突破常规玩电脑系列丛书

智美利达

怎么样，动心了吧？如果是，请赶快翻到目录页寻找你感兴趣的内容仔细阅读。相信我们，读完之后你一定不会失望的

COMPUTER

高手破解真经

计算机技术研究组　总策划

精彩内容导读

- 破解杂谈——寻找破解的理由
- 破解的相关技术资料
- 高手真经——积累的精华
- 透视"大虾"的武器库

【特别提示】

本书荟萃了众多破解名家的“不传之秘”，旨在与读者朋友进行经验交流，切勿用于其他目的

内蒙古大学出版社

突破常规玩电脑系列丛书

高手破解真经

计算机技术研究组　总策划

内蒙古大学出版社

书　　名：突破常规玩电脑系列丛书（1-7）
编　　著：武新华
出　　版：内蒙古大学出版社（呼和浩特市大学西路235号 邮编 010021）
责任编辑：赵英
封面设计：南永夫
发　　行：全国各地新华书店
印　　刷：河南省瑞光印务股份有限公司
开　　本：850×1168　　1/32
印　　张：7
字　　数：215千字
版　　期：2003年9月第1版　2003年9月第1次印刷
标准书号：ISBN 7—81074—508—5/TP・27
印　　数：1—5000册
定　　价：112.00元（本册定价16.00元）

为什么购买这本书

这是一本有关计算机加密与解密问题的书籍。这本书既是写给普通电脑迷的，同时更适合那些孜孜于计算机软硬件程序的探索者——Cracker。

对于普通的电脑迷，阅读本书的意义意味着你再也不需面对日益繁多的共享软件而茫然无措。我们知道，你曾经为它们心动，因为你确实需要它们的帮助去驾御你的计算机世界；但很多时候你又非常无奈，你无奈于你的钱财，更无奈于对加密解密技术的无知以及由此导致的对你心爱之物的不可获得。与你相似的苦恼我们也曾经历，更深知援助之手在这一时刻所具有的意义。我们无法助你钱财，但有时候知识却远比钱财重要。这本书便具有这样的作用。

我们相信，有这样一本书置于你的案头，那许许多多在你过去看来难于登天的事情，你会突然发现却原来如此简单。

而对于更高一级的电脑玩家 Cracker 来说，阅读本书的意义却另有不同。去不断地探索未知，是每一个 Cracker 心目中永远的诱惑。作为一个 Cracker，注定了你与未知的对抗，而不能掌握一些必要的软件破解技术，是你无法忍受的羞耻。

的确，有那么多的共享软件，而你却不明白它们的程序原理，这是有辱于 Cracker 的称号的。当然，Cracker 的目的不是单纯地破解软件，而是通过跟踪软件了解程序思路，从而写出更好的程序。

破解也不在于数量多寡，关键是掌握方法，弄清注册码计算原理。本书中，我们集合了数十位破解高手苦心钻研出来的心得，提供了一般加密解密书籍都无法教你的秘技与妙招，我们相信，当你翻阅完这些 Cracker“老鸟”们轻易不会示人的“私藏秘典”，你也会很快地加入他们的行列。

本书就是这样一本讲解各种破解实例的教科书，这也是我们推荐你购买与阅读本书的理由。

目 录

第1章 破解杂谈：寻找破解的理由 **1**
1.1 WAREZ的无形帝国 1
1.1.1 了解软件盗版组织 1
1.1.2 破解正版软件的流程 2
1.1.3 RAZOR1911的经历 4
1.1.4 外国政府的态度 6
1.1.5 中国盗版市场现状 7
1.2 寻找破解的理由 8
1.2.1 关于破解的一些想法 9
1.2.2 互联网时代的软件保护 10
1.2.3 换一只眼看程序员 12
第2章 破解的相关技术资料 **15**
2.1 有关于编程 15
2.1.1 VXD,KMD,WDM基本概念 15
2.1.2 用Delphi写小执行程序 19
2.1.3 Visual CHM2.x的加密算法 24
2.1.4 程序的自删除 26
2.1.5 得到进程的父进程 27
2.1.7 “金山词霸”屏幕取词的奥妙 29
2.1.8 利用硬件信息实现共享软件的安全注册 35
2.1.9 中断向量：由一只病毒说开去 39
2.2 学习PE文件技术 42
2.2.1 Api函数地址的“手动”获取 42
2.2.2 PE操作和重定位 49
2.2.3 关于PE可执行文件的修改 63
2.2.4 手工构造PE程序 78

2.2.5 用32位吸脂工具为应用程序减肥 81
2.3 SEH技术与逆向工程的应用 104
2.3.1 SEH in ASM技术的研究 104
2.3.2 Part 4 关于异常处理的嵌套和堆栈展开 114
2.3.3 逆向工程——"变速齿轮"研究手记 126
2.4 Ring0权限与Win32Asm编程 129
2.4.1 Ring0权限的取得 129
2.4.2 Ring0代码的实现 140
2.4.3 WIN 95中代码不用VXD获得0级特权的方法 149
2.4.4 Win32Asm教程 151
第3章 高手真经：积累的精华 165
3.1 经验的点滴 165
3.1.1 熟悉FI原理 165
3.1.2 使Soft-ICE在程序入口处停下来 166
3.1.3 TRW2000一点小小的经验 167
3.1.4 对付"禁止注册表编辑"的N招 167
3.1.5 如何在DOS窗口中输入汉字 168
3.1.6 RUNDLL.exe 命令详解 169
3.1.7 BIOS密码清除的原理 175
3.1.8 用VC助手进行跟踪破解 175
3.2 关于DOS程序的破解 177
3.2.1 DOS下破解Ghost Demo的log用法 178
3.2.2 在DOS下可执行文件的装入和执行 183
第4章 透视"大虾"的武器库 185
4.1 共享软件问题 185
4.1.1 时光倒流——调整软件使用期限 186
4.1.2 注册表分析工具 188
4.1.3 在注册表中调整软件使用时限 197
4.2 光盘的加密与解密 202
4.2.1 光盘加密流技术 203
4.2.2 使用CD-Protector软件加密光盘 205

4.2.3 使用 FreeLock 加密数据光碟光盘加密流技术.....208
4.2.4 破解加密光盘.....213

第 1 章 破解杂谈：寻找破解的理由

- WAREZ 的无形帝国
- 寻找破解的理由

盗版软件在我国是如此的肆虐，而且是难以遏制，简直就成了顽症。那么是什么原因使得盗版软件不能被彻底铲除呢？

从表面上看是因为我国人均收入还太低，无力支付购买软件的昂贵费用。而从实质上看，是因为我国的软件破解者太少了，以致于使盗版软件有了众多的客户。

如果我国的软件破解者较多，这时盗版软件的客源较少，使得它没有了经营的余地，那么盗版软件也就会自行消失了。当然，就目前来说，我国打击盗版软件的工作还是任重而道远的。

1.1 WAREZ 的无形帝国

就我国，乃至全世界来说，谁也不敢说自己的个人电脑里没有一个软件是非法的呢？因为如果电脑软件全部通过支付金钱的方法获取正版软件的话，对于每一个电脑使用者，特别是游戏玩家等一类需要经常更新软件或经常尝试使用新软件的电脑用户，购买软件的开支是相当大的。可以说没有盗版软件，我国乃至世界的 IT 业就不会有这么快的发展速度，这么说似乎也并不夸张。

那么是谁制作了那些盗版软件？，您想了解他们的身份和来历么？想了解他们的组织结构和体系么？笔者是在一个偶然的机会下，了解到了这一切，现在就听我一一道来吧。

1.1.1 了解软件盗版组织

最早的软件盗版组织在 70 年代末 80 年代初就已经出现了，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。就这样，一种奇怪的自发性民间组织在国外诞生了。

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，同一地区组织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，互联网的日益发展，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“0DAY”组织成员为荣。

那么“WAREZ”是什么意思呢？“WAREZ”是指国外从事软件盗版制作者的统称。“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。“0 D AY”也具有相同的意思。

在美国的一些大学中，如果一个学生是“0DAY”成员，他的计算机教师甚至会考虑在他的成绩单中加分，因为加入此种盗版组织意味着他在技术上的优秀。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。

下面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。

1.1.2 破解正版软件的流程

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 2.8×65，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 光盘镜像包，使用者全部下载后再将其解压刻录成光盘，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。

它还将告诉你今天有那些游戏上传、昨天有那些游戏上传、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。

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 IP 地址，看是否是它的成员，而且 IP 通过检验进入 FTP 后会看到欢迎词，以及“本站是 XX 组织北美第 XX 发行站”之类的字样。

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。

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了，那么你将从组织中自动淡出。

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。

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盗版软件中的.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。

除去这种非法的盗版游戏传播工作，“0DAY”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，这招实在算不上文明。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RAZOR1911、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盗版图形软件几乎都是由这个组织破解的。

1.1.3 RAZOR1911的经历

下面我们来介绍一下RAZOR1911组织从1985年至今在Commodore64，Amiga和PC机上的经历（C64和Amiga都是80年代的4位/8位游戏机），因为它是此类组织发展历程中最具代表性的一个。

1985年10月，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。当组织成立起来以后，该给自己的组织起一个好名字呢？一个朋友为他们起名叫RAZOR2992，但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，他们回答说因为在C64游戏机破解组织中，有太多没脑子的孩子用类似666这种号码加在他们的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。

起初，他们并不很清楚成立一个小组都需要些什么，但他们从1941、Section 8、Jedi2001、Hellmates、SCC等著名的软件破解小组那里得到了很多灵感。

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，但其中一些至今还在Commodore64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 CrackingCrew（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“顶极精英”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 RawDeal 的 Laffen，获得了“年度最佳解密高手”的称号。

当时 FAIRLI GHT 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，好的图像和动听的音乐，后来它们大部分都遗失了。

不像许多新成员所想象的那样，RAZOR1911 的老成员们都希望该组织成为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 RAZOR1911 吸收进去。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 Rockets 和 StripPoker II。但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 AMIGA 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。

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，更为困难的是，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。

未来走向何方？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 Darwin 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 DoctorNo、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，在行业内口碑甚好。

从此，他们由紧凑、精干、高效率的小组很快变为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 年以后，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 的名义零星地破解了一些光盘版游戏，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，更甚至有些人物被警方逮捕和备案。但他们还是度过了难关，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，从中可以了解到他们许多被遗忘的秘密。

1.1.4 外国政府的态度

由于盗版制作者很有一种黑客精神：追求绝对技术，追求完全共享。而且他们的行为在客观上已经侵犯了软件厂商的利益。更何况你不为盈利，并不代表着别人也不想盈利！在加拿大、德国和南非等地，盗版软件销售十分猖獗（我国不也如此吗？），而在俄国一切都几乎是公开的。

实际上俄国的 DD 组织就直接从事赢利性销售，几乎所有的盗版组织都被大公司告上过法庭。

最近的例子是关于 EA 公司出品游戏 FIFA2000 的。由于盗版组织的“提供组”成员渗入 EA 公司内部，致使母盘外流，结果盗版 FIFA2000 比正版提前出了 1 个月。

EA 公司愤怒之中在俄国、英国和德国分别将 DD、MYTH 和 CLASS 告上法庭。俄国 DD 组织成员被抓，判刑，后来司法部门收受贿赂，将该组织成员释放。英国法院则认为 MYTH 只在网上传播硬盘版，自己没有网站和广告，没有万维网（WWW）的链接，没有赢利，所以判定 MYTH 组织无罪。

德国的 CLASS 则只是罚款了事，没有追究任何刑事责任。但是现在的盗版组织都不敢碰 EA 这样的大公司，他们总是等 EA 的正版游戏出品了再做破解版，因为这

种公司的势力实在太大了。

其他的时候盗版总是比正版出得快，《暗黑破坏神Ⅱ》（DIABLOⅡ）的盗版（光盘破解版）比美国本土正式版提早两天上市而且破解得相当完美！其原因正如上所述，正版从业者中有些本身就是“WAREZ”成员。

这些还只是游戏软件，在国外应用软件破解在某种程度上比游戏软件的破解技术难度高得多，而且风险也更大。以北美地区为例，任何一款正版游戏最高售价也不过499 美元，而正版应用软件的价格都要上 100 美元，而盗版软件一张只卖到 9 美元。

这种价格差听起来很容易让大家联想到本国的盗版现状，盗版组织四处网罗的枝蔓在本国又是如何延伸的呢？

1.1.5　中国盗版市场现状

中国最早的个人“WAREZ”组织志愿者、中国“中文解密基地”网站站长曾想建立自己的“CHINA 0DAY”组织，而且他在国内的志同道合者也不在少数，但是他们很快发现在中国不可能产生“0DAY”组织。

很多人把原因简单地归结为某种“民族性”的障碍，这是不对的。这里面存在很大的经济因素、社会因素和技术因素的问题。

从经济上讲，欧美国家 IT 业和电信业本来就发达，每年个人无论在软硬件消费还是网络服务费用上，相对于人均收入都是微乎其微的。经济的发达带动了社会的发展和教育水平的进步，这意味着在发达国家更多有计算机天赋的青年可以有条件从事这一爱好，而在中国如果一个计算机天才在山区诞生了，那么他永远将无法证明自己。

而即使当一个中国青年终于可以承担自己在计算机上投入的金钱时，他已经不具备加入“0DAY”的条件和精力了。

谈到技术，中国目前网络带宽很难让人满意，每秒钟十几 K 怎么和国外 150 兆/秒以上的速度相比？不要说 0 DAY，就是上传下载恐怕也要 5DAY 不止啊。把这一切制约因素都通通抛开不谈，仅仅说一句“中国人没有这种素质和意识”是不公平的。

如果说以上的青年还只是对电脑技术的迷恋，那么 GAMEZ88 组织可就完全不是这样了。据说它是 FAIRLIGHT 一个 18 岁在斯坦福大学读书的成员在中国搞的一个纯赢利组织，具体成员分布不详。

GAMEZ88 的游戏都是在国外破解然后在国内压制成盘的，真正好的技术在国外，

国内盗版组织几乎不具备破解能力。据说FAIRLIGHT专门有外国组，负责破解多语种游戏软件。

简体中文版《魔法门之英雄无敌III》的硬盘版很可能就是靠国外小组破解的。这是国内比较有来历的盗版组织，其他的一些零散组织则采取互相盗用或到国外WWW网站下载的方式制作盗版光盘。另外香港也是一个盗版天堂，大陆的许多盗版软件都是从那里流入的。

这里有一个很大的怪圈：

盗版商人痛恨伪正版商，因为他们比自己谋取了更多的暴利。一张盗版盘成本2元，利润只有1元，这1元还是层层批发商一起来分的。而伪正版商很可能与一些正版厂商内部人员串通，用低廉报酬获得图片、攻略和手册说明书，然后便翻版印制，以盗版的成本和正版的价格出售给拥护正版游戏的玩家。

而另一方面盗版制作者却巴不得国家下力气抓盗版，盗版销售被限制了，盗版商赔了，但是由于光盘的减少，制作者反而会奇货可居而赚得更多！这就是中国盗版市场的冰山一角。

本节到这里就结束了，由于信息来源的局限性，某些具体细节的真实个人已无从验证，有兴趣的读者欢迎继续与个人交流看法。

最后要说的是，个人出版本系列图书的目的，不是为盗版行为歌功颂德。它是对劳动的不尊重，更是阻碍经济正常运转的毒瘤，无论盗版者的初衷是什么，他们都永远是要打击的对象。

但是，WAREZ是“不以赢利为目的纯技术团伙”，他们有自己的信念和约定俗成的行规，他们没有自己网站，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“0 DAY”组织成员为荣，只不过他们的成果被那些商人所利用才有今天的所谓“盗版软件”。

这正是大家现在嘴里所说的“黑客”和以前所指真正意义上的“Hacker”之间的区别。

1.2 寻找破解的理由

由上面叙述的内容，我们可以知道，国内的破解者和盗版者与国外比起来是有很大差距的。而且国内出售的绝大多数盗版软件都是从国外流入或从国外网站上下载下

来的。

① 破解者及相关

大约二年以前，一群和软件开发者称兄道弟的破解者被一群 Cracker 骂的狗血淋头，吐沫星飞扬。

半年以前国内的一个著名破解收集站点，被一伙收了费的 Cracker 黑了所有镜像，不得不宣布关站。

② D 版用户及相关

各大论坛和 BBS 充斥着："救救我，Photoshop 6.0 的注册码！""我给大家磕头了，请告诉我 Flash5.0 如何注册！"……

许多网站的站长在下载的软件的后面写到："请使用我注册的的注册码：xxx xxx-xxxxxx 请点击我的广告"

还有更多的用户用着盗版的 Word 向杂志投稿：盗版软件不稳定，都带病毒，还会破坏硬件……

再看看国外：

0day 公布过所有重量级软件的破解和下载，却没有要求大家点击什么，辗转传入国内的 ZIP 包中依旧保留着 nfo 的身影。

无数个人 FTP 站点中，XXXX.XXX.XXX-X.X.X-XXX 的目录随处可见。

哎，中国的 Cracker 你总是为了自身的水平和名气而破解吗？中国的用户难道你就是永久的享受者吗？

1.2.1　关于破解的一些想法

这里所讲的破解，是破解软件而非破解网站，希望大家在阅读本节之前，首先弄清楚这个问题。

破解对于一些人可能会感到很神秘，正因为这个原因，有很多人学起了破解。当然去学破解并不难，网上关于破解的文章有很多，去照猫画虎的破几个软件是很容易的一件事。

然而在学习的同时，你可能没想到，你对软件的价值观念，在随着你对破解的痴迷（破解完一个软件后，会有一种自豪感和成就感，这种感觉真的很好，会驱使你破第 2 个，第 3 个……）而发生改变。你将不再想用钱去买一些共享软件，你破不了的

可能会把它删了，也不会因为这个软件好而去买它。

就这样你花在破解上的时间会越来越多。可是您的经济来源是否有问题呢？因为现在社会上招人没有也不可能有要招会破解的，只懂破解不能也不可能使你在社会上生存。那么连生存都成了问题，还从何谈起破解呢？

所以笔者希望正在学破解的人和天天玩破解的人，能够认识到这一点（破解只能当兴趣不能当工作）。

因此时常有人感叹，为什么中国软件产业的发展远远落后于印度呢？为什么中国会有那么多的盗版软件呢？就是因为在外国有大量软件破解者的存在!!

软件公司及个人耗尽心血、时间等，辛辛苦苦开发出软件，很快就被他们破解、发布，败坏了道德标准。软件公司及个人投入得不到回报，哪有资金继续开发软件？哪有资金扩大规模？这样就造成中国的软件公司绝大部分都是小公司、小作坊式企业，个人才能得不到发挥，整日还得为三餐犯愁，出现了张小龙（FOXMAIL 作者）式的悲剧人物。

软件公司及个人刚要成长，就被扼杀在摇篮中！中国的软件产业得不到发展的罪魁祸首就是盗版软件!

1.2.2 互联网时代的软件保护

软件作为一种无形的产品，凝聚了开发者的辛勤劳动，然而，开放平台上的软件几乎从一开始就受到盗版问题的困扰，盗版者常常会让软件厂商血本无归。多数商业软件采取了保护措施来防止盗版。进入互联网时代后，软件保护技术遇到了新的挑战，也看到了新的机遇。

对于传统的单机软件，软件加密有通过软件和硬件两种方式。由于软件加密在对抗调试跟踪上有一定的局限性，现在主要用于低强度加密。

硬件加密经过了几代产品的发展，从最初的使用实现专门计算功能的扩展卡加密到软件狗加密，再到具有编程、抗跟踪能力的软件狗，一直在不断完善中，而且硬件加密的加密强度一直强于同时代的软件加密技术。

在开放的 Internet 时代，软件行业的发展对软件保护创造了更多的机遇，也提出了更高的要求。各类厂商潜心开发研制了新型保护软件，软件保护向着互联网时代飞速迈进。