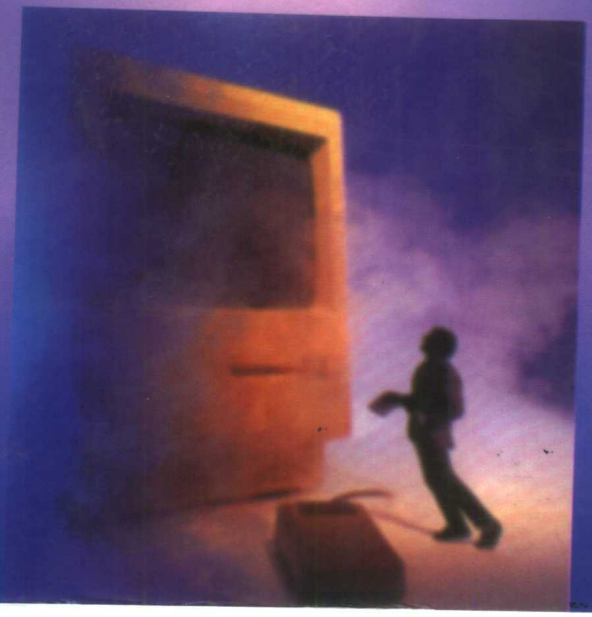
当代计算机职业培训系列教程

# 计算机病毒剖析大全



黄瑞强 编著

机械工业出版社

当代计算机职业培训系列教程

# 计算机病毒剖析大全

黄瑞强　编著

机械工业出版社

## 内 容 简 介

本书详细地介绍病毒起源，阐述计算机病毒分类、原理及解毒方法，并对数十种目前流行较广，危害较大的病毒，逐一进行剖析，详细给出了查毒及消除病毒的方法。

本书适合于计算机系统维护人员、技术开发人员及一般计算机用户、大专院校师生阅读。



**本书版权登记号：图字：01-96-0680**

**图书在版编目(CIP)数据**

计算机病毒剖析大全/黄瑞强编著. —北京：机械工业出版社，1996.7

ISBN 7-111-05188-2

Ⅰ.计… Ⅱ.黄… Ⅲ.计算机病毒-研究 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(96)第 10387 号

出 版 人 马九荣(北京市百万庄南街 1 号 邮政编码 100037)

责任编辑：李会武

三河永和印刷厂印刷·新华书店北京发行所发行

1996 年 7 月第 1 版·1996 年 9 月第 2 次印刷

787×1092mm 1/16·7.75 印张·200 千字

5 001—9 000 册

定价：16.00 元

# 序　言

计算机病毒，相信您一定不陌生，大部分使用过计算机的人，都曾经有过中毒的经历，运气好的话，还可以使用一般查毒程序立即检测出来，但也有不少的使用者是在病毒发作时，才发现病毒的存在。遇上比较好心的病毒，发作时顶多演奏一些音乐或是在屏幕上显示一些信息吓吓人，但是万一碰到比较恶劣的病毒，那您的硬盘大概就此报销了。至于事后的资料重建工作，则往往要花费上数小时、数天甚至数月的时间，更甭提那些根本无法重建的资料文件了。

近来由于局域网及 Internet 的盛行，使得计算机病毒有更顺畅的活动空间，一个硬盘同时感染上数种病毒已经不是什么稀奇的事，学校计算机中心的计算机集体中毒事件亦比比皆是。而国内有关计算机病毒方面的书籍，大部分皆为翻译或是抄袭国外的作品，其中讲的尽是一些非常抽象而不切合实际的理论，或是干脆列举一些国外老旧病毒的发作实例。

作者目前正从事“黑将病毒克星”软件的设计工作，必须成天与计算机病毒为伍，故有机会搜集到国内各种流行的病毒。本书中所剖析的每一个病毒，作者都花了不少的功夫实际跟踪过。这其中经常为了研究一个病毒的特性而彻夜不眠，或是为了“验证”病毒的破坏力，而毁了硬盘无数次。现在将这些得来不易的病毒资料集成书发表，希望本书能成为您对付计算机病毒不可或缺的一本工具参考书。

本书共分为三大部分，第一部分为计算机病毒知识篇，目的在于让读者能够了解各类型病毒的感染及治疗原理，并告诉您如何检测及采样新病毒。另外本部分亦澄清了几个错误观念，并附上 30 个读者最常提出的问题及其解答。希望通过此部分的说明，能够使您了解一些比较正确的计算机病毒观念。

第二部分为计算机病毒解毒篇，此部分包含了目前流行病毒的特征介绍，并公布其识别字符串及解毒方法。一般初学者即使不会编写解毒程序，亦可照着书中的解毒实例操作，以达到自行治疗的效果。会写程序的读者更可利用本部分所公布的解毒资料，以自己最擅长的计算机语言，编写查毒或解毒程序。

最后一部分为计算机病毒整理篇，读者可通过本部分的内容，快速查阅出各个病毒的特性及病毒彼此之间的血缘关系。而“病毒名称对照表”更可使您对众多的病毒名称不再感到混淆不清。

本书虽经再三校阅，但疏误在所难免，尚祈读者批评指正。

黄瑞强

# 目 录

序言
第一部分 计算机病毒知识篇 …… 1
第 1 章 计算机病毒的分类及感染原理 …… 1
1.1 什么是计算机病毒 …… 1
1.2 计算机病毒与特洛伊的区别 …… 1
1.3 计算机病毒的分类 …… 2
1.4 开机型病毒的感染原理 …… 2
1.5 文件型病毒的感染原理 …… 4
1.6 复合型病毒的感染原理 …… 7
第 2 章 治疗病毒的原理及检测和采样新病毒 …… 8
2.1 开机型病毒的治疗原理 …… 8
2.2 文件型病毒的治疗原理 …… 9
2.3 复合型病毒的治疗原理 …… 11
2.4 利用 SYS 程序治疗开机型病毒 …… 11
2.5 无法治疗的病毒 …… 12
2.6 新病毒的检测方法 …… 12
2.7 新病毒的采样方法 …… 12
第 3 章 几个错误的观念 …… 14
3.1 概述 …… 14
3.2 特洛伊型、爆炸型、隐形飞机式病毒 …… 14
3.3 不可执行中毒软盘上的文件 …… 15
3.4 如何清除内存中的病毒 …… 15
3.5 程序最好具有自我治疗的能力 …… 15
3.6 病毒可突破防写标签的保护 …… 16
3.7 病毒藏在 CMOS RAM 中 …… 16
3.8 能解最多种病毒的程序就是最好的 …… 17
3.9 万能自制解毒剂 …… 17
第 4 章 局域网与计算机病毒 …… 19
4.1 基本概念 …… 19
4.2 如何编写网络版的解毒程序 …… 19
4.3 可能会遇到的问题 …… 20
第 5 章 计算机病毒问答集锦 …… 21
第二部分 计算机病毒解毒篇 …… 29
第 6 章 治疗病毒的注意事项 …… 29
6.1 一般注意事项 …… 29
6.2 利用标识字符串检测病毒 …… 29

第 7 章　流行病毒总剖析 …… 32
1　382/Virus102 病毒 …… 32
2　405 病毒 …… 32
3　1181/1184 病毒 …… 33
4　1451 病毒 …… 35
5　1554/1559 病毒 …… 37
6　1813 病毒 …… 39
7　1813-B 病毒 …… 40
8　2187 病毒 …… 42
9　2900/Taiwan3 病毒 …… 44
10　3012 病毒 …… 46
11　Aircop(空中警察)病毒 …… 48
12　Airwolf(飞狼)病毒 …… 49
13　Bee(小蜜蜂)病毒 …… 51
14　Bloody 病毒 …… 53
15　Blue Danube(蓝色多瑙河)病毒 …… 54
16　Brain(大脑病毒)病毒 …… 56
17　Cartier 病毒 …… 58
18　Disk killer(硬碟杀手)病毒 …… 60
19　DOOM I(毁灭病毒第一代)病毒 …… 62
20　DOOM I-B(毁灭病毒第一代 B 型)病毒 …… 63
21　DOOM II(毁灭病毒第二代)病毒 …… 64
22　Friday the 13th(13 号星期五)病毒 …… 66
23　Friday-B(13 号星期五 B 型)病毒 …… 68
24　Friday-C(13 号星期五 C 型)病毒 …… 69
25　Greensleeves(绿袖子)病毒 …… 71
26　Ha! Ha! (哈哈病毒)病毒 …… 73
27　Ha! Ha! -B(哈哈病毒 B 型)病毒 …… 75
28　Joshi 病毒 …… 77
29　MusicBug V1(音乐臭虫)病毒 …… 78
30　New Aircop(新空中警察)病毒 …… 80
31　New Aircop-B(新空中警察 B 型)病毒 …… 81
32　PLASTIQUE 5.21(塑料炸弹)病毒 …… 81
33　PLASTIQUE-27 病毒 …… 83
34　Stoned(石头病毒)病毒 …… 85
35　Stoned-B(石头病毒 B 型)病毒 …… 88
36　Stoned-C(石头病毒 C 型)病毒 …… 89
37　Stoned II(石头病毒第二代)病毒 …… 90
38　Sunday(快乐星期天)病毒 …… 92
39　Sunday-B(快乐星期天 B 型)病毒 …… 94
40　Sunday-C(快乐星期天 C 型)病毒 …… 95
41　Sunny(晴天炸弹)病毒 …… 97
42　Sunny-B(晴天炸弹 B 型)病毒 …… 98

43 Symphony No. 40(第 40 号交响曲)病毒 …… 99
44 Two Tigers(两只老虎)病毒 …… 101
45 Vienna(维也纳)病毒 …… 103
46 Vienna-B(维也纳 B 型)病毒 …… 104
47 Wolfman(狼人)病毒 …… 105
第三部分 计算机病毒整理篇 …… 107
第 8 章 病毒特性一览表 …… 107
第 9 章 病毒名称对照表 …… 109
第 10 章 病毒血缘关系表 …… 111
第 11 章 病毒发作时间表 …… 112
附录 A DEBUG 指令摘要 …… 113
附录 B .EXE 文件的 Header 结构 …… 115
附录 C 中英文名词对照表 …… 116

# 第一部分　计算机病毒知识篇

## 第 1 章　计算机病毒的分类及感染原理

### 1.1　什么是计算机病毒

计算机病毒就是一个程序，其可能隐藏在磁盘的引导扇区、分区表或是程序文件中，具有自我复制的能力，在某特定条件成立时，即从事某特定的(破坏)动作。

从上面的定义可知，计算机病毒共包含两段程序，第一段程序专门负责做感染动作(自我复制)，第二段程序则用来判断某特定条件是否成立，若成立便执行破坏计算机资源或是吓唬使用者的动作。

我们可将一般文书软件与病毒程序做个比较，您便可对计算机病毒有更深一层的了解。前者的目的在于让使用者很方便地去处理文书资料，而后者的目的则在于感染及破坏；前者可用 DIR 指令确定其位置，而后者为隐藏在磁盘的某一处，使用者根本不知道它的存在；最重要的是，前者的执行乃出自于使用者本身意愿，而后者的执行则出自于病毒事先的安排(感染)，使用者完全不知情。

### 1.2　计算机病毒与特洛伊的区别

许多人常将电脑病毒与特洛伊程序搞混，甚至有“特洛伊型病毒”的名称出现，于是许多根本不是病毒的文件，亦被冠上病毒的名称，使得一般人误以为市面上真有那么多种病毒，事实上不然。

所谓特洛伊木马(Trojan Horse)，或称特洛伊程序，是指一个执行时表面上看起来正常，而暗地里却从事破坏动作的程序。

这个名词起源于古希腊“木马屠城记”的神话，当希腊人久攻不下特洛伊(Troy)城时，便假装撤退，并送给特洛伊人一只大木马，内藏一批希腊士兵。特洛伊人不疑有诈，便将大木马推入城内，当夜晚来临时，藏在大木马内的士兵便悄悄地将城门打开，城外的希腊人则一拥而入，一举攻下特洛伊 城，这就是 Trojan Horse 名称的由来。

所以我们可以把特洛伊程序看成是一个假的礼物，表面上看起来“还不错”，但实际上它却在暗地里破坏您计算机内的资源。有时这种特洛伊程序是程序设计者不小心写错而产生的，由于在执行时“表面”上看起来一切正常，故连设计者本身亦不知情。

综上所述，我们可以很清楚的看出计算机病毒和特洛伊程序有何不同，即计算机病毒具有感染的能力，而特洛伊程序则无。换句话说，计算机病毒就是具有自我复制能力的特洛伊程序。而我们真正关心的，亦即本书所要探讨的是计算机病毒，而不是特洛伊程序，因为只要您不随便去执行不明的程序文件，便可避免碰到特洛伊程序。

从另外一个观点来看，只要您在撰写程序时，不小心产生了一个 Bug，而这个 Bug 将导致计算机系统不正常的运作，更糟糕的是您并不知情，于是您也制造出了一个特洛伊程序，象这种情况屡见不鲜，很显然并不是我们所要研究的课题。

## 1.3 计算机病毒的分类

若依据病毒程序感染的途径，则可将计算机病毒分为三大类。

1）开机感染型病毒。本类型病毒通过执行开机动作，作为感染的途径。比较流行的此类型病毒有“Brain”、“Disk Killer”、“Aircop”、“Stoned”、“Stoned II”等。

2）文件感染型病毒。本类型病毒通过执行中毒程序，作为感染的途径。若以病毒是否常驻内存来划分，还可将本类型病毒细分为以下两种。

①常驻式。如“13 号星期五”、“Sunday”、“1554”“1181”及“Wolfman”等病毒。

②非常驻式。如“Vienna”、“Sunny”、“382”、“405”及“Cartier”等病毒。

3）复合感染型病毒。综合上述两类型病毒的“功能”于一身的病毒，即不管是用病毒磁盘开机也好，或是执行已感染病毒的程序，都将难逃中毒的命运。比较流行的此类型病毒，有“塑胶炸弹”及其变种“蓝色多瑙河”、“第 40 号交响曲”等。

说明：有的人将仅感染 COMMAND.COM 的“Lehigh”病毒归于另外一种类型，作者认为没有这个必要，因为“Lehigh”病毒只不过是文件感染型病毒的特例罢了，病毒类型划分太多，反而会使大众观念混淆。

说明：市面上还有所谓“特洛伊型”、“爆炸型”及“隐形飞机式”病毒等奇怪的名词，事实上所有的病毒皆属于上列三大类型，这点我们将在第 3 章中提出来加以讨论。

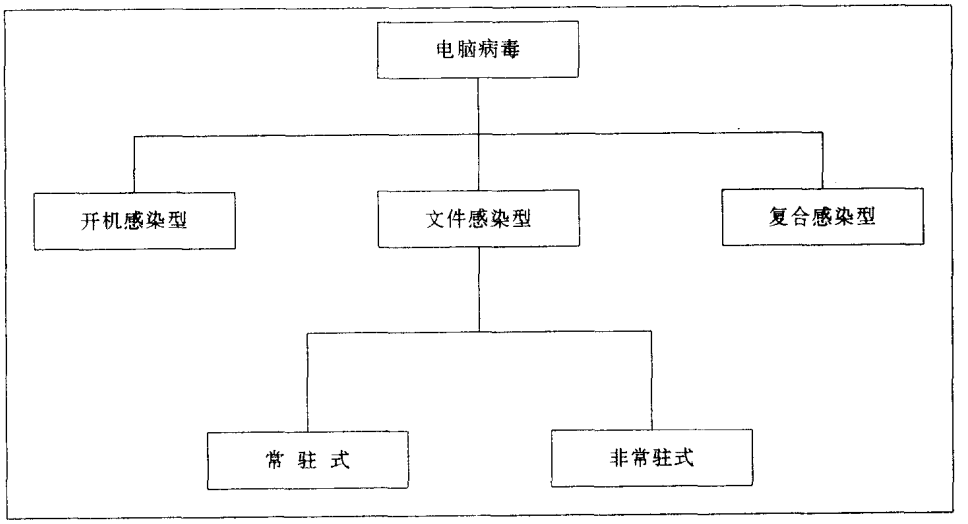



图 1-1 电脑病毒的分类

## 1.4 开机型病毒的感染原理

上节我们提过，开机型病毒通过执行开机的动作作为感染的途径。为了说明方便起见，我们将分别针对病毒感染软盘及硬盘的原理做说明，首先让我们来看看一般正常软盘的开机动作，如图 1-2 所示。

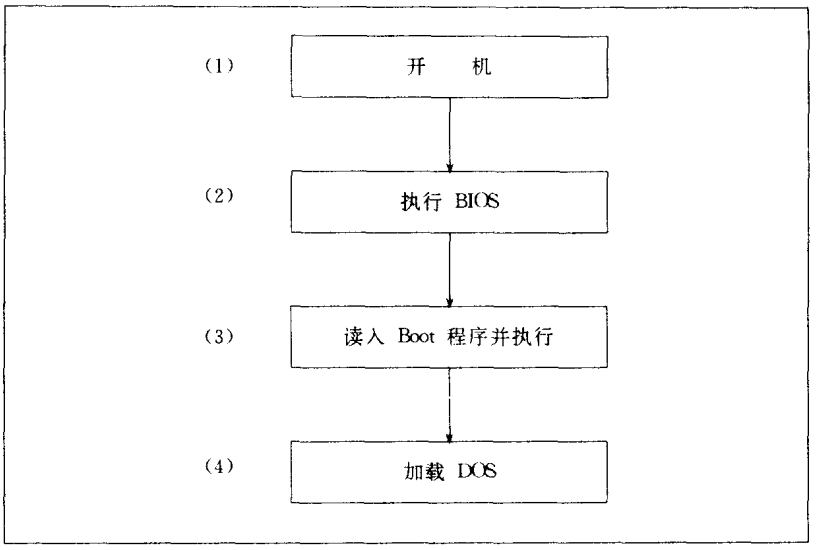



图 1-2 正常的软盘开机动作

假设某张开机软盘已经感染病毒的话，那么该软盘上的 Boot 扇区将存放着病毒程序，而不是 Boot 程序。换句话说，图 1-2 的第 3 个动作，将变成“读入病毒程序并执行”，等到病毒侵入内存后，再由病毒程序读入原始 Boot 程序，如图 1-3 所示。

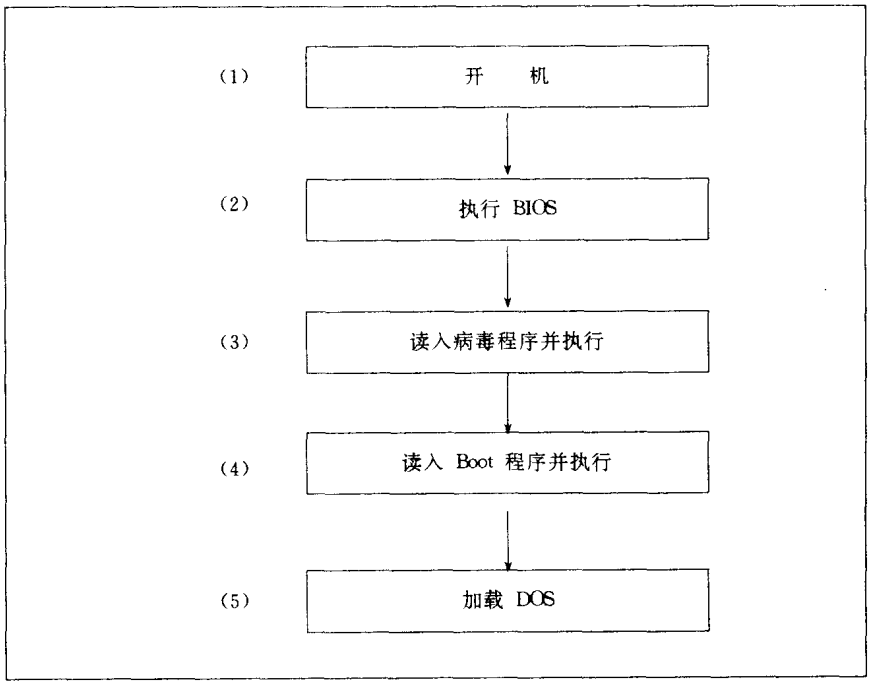



图 1-3 已中毒软盘的开机动作

既然病毒较 DOS 先一步进入内存中，自然在 DOS 下的所有读写动作亦受病毒控制，所以使用者只要对另一张干净软盘进行读写时(如 DIR、COPY 等指令)，躲在内存中的病毒，便可

立即感染该张软盘。

至于硬盘被感染病毒原理和软盘相同，但因硬盘多了一个 Partition 扇区，故我们特别分开加以说明，图 1-4 为一般正常硬盘开机动作。

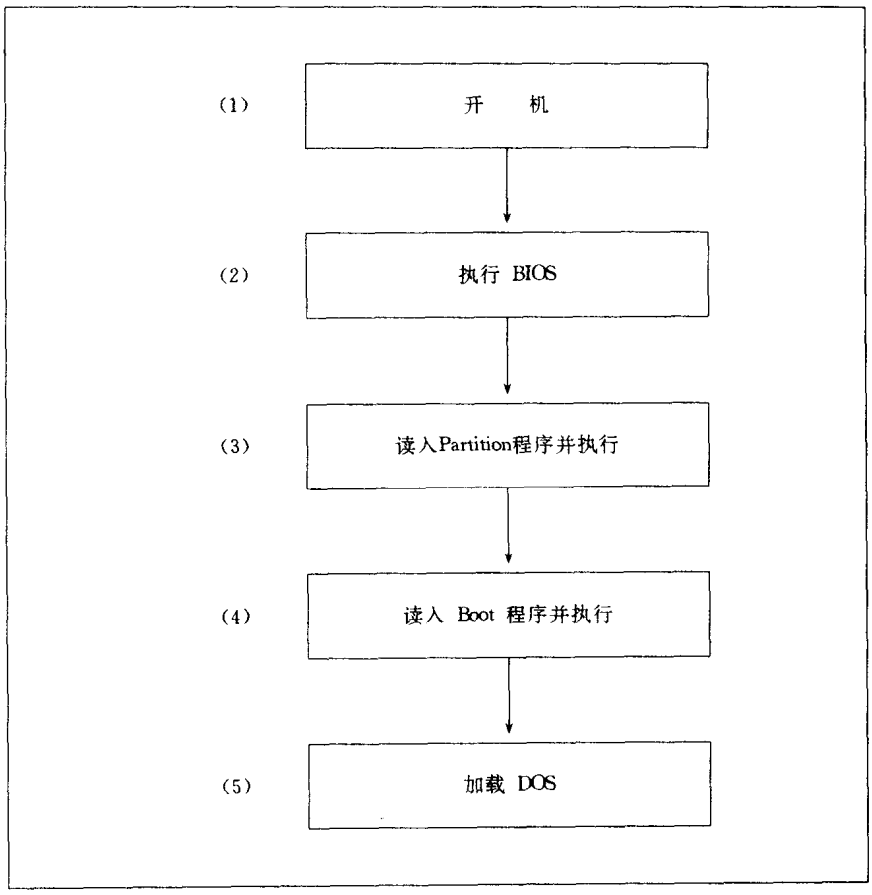



图 1-4 正常的硬盘开机动作

读者应该很明显地看出，硬盘的开机动作，只比软盘的开机动作多了一道手续，即“读入 Partition 程序并执行”。有关硬盘 Partition 扇区的内容，可参考第 6 章 Q11 的说明。

和感染软盘不同的地方是，病毒不但可以感染硬盘的 Boot 扇区，亦可以感染硬盘的 Partition 扇区。属于前者的病毒有“Brain”、“Disk Killer”及“Aircop”等，其开机动作如图 1-5 所示。属于后者的病毒则有“Stoned”，“Stoned II”及“Joshi”等，其开机动作如图 1-6 所示。

不管是软盘也好，硬盘也好，开机型病毒一定是比 DOS 早一步进入内存中，并控制读写动作(亦即拦截 INT 13h)，伺机感染其他未中毒的磁盘，这就是开机型病毒感染磁盘的原理。

## 1.5 文件型病毒的感染原理

由于文件型病毒尚可分为常驻式与非常驻式两种类型，而其感染的方法亦不相同，故我们将分开讨论其感染的原理。

顾名思义，常驻式病毒便是病毒必须常驻在内存中，以达到感染其他文件的目的。而由于

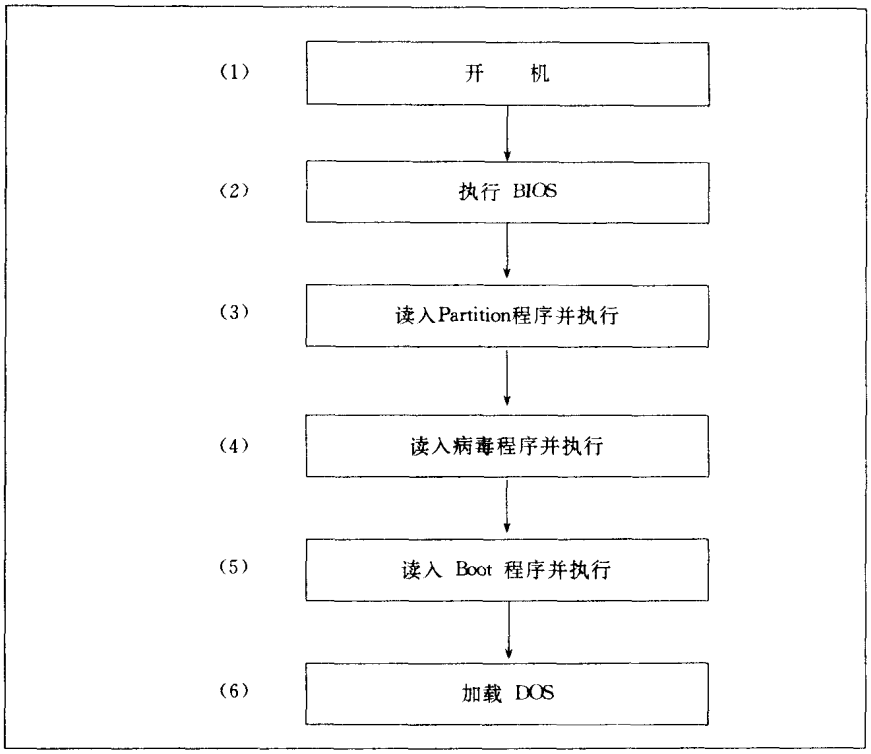



图 1-5 硬盘 Boot 扇区感染病毒的开机动作

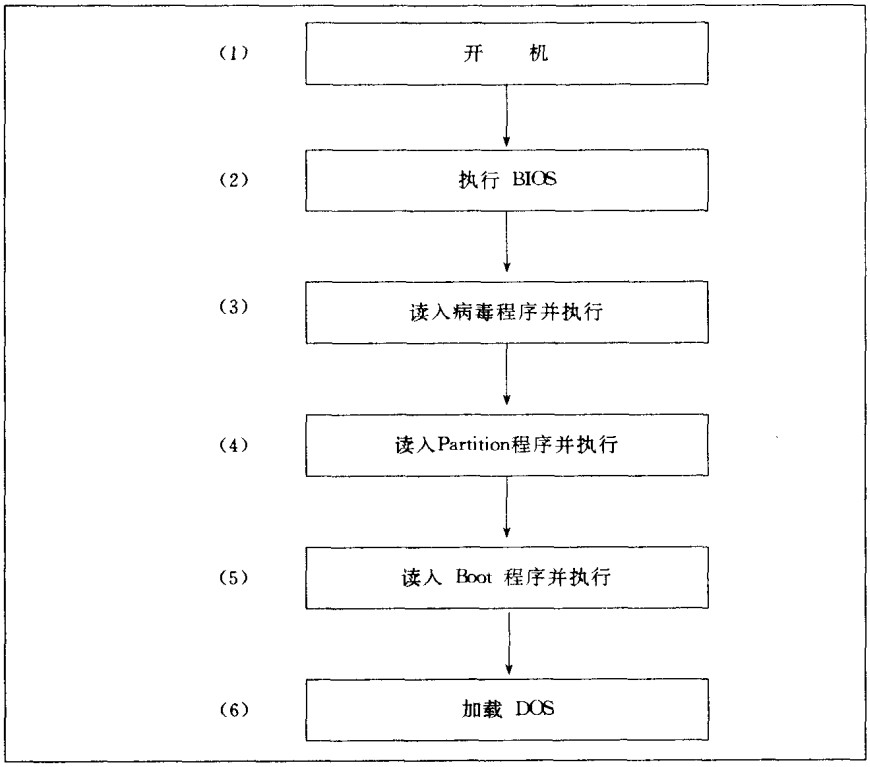



图 1-6 Partition 扇区感染病毒的开机动作

每一个程序文件在执行时，皆会调用 INT 21h，故病毒必须拦截 INT 21h 的调用，使其先通过

病毒程序，再去执行真正的 INT 21h 服务程序。为了达到这个目的，病毒便得修改中断向量表，使得记录 INT 21h 地址的值，变成记录病毒程序地址的值，如图 1-7、图 1-8 所示。

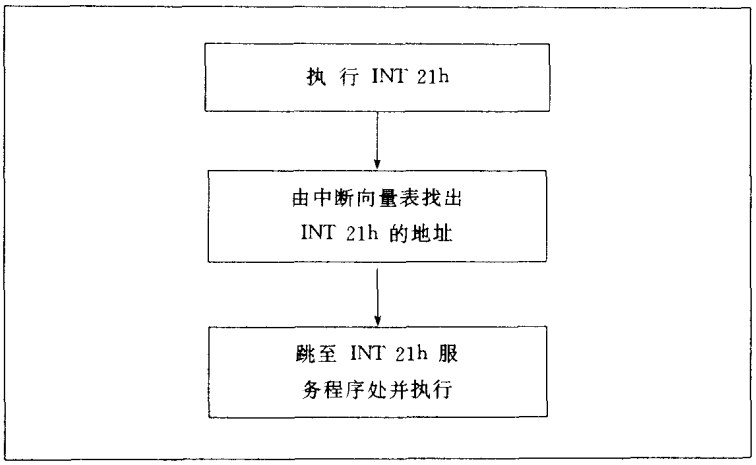



图 1-7 病毒常驻前的流程图

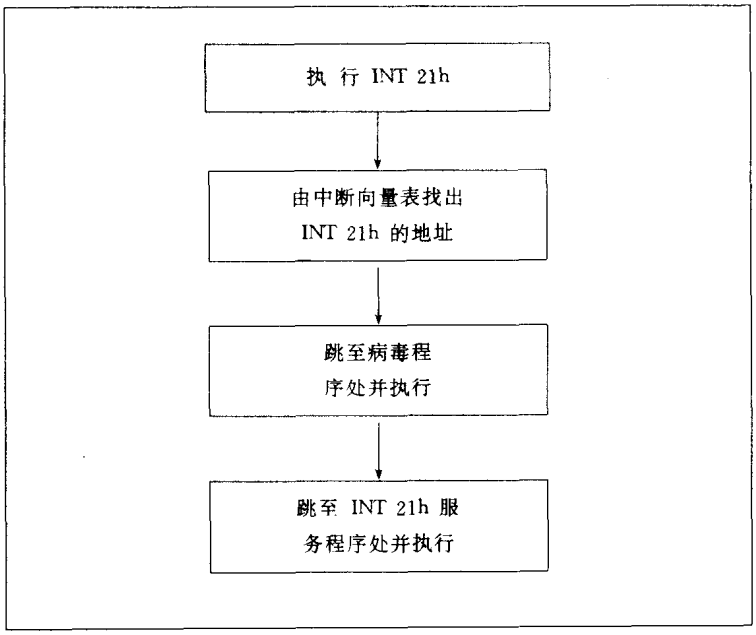



图 1-8 病毒常驻前的流程图

如此一来，每个要被执行的程序文件都要先通过病毒“检查”是否已中毒，若未中毒则病毒便会感染该文件，这就是常驻式病毒的感染原理。

值得一提的是，并非所有的病毒都是利用修改中断向量表，使得控制权转移到病毒手中。有的病毒则根本不去动中断向量表，而是直接修改 INT21h 服务程序，使其指向病毒程序。如此一来，若想通过检查中断向量表，以判定有无病毒常驻的方法便无效了，如国内非常流行的“1554/1559”病毒就是采用此法。

至于非常驻式病毒的感染原理就更简单了，只要一执行中毒的程序文件，病毒便立即寻找

磁盘中尚未感染病毒的文件，若找到了便加以感染。整个过程干净利落，根本不需要常驻式内存，所以大体上说来，这类病毒比常驻式病毒还要难被检测出来。

## 1.6 复合型病毒的感染原理

在看完了开机型与文件型病毒的感染原理后，相信您便能很容易地了解复合型病毒如何起作用。以开机动作来说，假设以感染复合型病毒的磁盘开机，那么病毒便先潜入内存中，并拦截 INT 13h，以伺机感染其他未中毒的磁盘。而当 DOS 载入内存后，病毒再拦截 INT21h 以达到感染文件的目的。

现在考虑另外一种情形，假设现在执行了一个感染复合型病毒的文件，那么该病毒除了会常驻内存，拦截 INT 21h 以感染其他文件外，尚会直接感染磁盘的引导扇区，或是分区表。所以下次当用该磁盘开机时，病毒便同时侵入内存了。

综上所述，可知不管是用中毒的磁盘开机也好，或是执行已中毒的程序文件，这类病毒都能立即侵入内存中，并伺机感染其他的磁盘或文件，这就是复合型病毒最难缠的地方。复合型病毒的出现，着实为计算机病毒的“发展”带来了另一次革命。

# 第 2 章　治疗病毒的原理及检测和采样新病毒

在了解了各类型病毒的感染原理后，我们便可针对不同类型的病毒，采取不同的治疗方法。打个比方来说，对于一张感染开机型病毒的软盘，您便不需去治疗该软盘上的文件，因为开机型病毒是不会感染文件的！

## 2.1　开机型病毒的治疗原理

在探讨开机型病毒的治疗原理前，让我们先来看看一般软盘及硬盘的物理构造，如图 2-1、图 2-2 所示。

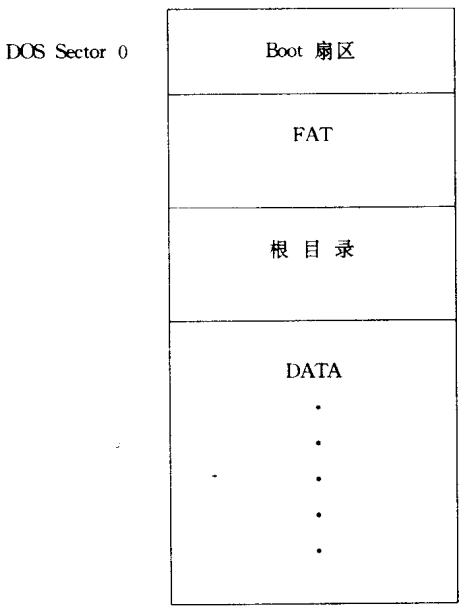



图 2-1 软盘物理分布图

我们可以很明显地看出，病毒若想一开机便常驻在内存中，它势必得感染 Boot 扇区或是硬盘 Partition 扇区，因为这两区是磁盘最开始被加载并执行的地方。所以我们要做的便是：找出原始 Boot 扇区或 Partition 扇区的存放地址，并将其移回原位(覆盖病毒)。这就是开机型病毒的治疗原理。

就软盘而言，病毒常将原始 Boot 扇区移至根目录的最后一扇区，如“Stoned”、“Stoned II”等病毒，或是移至软盘最后一扇区，如“Aircop”、“New Aircop”等病毒，其目的在于保护原始 Boot 扇区，使其不轻易被后来的文件所覆盖。有的病毒则干脆自己格式化另外一个磁盘，以存放原始 Boot 扇区及病毒码，如此便不会被人轻易发现了，如“Joshi”病毒等。

至于硬盘，那就更方便了，连格式化另外一个磁道的动作都可省下来，因为硬盘本来就有一块区域根本没有被使用，那就是硬盘的第 0 面，第 0 磁道。此磁道除了第 1 个扇区有存放 Partition 程序及分区表外，其他剩下的扇区便闲置不用。而这些扇区正是原始 Boot 或 Partition

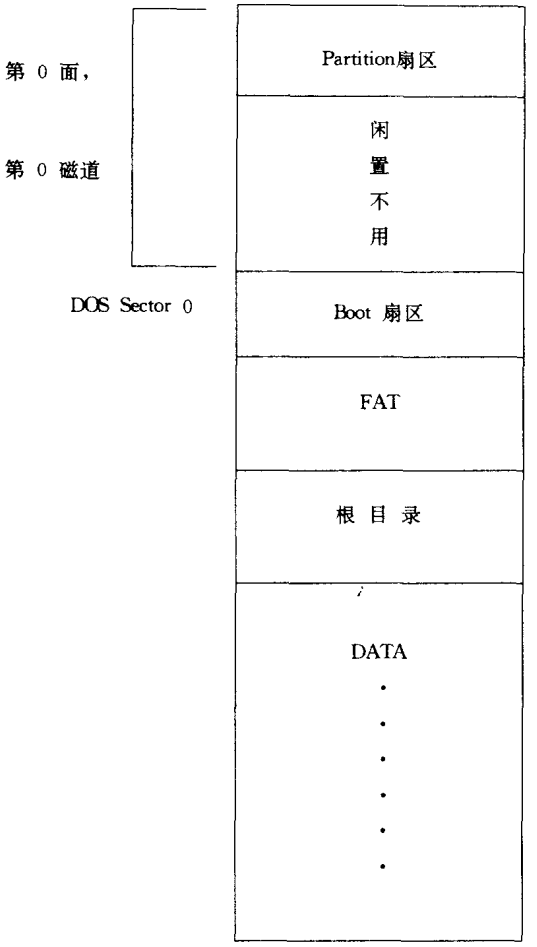



图 2-2 硬盘物理分布图

扇区及病毒码藏身的最佳场所，例如“Disk Killer”、“塑胶炸弹”系列病毒等都利用到此区。很遗憾的是这块区域 DOS 根本就管不到(即无法以 DOS 指令或是 INT 21h 调用读写此区)，请参考图 2-2，DOS 的第 0 个扇区是从 Boot 扇区开始，而非 Partition 扇区。

## 2.2 文件型病毒的治疗原理

作者在此必须先强调一点，最好最快的文件型病毒解毒方法，便是直接从备份(原版)软盘上，将未中毒的文件拷贝回来(覆盖中毒文件)即可。而本书皆假设中毒文件没有做备份，或是连备份文件也感染病毒的情况下，应该如何对该文件做解毒的工作。

由于可执行文件分为.COM 及.EXE 两种，其被感染的方式有所不同，故治疗原理亦有所差别，所以我们将分开来加以讨论。

假设图 2-3 为某一未中毒的.COM 文件，那么该文件在感染病毒后的“模样”，可能会有如图 2-4、图 2-5 两种情况。

当然这里列出的只是 2 种比较“标准”的感染模式，至于其他细节动作(如将病毒原始程序

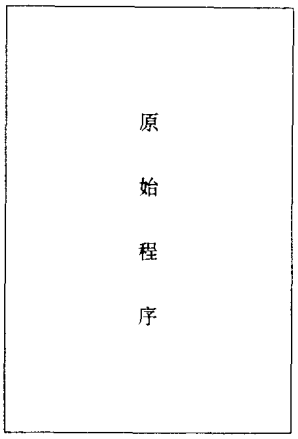



图 2-3　中毒前的.COM文件

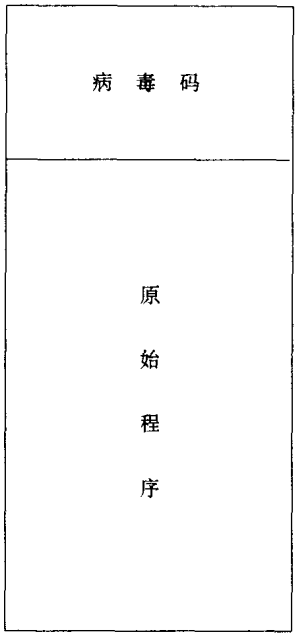



图 2-4　中毒后的.COM文件（第 1 类型）

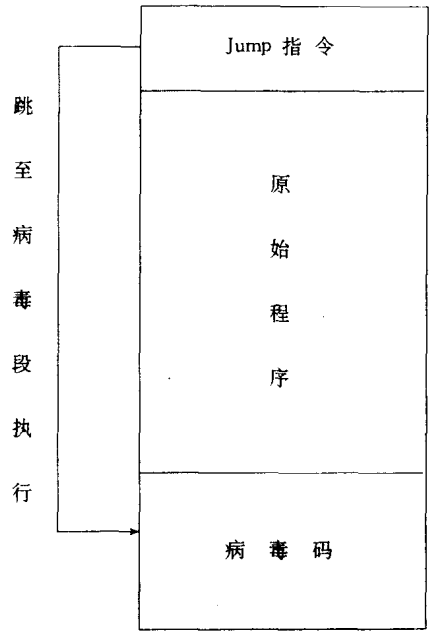



图 2-5　中毒后的.COM文件（第 2 类型）

转码，或是分割原始程序，有的甚至直接覆盖掉原始程序等），则视各病毒而有所不同，我们将在本书第二部分（计算机病毒解毒篇）加以详细说明，这里所要讲的只是一个解毒的大体观念。

由图 2-4、图 2-5，读者可以非常容易的看出，要治疗.COM 文件，仅需将病毒部分“切除”即可，实际情形亦是如此，问题是我们怎么知道哪一段是病毒码，哪一段又是原始程序呢？这就需要靠跟踪病毒码得到答案。

至于治疗.EXE 文件就比较麻烦了，因为它比.COM 文件多了一个 Header，请参考图 2-6、图 2-7（有关 Header 的结构及其相关资料，请参考本书附录 B）。

由图 2-7 我们可以看出，病毒若想要感染.EXE 文件，则必须修改其 Header 内的信息，使