那么到底什么是扫描器呢?其实扫描器是一种自动检测远程或本地主机安全性弱点的程序,通过使用扫描器你可以不留痕迹的发现远程服务器的各种 TCP 端口的分配及提供的服务,和它们的软件版本,这就能让我们

间接的或直观的了解到远程主机所存在的安全问题。有些读者有很多扫描工具,可扫描到端口之后就不知道该干什么了,其实端口是入侵主机的必由之路,进入主机有好几种方式,可以由 Telnet (Port 23) 或 SendMail (Port 25) 或 FTP 或 WWW (Port 80) 的方式进入,一台主机虽然只有一个位址,但是它可能同时进行多项服务,所以如果你只是要“进入”该主机,这些 Port 都是很好的进行方向。当然还有很多 Port,只要你知道了对方的哪个端口开着,就可以进行入侵了。

如果读者不是很着急,那么敬请等待我们《黑客防线 5》与您见面,我们将带你全面了解扫描器知识。

19、黑编们好,我是一个想了解黑客的菜鸟,经常听别人说:机器中了木马程序后,会留下一些开放的端口,作为后门,我想了解一些木马程序的默认端口?

为了让大家能更全的了解端口知识,我们将计算机的端口整理后提供给读者:

15 = NETSTAT PORT

21 = Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, ebEx, Win-Crash

22 = SSH PORT

23 = Tiny Telnet Server

25 = Shtrilitz Stealth, Terminator, WinPC, WinSpy, Kuang2 0.17A - 0.30, Antigen, Email Password Sender, Haebu Coceda, Kuang2, ProMail trojan, Tapiras

31 = Agent 31, Hackers Paradise, Masters Paradise

41 = DeepThroat

53 = DOMAIN PORT



58 = DMSetup
63 = WHOIS PORT
79 = Firehotcker
80 = Executor 110 = ProMail trojan
90 = DNS PORT
101 = HOSTNAME PORT
110 = POP3 PORT
121 = JammerKillah
137 = NETBIOS Name Service PORT
138 = NETBIOS Datagram Service PORT
139 = NETBIOS Session Service PORT
194 = IRC PORT
406 = IMSP PORT
421 = TCP Wrappers
456 = Hackers Paradise
531 = Rasmin
555 = Ini - Killer, Phase Zero, Stealth Spy
666 = Attack FTP, Satanz Backdoor
911 = Dark Shadow
999 = DeepThroat
1001 = Silencer, WebEx
1011 = Doly Trojan
1012 = Doly Trojan
1024 = NetSpy
1045 = Rasmin
1090 = Xtreme
1095 = Rat
1097 = Rat
1098 = Rat
1099 = Rat
1170 = Psyber Stream Server
1170 = Voice
1234 = Ultors Trojan
1243 = BackDoor - G, SubSeven
1245 = VooDoo Doll
1349 = BO DLL
1492 = FTP99CMP



1600 = Shivka - Burka
1807 = SpySender
1080 = SOCKS PORT
1981 = Shockrave
1999 = BackDoor 1.00 - 1.03
2001 = Trojan Cow
2023 = Ripper
2115 = Bugs
2140 = Deep Throat
2140 = The Invasor
2565 = Striker
2583 = WinCrash
2801 = Phineas Phucker
3024 = WinCrash
3129 = Masters Paradise
3150 = Deep Throat, The Invasor
3700 = Portal of Doom
4092 = WinCrash
4567 = File Nail
4590 = ICQTrojan
5000 = Bubbel, Back Door Setup, Sockets de Troie
5001 = Back Door Setup, Sockets de Troie
5321 = Firehoteker
5400 = Blade Runner
5401 = Blade Runner
5402 = Blade Runner
5550 = JAPAN Trojan - xtcp
5555 = ServeMe
5556 = BO Facil
5557 = BO Facil
5569 = Robo - Hack
5742 = WinCrash
6400 = The Thing
6666 = IRC SERVER PORT
6667 = IRC CHAT PORT
6670 = DeepThroat
6711 = SubSeven



Pc friend ·

6771 = DeepThroat
6776 = BackDoor - G, SubSeven
6939 = Indoctrination
6969 = GateCrasher
6969 = Priority
7000 = Remote Grab
7300 = NetMonitor
7301 = NetMonitor
7306 = NetMonitor
7307 = NetMonitor
7308 = NetMonitor
7626 = G_Client
7789 = Back Door Setup, ICKiller
9872 = Portal of Doom
9873 = Portal of Doom
9874 = Portal of Doom
9875 = Portal of Doom
9989 = iNi - Killer
10067 = Portal of Doom
10167 = Portal of Doom
10520 = Acid Shivers
10607 = Coma
11000 = Senna Spy
11223 = Progenic trojan
12223 = Hack?9 KeyLogger
12345 = GabanBus, NetBus, Pie Bill Gates, X - bill
12346 = GabanBus, NetBus, X - bill
12361 = Whack - a - mole
12362 = Whack - a - mole
12631 = WhackJob
13000 = Senna Spy
16969 = Priority
20001 = Millennium
20034 = NetBus 2 Pro
21544 = GirlFriend
22222 = Prosiak
23456 = Evil FTP, Ugly FTP



- 26274 = Delta Source
- 29891 = The Unexplained
- 30029 = AOL Trojan 30100 = NetSphere 1.27a, NetSphere 1.31
- 30101 = NetSphere 1.31, NetSphere 1.27a
- 30102 = NetSphere 1.27a, NetSphere 1.31
- 30103 = NetSphere 1.31
- 30303 = Sockets de Troie
- 31337 = Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO
- 31338 = NetSpy DK 31338 = Back Orifice, DeepBO
- 31339 = NetSpy DK
- 31666 = BOWhack
- 31785 = Hack Attack
- 31787 = Hack Attack
- 31789 = Hack Attack
- 31791 = Hack Attack
- 33333 = Prosiak
- 34324 = BigGluck, TN
- 40412 = The Spy
- 40421 = Agent 40421, Masters Paradise
- 40422 = Masters Paradise
- 40423 = Masters Paradise
- 40426 = Masters Paradise
- 47262 = Delta Source
- 50505 = Sockets de Troie
- 50766 = Fore
- 53001 = Remote Windows Shutdown
- 54321 = School Bus .69 - 1.11
- 60000 = Deep Throat
- 61466 = Telecommando
- 65000 = Devil
- 69123 = ShitHeep

注:现在的木马的端口,都可以重定义的,上面含有的木马端口只是它们的默认端口。