《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

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)

电子工业出版社总发行　各地新华书店经售

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　　1990 年 9 月第 1 次印刷

印数：1–12,000 册　　定价：2.50 元

书号：ISBN7–5053–1111–5／F · 179

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

目　　录

第一章　计算机病毒概述

1. 什么是计算机病毒？ …… (1)
2. 计算机病毒是在什么情况下出现的？ …… (1)
3. 计算机病毒的来源有哪些？ …… (1)
4. 计算机病毒是如何分类的？ …… (2)
5. 计算机病毒一般具有哪些特点？ …… (2)
6. 微型计算机病毒寄生的主要载体是什么？ …… (2)
7. 计算机病毒在磁盘中存储有哪几种情况？ …… (2)
8. 计算机病毒的寄生方式有哪几种？ …… (3)
9. 目前计算机病毒的破坏作用表现在哪些方面？ …… (3)
10. 计算机病毒的工作过程应包括哪些环节？ …… (3)
11. 计算机病毒有哪些共性？ …… (4)
12. 不同种类的计算机病毒的传染方式有何不同？ …… (6)
13. 计算机病毒传染的先决条件是什么？ …… (6)
14. 计算机病毒的传染通过哪些途径？ …… (6)
15. 计算机病毒的传染是否一定要满足条件才进行？ …… (7)
16. 微型计算机病毒对系统的影响表现在哪些方面？ …… (7)
17. 计算机病毒传染的一般过程是什么？ …… (7)
18. 可执行文件感染病毒后又怎样感染新的可执行文件？ …… (7)
19. 操作系统型病毒是作样进行传染的？ …… (8)
20. 操作系统型病毒在什么情况下对软、硬盘进行感染？ …… (8)
21. 操作系统型病毒对非系统盘感染后最简单的处理方法是什么？ …… (8)
22. 目前发现的计算机病毒主要症状有哪些？ …… (8)
23. 目前传入我国的计算机病毒主要有哪几种？ …… (9)
24. 用户如何预防计算机病毒？ …… (9)
25. 如何从管理措施上预防计算机病毒的传播？ …… (10)
26. 在什么情况下怀疑计算机病毒已入侵？ …… (10)
27. 何谓计算机病毒的静态检查和动态检查？ …… (10)
28. 计算机病毒的检测有哪几种方式？ …… (10)
29. 怎样通过计算机病毒的传染机制检测病毒？ …… (11)
30. 怎样通过系统内存容量的变化检测病毒？ …… (11)
31. 诊治计算机病毒的一般步骤是什么？ …… (12)

第二章　检测和防治微型计算机病毒的准备

32. 诊治微型计算机病毒应在哪些方面作些准备? …… (13)
33. DOS由哪几部分组成?各部分的功能是什么? …… (13)
34. 正常情况下DOS启动的过程是怎样的? …… (15)
35. DOS是怎样划分磁盘空间的? …… (17)
36. 什么是磁盘参数表? …… (17)
37. 文件目录表向用户提供哪些信息? …… (18)
38. 文件分配表向用户提供哪些信息? …… (19)
39. PC-DOS怎样使用文件目录表和文件分配表FAT? …… (19)
40. 各类磁盘基本输入／输出参数有哪些? …… (20)
41. 已知病毒程序所在扇区号怎样找出FAT对应位置上损坏标志"FF7"? …… (20)
42. PC-DOS引导记录中前32个字节的含义是什么? …… (20)
43. ROM BIOS有哪些功能?由哪几部分组成? …… (22)
44. PC-DOS的系统中断是怎样分配的? …… (23)
45. ROM BIOS提供哪几种类型的中断? …… (24)
46. 在PC-DOS支持下格式化的硬盘和软盘在结构上有何不同? …… (25)
47. PC-DOS启动后内存分配情况是什么样? …… (26)
48. 怎样使用DEBUG程序? …… (26)
49. 怎样使用PCTOOLS工具软件? …… (28)

第三章　微型计算机常见病毒的分析与消除

50. 圆点病毒有哪些别名? …… (30)
51. 圆点病毒是哪一种类型的病毒? …… (30)
52. 圆点病毒是何症状? …… (30)
53. 圆点病毒的组成包括哪些部分? …… (30)
54. 感染圆点病毒后DOS启动的过程是作样的? …… (30)
55. 圆点病毒程序的引导部分装入内存后主要做哪几件事? …… (30)
56. 圆点病毒的变异病毒有哪些?症状如何? …… (31)
57. 圆点病毒特征有哪些? …… (31)
58. 圆点病毒在磁盘中是如何存放的? …… (31)
59. 圆点病毒是在什么情况下被引导的? …… (32)
60. 圆点病毒的工作机理是什么? …… (32)
61. 感染圆点病毒盘与正常磁盘有哪些不同之处? …… (32)
62. 圆点病毒有否破坏作用? …… (33)
63. 圆点病毒的感染方式有哪些? …… (33)
64. 圆点病毒传染的条件是什么? …… (33)
65. 圆点病毒传染的过程是如何进行的? …… (33)
66. 圆点病毒在什么情况下对硬软盘进行感染? …… (33)

67. 圆点病毒的静态传染和动态传染有何区别? …… (34)
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? …… (34)
69. 怎样诊断软硬盘是否有圆点病毒? …… (34)
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? …… (36)
71. 清除圆点病毒应从哪些方面入手? …… (47)
72. 怎样消除圆点病毒? …… (47)
73. 怎样使磁盘免疫圆点病毒侵入? …… (48)
74. 大麻病毒有哪些别名? …… (48)
75. 大麻病毒是哪一种类型的病毒? …… (48)
76. 大麻病毒有何症状? …… (49)
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? …… (49)
78. 大麻病毒的破坏性对软盘和硬盘是否相同? …… (51)
79. 大麻病毒是如何在磁盘上存放的? …… (51)
80. 大麻病毒与圆点病毒在传染方式有何不同? …… (51)
81. 怎样检测大麻病毒? …… (52)
82. 为什么对感染大麻病的硬盘进行普通格式化不能消除?怎样解决? …… (52)
83. 消除大麻病毒常采取哪些方法? …… (53)
84. 非系统软盘如何免径大麻病毒入侵? …… (53)
85. Brain病毒有哪些别名?是什么类型病毒? …… (53)
86. Brain病毒有何症状? …… (54)
87. Brain病毒的标志是什么? …… (54)
88. Brain病毒的特征是什么? …… (54)
89. Brain病毒与圆点病毒在磁盘上存放有何不同? …… (54)
90. Brain病毒在内存中如何实现链接? …… (54)
91. Brain病毒感染的方式有哪些?在磁盘上是如何分布的? …… (54)
92. Brain病毒在什么情况人破坏盘上的数据? …… (54)
93. 怎样检测Brain病毒? …… (54)
94. 清除Brain病毒分哪几步? …… (55)
95. 怎样才能使软盘具有免除感染Brain病毒能力? …… (55)
96. 黑色星期五病毒有哪些别名? …… (55)
97. 黑色星期五病毒是哪一种类的病毒? …… (55)
98. 黑色星期五病毒有哪些表现形式和症状? …… (55)
99. 黑色星期五病毒传染哪些机型?传染的主要途径有哪些? …… (56)
100. 黑色星期五病毒由哪几部分组成? …… (56)
101. 黑色星期五病毒标志是什么?如何显示这种标志? …… (56)
102. 如何诊断黑色星期五病毒的存在? …… (58)
103. 怎样清除黑色星期五病毒? …… (58)
104. 怎样预防黑色星期五病毒的侵入? …… (59)
105. 黑色星期五病毒是否感染PC—DOS的内部命令? …… (59)

106. 648病毒是一种什么性质的病毒? …… (59)
107. dBASE病毒是一种什么样的病毒? …… (59)
108. 雨点病毒是一种什么样的病毒? …… (59)
109. 怎样消除杨基多得病毒? …… (60)

第四章　微型计算机常用检测和解病毒软件及其使用简介

110. 目前常用检测和解病毒软件主要有哪些?怎样使用? …… (61)
111. 国内还有哪些检测和消除病毒软件? …… (66)

附录1.　计算机病毒名称中英文对照表 …… (68)
附录2.　微型计算机病毒一览表 …… (69)
附录3.　世界流行的其他52种计算机病毒简介 …… (71)

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 . ! . 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。

(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。

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人的有效方法，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