★计算机反病毒技术

# 计算机
# 反病毒技术

★ 唐常杰　胡　军　著



★電子工業出版社

# 计算机反病毒技术

唐常杰　胡军　著



电子工业出版社

## 内 容 提 要

本书由浅入深地介绍了计算机病毒的历史、现状、危害性。通过分析源程序病毒代码，讨论了计算机病毒的基本构造、传播机理、解剖技术、相关的 DOS 技术、磁盘结构知识。介绍了诊治计算机病毒的比较论方法和实证法。书中列出了病毒克星系列软件的全部源程序；讨论了这套软件诊治四大类病毒的技术，即诊治 DOS 上的一切主引导扇区寄生型（包括未来的）、引导扇区寄生型、中断服务程序寄生型的病毒、以及诊断一切可执行文件寄生型病毒。其中 V-Doctor 还带有知识库，可通过学习，积累知识，摘除各种寄生在执行文件中的已知病毒类的程序块。

本书可作为广大程序员、计算机科研人员、大中专学生的参考资料或教材。



计算机反病毒技术

唐常杰 胡 军 著

责任编辑：王昌铭 徐云鹏

*

电子工业出版社出版（北京市万寿路）

电子工业出版社发行 各地新华书店经售

电子工业出版社计算机排版室排版

总参工程兵印刷厂印刷

开本：787×1092 毫米 1/16 印张：12 字数：299.2 千字

1990 年 6 月第 1 版 1990 年 6 月第 1 次印刷

印数：30100 册 定价：5.50 元

书号：ISBN7-5053-1116-6/TP・181

# 前　言

计算机病毒以其在全球的大规模疫情，造成的严重损失和心理损害，以及对未来信息系统的威胁，从反面为反病毒工作者设立了课题，集合了大批人才，从而也为病毒本身挖掘了坟墓。

综观近年诊治计算机病毒技术，大致可归纳为三种思想。一、效果论：视被考查系统为黑箱，从外部观察总体效果，根据屏幕显示、速度、文件消失等现象判断感染病毒类型。二、解剖论：通过软件工具（如 Debug，Pc Tool）解剖软件，在机器码一级上实证施治。在这一方法论指导下，本书列出了我们研制的、带有知识库的 V-Doctor 的全部程序，它能通过学习，积累知识，对寄生了已知的多种病毒类的软件，自动地作“外科”手术，切除病毒代码。三、比较论：这是我们提出并主张的方法论。基本方针是：1. 以寄生类型分类；2. 归类提取特征正本；3. 对比诊断；4. 凡出现异常，则用正本覆盖；5. 实证法回收磁盘空间。比较论方法类似于中西医结合。由此而开发出的广谱抗病毒软件具有诊治四大类病毒的能力。即诊治在 DOS、CCDOS 运行的一切（包括已存在，但尚未发现的和未来的）主引导扇区寄生型，引导扇区寄生型，中断服务程序寄生型计算机病毒，以及诊断一切可执行文件寄生型病毒。

全书内容按由浅入深的原则安排，先简单，后复杂；先现象，后本质；先实践，后理论；先讲一般思想，后分析技术细节。

如果读者只需要一个应急方案，可以只读第三章。只需要学会开发两个广谱抗病毒软件的读者，可以学习前四章，上机实践，调试完程序。需要深入了解病毒解剖结构及反病毒技术细节的读者，应读完全书并上机动手实践。

各章内容组织如下：

第一章介绍了计算机病毒的简单历史，现状，危害性，现象和防治策略。第二章通过解剖两个简单源程序讨论了计算机病毒程序的主要结构，传播机制和一般原理。第三章介绍简单的防治技术。在不需深入研究，不需投资，不需开发专门软件前提下，根据这章内容，也能利用现成软件工具治理两类病毒。

第四章详细地介绍了广谱病毒克星软件，并列出了全部源程序（用 Turbo Pascal4.0—5.5 版本开发的）。4.1～4.9 每节介绍一个源程序模块（单元）。4.10 节给出了能诊治四类病毒的交互式病毒克星 U-Killer·EXE。4.11 节给出了能自动诊治三类病毒的免疫程序 Auto Kill·EXE。程序清单中插入了详细的中文注解，中英文对照的主要名词缩写。为了改善可读性，采用了自明的标识符。所有程序都调试通过，经过用户考验。　为了适应技术的发展，软件都采用了开放式结构，例如匹配串和查字节数程序与数据库分离，数据库文件可用任何字处理软件编辑。读者除了能学到反病毒技术外，还能受到良好的程序设计风格的熏陶。

第五章介绍了磁盘构造，主引导扇区（分区表），引导扇区，BPB，FAT 以及与病毒有关的 DOS 技术细节，为深入解剖计算机病毒奠定基础。

第六章剖析了一批典型计算机病毒，如小球病毒（Ascii7），大麻病毒（Marijuana，Stoned），巴基斯坦智囊病毒（Brain），黑色星期五（Jerusalem-B），杨基病毒（Yan Kee doodle），并深入分析了多种病毒的并行感染，交叉感染和链式感染。

第七章介绍了用通用软件工具（如 Debug，Pc Tools，Noton Unility）诊治计算机病毒的技巧。

第八章给出了带数据库的免疫软件和一个带知识库的病毒医生 V-Doctor 软件的全部源程序(已全部调通),后者能通过学习积累知识,自动地切除嵌入执行文件中的病毒寄生代码块。

第九章给出了计算机病毒克星系列软件的详细使用说明,便于读者使用软件。

书末的附录一给出了几十种常见病毒的特征资料以及相关的病毒克星疗法。附录二给出了对应于若干 DOS 版本的常用磁盘的基本参数。附录三给出了病毒克星中广泛调用的通用工具过程单元源程序。附录四给出了工具单元的源程序。附录五给出了字节数清单、格式及部分常用软件的字节数数据。

计算机病毒与反病毒技术的历史尚短,作者水平有限,书中难免有欠妥之处,恳请批评指正。

编 著 者

1990 年 5 月于四川大学计算机系

# 目　录

# 第一章　计算机病毒简介

## 1.1　计算机病毒的发生和发展

考察如今泛滥于电脑，威胁着信息系统安全的计算机病毒的构想泉源，要追溯到科学幻想小说。

1975 年，美国科普作家约翰·布鲁勒尔(John Brunner)写了一本名为《Shock Wave Rider》(震荡波骑士)的书，该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事，令人耳目一新，成为当年最佳畅销书之一。

1977 年，另一位美国科普作家托马斯·J·雷恩推出轰动一时的《Adolescence of P1》。雷恩构思了一种神秘的，能够自我复制、利用信息通道传播的计算机程序，并称之为计算机病毒。

这些病毒飘泊于电脑之内，游荡于硅片之间，控制了 7000 多台计算机的操作系统，引起混乱和不安。

计算机病毒从上述的科幻小说到大规模泛滥仅用了十年时间。

1987 年 5 月，美国罗德岛《普罗威斯顿日报》编辑部发现存储在计算机中的文件变成了如下字符串"欢迎进入土牢，请小心病毒，如需疫苗，请与我们联系。×××与×××敬上，帕金斯坦尼电脑公司"。当专家进一步追查时，发现这个病毒程序早已广泛传播，遍布于该报社计算机网络系统的各个结点。事后了解到，该程序是帕金斯公司防止非法复制的自卫性病毒。

1987 年 12 月，一份电子邮件给 IBM 公司传送了一份能自我繁殖的圣诞祝贺程序，每当用户显示内容时，以链式反应的方式自我复制到用户的收件人目录下，最后导致网络拥挤，部分停机。

1988 年 3 月 2 日，早已潜伏，并广泛散布于苹果机的病毒发作，这天受感染的苹果机停止工作，只显示"向所有苹果电脑的使用者宣布世界和平的信息"。以庆祝苹果机的生日。

如果说上述事件还只是计算机流氓(Cyber Punk)的恶作剧，那么 1988 年 11 月 2 日发生在美国重要的计算机网络 Intel Net 的莫里斯蠕虫事件则是一场损失巨大，影响深远的大规模"病毒"疫情了。美国康乃尔大学一年级研究生罗特·莫里斯(Robbet·T·Morris)写了一个蠕虫程序(Tap worm)。该程序利用 Unix 系统中的某些缺点，利用 finger 命令查联机用户名单，然后破译用户口令，用 Mail 系统复制、传播本身的源程序，再调网络中远地编译生成代码。从 11 月 2 日早上 5 点开始运行，到下午 5 点已使联网的 6000 多台 Unix 4BCD，VAX，Sun 工作站受到感染。虽然莫里斯蠕虫程序并不删除文件，但无限制的繁殖抢占了大量时间和空间资源，使许多联网机器被迫停机。有报道，直接经济损失在 6000 万美元以上，莫里斯也受到法律制裁，根据 1986 年制定的有关法律，应处以五年监禁和 25 万美元罚款。1990 年 5 月 5 日纽约地方法院宣布对莫里斯的有期徒刑缓期三年执行，罚款一万美元，罚做社会服务工作 400 小时。莫里斯蠕虫事件引起了美国全社会和计算机界的震惊，专家们在法律，道德、反病毒技术等方面发表了大量评论，许多公司，研究所，各家纷纷发表道德宣言，表示要教育职工、学生，不制造计算机病毒，不传播"病毒"。

1989 年 11 月 13 日，星期五，一个被称为“黑色星期五”的恶性病毒在长期潜伏、广泛传播后，在全世界数十万台运行 DOS 的微机上发作。在这天，每运行一个文件，则被删除一个，许多微机用户被迫停机，在全世界造成的损失难以估计。

近年来，随着国外软件的引进和我国计算机技术的普及，十多种计算机病毒已在我国出现，并以惊人的速度蔓延，威胁着信息系统的安全。

据《参考消息》1989 年 8 月 2 日刊登的一则评论，列出了下个世纪的国际恐怖活动将采用五种新式武器和手段，计算机病毒名列第二，给未来的信息系统投上了一层阴影。

一段时间以来，反病毒技术还处于尾追造病毒技术的状态，一般是先提取标本，再解剖分析，才能发明疫苗，等解毒软件出笼，病毒已传播泛滥，十分被动。

计算机面临“病毒”的挑战，研究完善的广谱抗病毒软件和预防技术，已成为目前极待攻克的新课题。

## 1.2 诊治方法论

如何诊断一台计算机、一个软件是否感染了计算机病毒呢？至少有下列三类方法：即效果论，解剖论和比较论方法。

一、效果论（或黑箱论）方法

把一台计算机或一个软件系统理解为一个黑箱，能感知的仅是输入和输出，用户从外部对系统进行观察，这种方法类似于中医诊病，采用望诊和主述。例如，下列症状提示系统可能已被感染：

1. 运行速度明显减慢。

2. 用户未对磁盘读写，却观察到磁盘指示灯亮。

3. 列目录显示出软件的字节数增大（类似医生观察人的体重，血压指标）。

4. 病毒软件的自白。例如屏上显示‘Your PC is Stoned’，提示有合法大麻病毒；用 dir 列目录或 Label 查卷标时，见卷标被改为 Brain，提示有巴基斯坦智囊病毒；屏上显示 Ascii7 字符（小球）作弹性碰撞运动，提示有小球病毒；奏出一曲杨基曲，提示有杨基病毒。

5. 文件莫名其妙地消失。

病毒的表现常需一定条件，例如小球病毒在整点或半点（误差±0.8 秒）时，如调用 Int13（例如 dir）时开始发作，杨基病毒在下午 5 点整开始奏曲。创造病毒激活条件（类似医生在一定条件下培养细菌），是诊断计算机病毒的一种效果论方法。例如运行图 1.1 的程序（Turbo Pascal4.0 以上版本），可以激活杨基病毒或小球病毒。

```
program Check_Ascii7_virus;                          {激活小球病毒和杨基病毒}
{  To check viruses ASCII-7  and  Yanki  Doodle}
uses dos;
var Hour,Minute,Second,Sec100 : Word;      F : Text;
begin
    setTime(17,0,0,0);                               {时间设置为下午五点钟}
    GetTime(Hour,Minute,Second,sec100);              {取出时间}
    writeln(Hour,' : ',Minute,' : ',Second,' : ',sec100,' : ');   {写出时间}
    assign(F,'Test');
    {$I-} Rewrite(F),close(F);{$I+}
```

```
end.
```

图 1.1　激活小球病毒和杨基病毒的程序

二、解剖论方法

病毒程序或被病毒感染的程序通常具有解剖性特征，而日益发展的软件技术提供了许多能对软件进行外科手术的工具软件，如 debug，PC-Tool(PC-shell)，Norton，Unitity。举两例如下：

1. 确诊 D 号驱动器磁盘是否有小球病毒(D=0,1,2,分别表示 A:,B:,C:盘)。

```
C>Debug ↵
    -L 100  D,0,1 ↵{装入 D 号盘,0 扇区}
    -u ↵            {反汇编}
```

如果显示的第一条指令是 JMP 011E，则确诊已感染小球病毒。

2. 确诊 Test・COM 是否已感染“黑色星期五”。

```
C>Debug Test・COM ↵
-RCX ↵
CX：8177                    {Test・COM 的字节数,16 进位}
S100：L8177“sUMsDOS”        {搜索特征串}
××××：8171                 {在 8171 处找到特征串}
```

则可确诊已感染“黑色星期五”。

解剖论方法有下列难关：(1). 通常需用户熟练掌握软件“外科手术”工具，需较高的技巧，需要关于汇编和机器代码的知识；(2). 手术过程交互式操作，不能自动化地重复，熟练程序员也难免犯错误；(3). 如果不预知病毒特征，则需理解程序代码。由于病毒手段花样百出，需要较高的汇编技巧和实践经验。

本书第五章介绍了计算机病毒解析技术基础，第六章解剖了五种典型病毒，第七章作了手术治理病毒的示范。

三、比较论方法

在这一方法指导下，我们推荐下列诊治计算机病毒的五段法，即(1)按寄生类型对计算机病毒分类；(2)针对每类病毒，提取并保存一套重要数据的正确版本(例如不同版本的总引导扇区(分区表)、引导扇区、中断向量表、可执行文件字节数；(3)然后开发一套自动或半自动的检测系统，彻底扫描被查软件的参数(这类似于利用现代医学设备查病理数据)，再与正确版本对比，如发现异常，则提示已被病毒感染；(4)系统自动地或在用户启发下，覆盖错误数据；(5)最后以实证方法回收磁盘空间。

比较论方法的优点是：(1)广谱性。由于正确参数数据量不大，也容易得到，因而可以检查一切(包括未来的)病毒，消除一切病毒。(2)适应性。只要在检测系统中，向用户提供一套参数提取工具，则在未来的 DOS 新版本、新磁盘、新光盘或硅盘(带电池的 RAM 卡)下，由用户自己提取能数正本，因而可适应一切机型，一切版本和未来的操作系统。(3)简单性。这种方法对病毒不理解，不跟踪，只逐字节扫描并与正本比较，认定“非正即邪”，然后就“以正压邪”。操作统一、简单、重复性好，操作过程可自动化。

本书第四章给出了病毒克星软件的全部源程序并详细地分析了各个技术细节。

# 第二章　计算机病毒原理

## 2.1　计算机病毒程序的结构

在作深入分析以前，先看两个简单的，不造成实际危害的计算机病毒源程序：

### 2.1.1　一个批处理病毒程序

图 2.1 是一个在 DOS 上运行的以批处理程序形式驻留磁盘的计算机病毒程序。它十分简单，无伪装性，却有着病毒程序的典型结构，解释如下：

```
(文件名：AutoExec.BAT)
1    Echo Virus Demostration program          病毒显示程序
2    IF exist B：\Autoexec.BAT goto Virus     检查时机
3    Goto No_Virus                            时机不成熟，潜伏
4    Virus：                                  时机成熟了
5    B：                                      到 B 盘
6    Rename Autoexec.BAT Auto.BAT             改原文名，准备冒名顶替
7    Copy A：\Autoexec.BAY B：                复制自身
8    Echo I am Virus!                         表现症状
9    ：No_Virus                               正常程序入口
10   A：
11   \Auto                                    执行正常程序
12   Pause
```

图 2.1　一个批处理病毒程序

1. 病毒标本的制备。

取一张能启动机器的系统软盘，把原来的 AutoEXEC・BAT 人为地改成 Auto・BAT。然后用图 2.1 中程序，去掉行号，用冒名顶替它。

2. 运行效果

当用此盘启动机器时，如 B 盘也有 AutoEXEC・BAT，则把自身复制到 B:盘，并显示“I am Virus”(我是病毒)。从解剖角度看，第 2-8 行为病毒部分。感染后的程序相当于在原来的程序中嵌入了病毒程序。

### 2.1.2　一个寄生于 Command・COM 的病毒程序

图 2.2 是用 Turbo Pascal 4.0 以上版本编写的一个寄生于 Command・COM 的良性“病毒”程序。

“病毒”源制备方法如下：

1. 取一软盘、置 A 驱动器、格式化、装入 DOS 系统、将 Command・COM 更名为 Comm・

COM..

2. 将上述程序用 Turbo Pascal(4.0 以下)版本编译后再更名为 Command·COM,装入 A 盘,制备完成。

```
{$M,16384,0,0}                                                    {1}
Program Virus_command;        {寄生于 Command·COM 的病毒}          {2}
Uses Crt,dos;                                                     {3}
Var First3:strint[3];        User_Command:string;                 {4}
begin                                                             {5}
repeat                                                            {6}
  write('A'>);                          {给出一个正常的假象}       {7}
  readln(User_Command);                   {读入用户命令}          {8}
  Exec('A:\Comm.com'.' /C' +User_Command);  {用原解释器解释执行用户命令}
First3:=copy(User Command,1,3);           {查命令前三字符}        {10}
if  (First3='dir')or (First3='ver')then          {检查时机}       {11}
begin                          {命令为 DIR 或 VER,时机成熟}       {12}
  User_Command:='Copy A:\Comm.com'+'B:\Comm.com';{复制原解释器到 B:}
  Exec('A:\Comm.com',' /C' +User_Command);                        {14}
  User_Command:='Copy A:   \Command.com' +     {复制自身到 B:}
        B:\Command.com';                                          {16}
Exec('A:\Comm.com',' /C' +VCommand);                              {17}
  writeln('This is virus program');          {显示:'我是病毒 11,表现自己}
end;                                                              {19}
until False;
end.
```

图 2.2 一个寄生于 Command·COM的病毒程序

用 A 盘热启动机器后,Command·COM 自举,从而引导了寄生的"病毒"。第 7 行将显示 A>,等候用户输入命令 User-Command,第 9 行正常执行用户命令,第 10-11 行等候时机,每当输入命令为"dir"或"ver"时,开始繁殖,显示出"我是病毒(I am virus!)"。

程序能够给人以平安无事的假象主要是第 9 行调用真正的命令解释器 Comm·COM 来解释执行用户命令。Comm·COM 的代码量和功能占了这个冒名顶替的 Command·COM 的绝大部分,因此,可以看成是病毒程序寄生在 Command·COM 中。Command·COM 在 DOS 的最顶层,其它程序都是它的子进层。Command·COM 象一个外壳(shell)。因此寄生于类似程序的病毒又称外壳式病毒。

从上面可以看出,为了增强活力,"病毒"程序通常寄生于一个或多个被频繁调用的程序中(称为"宿主"),例如这里的 AutoEXEC·BAT 和 Command·COM。"病毒"程序包括引导,选择时机,传染和表现四个部分。计算机病毒通常是利用宿主被用户调用而引导的,例一和例二则分别利用了 AutoEXEC·BAY 和 Command·COM 的自举特性。

## 2.2 计算机病毒宿主

正如感冒病毒与患感冒的人是完全不同的两个客体,计算机病毒与病毒宿主是完全不同

的两个概念。在图 2.1 中，第 2-8 行是计算机病毒程序，而整个 AutoEXEC · BAT 是病毒的载体(或宿主)。在图 2.2 中，整个程序是计算机病毒的宿主，而病毒只是其中从检查时机到表现自己这一部分。形式化地描述，我们有如下的定义：

在运行时能够复制自身，并利用信息通道进行传播，以占用系统资源或造成其它危害为目的的程序块或程序集合，称为计算机病毒。被人工或计算机病毒强制地插入了计算机病毒的系统驻留程序和磁盘文件，分别称为计算机病毒的内存宿主和磁盘宿主。

每一种计算机病毒都有磁盘宿主，大多数病毒都有内存宿主。

以小球病毒 为例，感染小球病毒的引导程序是磁盘宿主，但是，系统启动后，引导程序已失去系统控制权，而计算机病毒寄生在系统中断程序 Int13H 中，Int13H 是内存宿主。同样地，感染黑色星期五的磁盘文件是磁盘宿主，而中断服务程序 Int8H 和 Int21H 是内存宿主。

如果把内存宿主比喻成传播疾病的疟蚊，则磁盘宿主是滋生疟蚊的沼泽地。因此，制止传染就要消灭内存宿主，而根治病毒就要诊治磁盘宿主。

## 2.3 计算机病毒的分类

在计算机病毒分类学中，有多种观点，例如可根据危害性，表面形式，解剖特点，或宿主类型等对计算机病毒进行分类。

按危害性分为良性和恶性病毒，以其是否销毁数据为定性分界线。但按此分类法，震惊计算机界造成重大损失的 Morris 蠕虫也要归为良性。

按表面形式，可引出定时炸弹、蠕虫、特洛伊木马等概念；按解剖特点，可引出前插式、后插式、间隙插入式等概念。这两种分类方法都有界线不清，对诊治无益的缺点。我们建议按宿主类型分类。如下：

1. 内存宿主型。

2. 磁盘宿主型。其中：B1，主引导区寄生型；B2，引导区寄生型，B3，可执行文件寄生型(EXE，COM，BAT，OVR，ObJ 文件)。

包含在不可执行的源程序中的病毒语句行可阅读，容易摘除，编译后成为可执行文件，才具有伪装性和危害性，因此归属于可执行文件寄生型。

## 2.4 分类诊治策略

主引导区(分区表扇区)，引导扇区，中断表共计 512+512+1024=2048 字节，不难提取上述三要素的无病毒的正本，加以保存。亦不难利用正本覆盖当前值。不管病毒程序如何千变万化，一定版本的 DOS，一定规格的磁盘对应的三要素正本是唯一的。因此用一正而压万邪，可轻取这三个寄生类型的计算机病毒。

病毒克星软件把提取正本的工具交给了用户，由用户在自己的软硬件环境下提取正本，就能适应 DOS 版本的升级和磁盘类型变化，从而能对付未来的病毒(详见第四章)。

执行文件的字节数是至关重要的指标，第 4.8 节将证明：不可能设计出个能攻击程序字节数的病毒程序。因此，提取和保存无毒可执行文件字节数存档，定期、自动地检查可执行文件的字节数，可以提供感染病毒的可疑程序清单，进而对执行该程序前后的中断表进行比较，以便确诊。

自然地，人们会要求能自动地对感染了病毒的可执行程序作“外科手术”，切除病毒程序块或加免疫标志。由于计算机病毒千差万别，迄今尚未总结出一般规律，目前我们的最佳成果是带有知识库的 V—Doctor·EXE。由反病毒工作程师理解并获取计算机病毒解剖结构参数之后，通过 V—Doctor 学习机制加进其知识库。因此 V—Doctor 只能切除已知的，经过深入研究的病毒代码块(详见第八章)。

# 第三章　防治计算机病毒的简单方法

这里所谓的“简单”，是指不需要深入钻研，不需要投资购买软件，不需要花大力气开发，而是利用现成的通用软件，按一定规则操作来防治病毒。事实上，这些方法主要靠手动，要求操作者仔细、认真、严格遵守 3.3 节的安全原则（其实这样做，其操作过程不能自动重复，使用手续上并不比第四章开发的病毒克星软件简单）。

## 3.1　消除引导区寄生型病毒

在保证内存中无病毒的条件下（例如用无病毒的系统软盘启动机器），用无病毒的 Debug 按照图 3.1 所示的方法提取引导区作为正本或用正本覆盖目标盘引导区，可以消除目标盘上的一切引导区寄生型病毒（其中扩展名.21S 表示 2.1 版本，软盘(Soft)）。

| 提取引导区： | 覆盖引导区： |
| --- | --- |
| Debug 〈CR〉 | Debug 〈CR〉 |
| L100 盘号 01 〈CR〉 | N DosBoot.21S 〈CR〉 |
| N DosBoot.21S 〈CR〉 | L 〈CR〉 |
| RCX | W100 盘号 01 〈CR〉 |
| CX：200 〈CR〉 | Q 〈CR〉 |
| W 〈CR〉 | |
| Q 〈CR〉 | |

图 3.1　用 Debug 提取和覆盖引导区

## 3.2　消除硬盘主引导区寄生型病毒

在保证内存无病毒的条件下，用未感染病毒的 Norton unility 程序 NU·EXE，按照图 3.2 所示的方法可以提取硬盘主引导区（即分区表扇区）作正本或用正本覆盖目标盘上总引导区，可以消除目标盘上一切寄生于主引导区（即分区表扇区）的计算机病毒（如大麻病毒）。

提取总引导区.　　依次选择下列菜单项：

Explore dise/Choose Item/Absolute sector/C：盘/
0 面，0 柱，1 道 总数 1/Write Item to disk/Abdolute sector/
File 模式/写 A：盘/文名：MainBoot.C/Yes

覆盖总引导区.　　依次选择下列菜单项：
到 A：盘/Choose Item/File/选文件 MainBoot, C/Write/
Absoluto Sector mode/写到 C：盘/0 面，0 柱，1 道/Yes

图 3.2　用 NU.EXE 提取和覆盖引导区

## 3.3 安全原则

进行上述两项操作时，请注意：

1. 操作之前，把重要的数据制作软盘备份，以防万一。

2. 先提取原来的主引导扇区、引导扇区，保存在工具盘（例如 A 盘）的 Old-Main・21C 或 Old-Boot・21C 中，这里 21C 表示 DOS 版本 2.1，C 盘。不要存在被处理盘上。这是因为手动操作，容易失误，一旦击键引起失误，被处理盘可能无法读出。失去了原来的引导扇区，就后悔莫及了。

3. 上述过程必须在无病毒条件下操作，否则提取和覆盖的引导扇区是带病毒引导扇区。

4. 坚持从哪里来，到哪里去的原则。因为不同盘上的分区表可能不同，引导区中的 BPB（磁盘基本参数块 Basic Parameter Block）可能不同，如果张冠李戴，被处理的盘则无法再读。因此，备份的扩展名上应能暗示版本号和盘号，以便区别来龙去脉。推荐用类似于 *・32C 的扩展名来对应于 DOS3.2 版 C 盘……等等。

5. 覆盖完后，不要急于重新启动机器，此时关于被处理盘的若干格式信息尚保留在内存中，应再提取一次引导区或分区表，与正本以及保存的原版对照，如有手误，尚可补救。

## 3.4 病毒传播链的重要环节

硬盘是计算机病毒传播链上的缓冲地，培养基和转播站。下列几条可以减少硬盘被感染的机会：

1. 尽量用硬盘起动，可减少 C 感染引导区寄生型及主引导区寄生型病毒。

2. 测试来历不明的软盘之前屏蔽 C 盘。例如 DOS 的外部命令 Assign C=B，可以把对 C 盘的操作转移到 B 盘上。有的机器上有 C 盘电源开关，可以关掉 C 盘电源。

3.1 和 3.2 所述方法，不能自动化，容易出错。感染一次，就得重新操作一次，十分繁琐。若干文献介绍过更复杂的方法。例如用 Debug 提取文件时，加上了修改过程，更易手误。有一条关于人类心理与行为的法则：凡是有可能出错，且仅仅依靠细心检查来维持运行的繁琐过程，就一定有人会出错。正是基于这一事实，人们才研制了各种机械互锁、电气互锁和安全装置，也正是基于这一条，我们才研究了下一章要介绍的广谱抗病毒技术。