# 计算机反病毒实用技术


胡存生　庄洪林　编著

人 民 邮 电 出 版 社

309.5
CS/1

# 计算机反病毒实用技术

胡存生　庄洪林　编著

人民邮电出版社

登记证号(京)143号

## 内 容 提 要

本书从微型计算机系统结构、工作原理角度入手，分析了计算机软、硬件系统尤其是DOS系统在安全性方面存在的固有弱点；在对几种有代表性的病毒程序进行详细、透彻剖析的基础上，提出了具有普遍意义的广谱反病毒技术；系统地介绍了计算机防病毒卡的工作原理、软硬件设计原理、制作方法及如何评估防病毒卡技术性能的方法；同时还介绍了常见诊治病毒工具软件的使用方法和注意事项。

本书适用于广大计算机研制、开发、应用人员和大中专院校的师生阅读参考。

**计算机反病毒实用技术**

Jisuanji Fanbingdu Shiyong Jishu

胡存生 庄洪林 编著

责任编辑 高乐忠

*

人民邮电出版社出版发行

北京东长安街27号

北京顺义振华印刷厂印刷

新华书店总店科技发行所经销

*

开本：787×1092 1/16 1994年5月 第一版

印张：10.75 1994年5月 北京第1次印刷

字数：261千字 印数：1— 8000 册

ISBN7-115-05199-2/TP·096

定价：9.60 元

# 前　言

计算机病毒的出现及迅速蔓延，给计算机的广大用户带来了极大的危害，严重地干扰了科技、金融、商业、军事等各部门的信息安全。据估计，目前计算机病毒的数量已超过5000种，且以每隔十个月翻一番的速度继续增长。面对如此众多的计算机病毒，如何进行有效的诊断和防治，已经成为摆在广大计算机工作者面前的一项重大课题。

我们根据自己多年来在计算机软、硬件维护、开发工作中以及在计算机病毒防治研究工作中所积累的经验，写成了本书。

本书共有七章。第一章介绍了计算机病毒概况，主要包括国内外计算机病毒和反病毒技术的发展概况。

第二章介绍了DOS系统的组成及其弱点。在分析DOS系统时，明确地说明了DOS系统的弱点，这对剖析病毒程序、编制消毒软件，将起到抛砖引玉的作用。

第三章通过剖析几种具有代表性的引导型病毒，介绍了如何识别、分析消除、以及防范引导型病毒的知识。

第四章主要介绍了如何诊断、剖析和消除文件型病毒的方法。

第五章主要介绍了不针对具体病毒特征，从病毒的共性角度出发诊断、分析、清除计算机病毒的广谱反病毒技术。其反病毒思想以及所列出的源程序清单均为作者几年来从事计算机防毒、消毒工作的经验总结。这些技术对诊治“新”病毒和“变种”病毒都十分有效。

通过第三、四、五章的学习，读者不仅能够学到诊治已知病毒的方法，还能够掌握有效的诊治未知病毒的技巧。

第六章向读者介绍了有关微机防病毒卡的基本知识及制作方法。学习了本章之后，读者可以了解到微机防病毒卡的工作原理、硬件结构、软件编程原理及如何评价一个防病毒卡的方法。有兴趣的读者，通过学习本章，还可以自己动手，制做一块实用的防病毒卡。

第七章介绍了几种常用的消毒软件的使用方法及注意事项。

附录中列举了世界流行的300多种病毒，包括病毒的中、外文名称对照，病毒的传播方式，被感染的程序所增加的字节数和病毒的破坏性等信息。

本书尽量避免过多的理论论述，重点在于解决实际问题的操作方法。书中给出的一些实例，无论是软件方面的源程序，还是硬件方面的电路图，均经过实际检验。

如果本书能够给从事计算机工作的朋友有所启发的话，我们将会感到莫大的欣慰，这也就达到了我们编著此书的目的。我们在几年的计算机病毒防治工作中深深地体会到，计算机病毒的防治工作，不仅需要专业人员，更需要广大计算机工作者的共同努力。

由于作者水平有限，书中难免有失误之处，恳请读者批评指正。

作　者

# 目　　录





此为试读,需要完整PDF请访问: www.ertongbook.com

# 第一章　计算机病毒简介

计算机病毒在问世后的短短几年中，其影响之广、危害之大，已令人警觉。但谁曾想，它也有一段神话般的经历，有一段从幻想到现实的过程。

## 第一节　计算机病毒发展概况

### 一、国外计算机病毒发展概况

1977 年，Thomas. t. Ryan 的科学幻想小说《The Aulescence of p－1》轰动了美国科普界。作者幻想出世界上第一个计算机病毒，可以从一台计算机传染到另一台计算机，最终将控制 7000 台计算机的操作系统，酿成一场灾难。有人认为，这实际上是计算机病毒的思想基础。

1980 年，IBM 公司的 PC 系列微型计算机逐渐成为世界微型计算机市场上的主要机型，由于其性能优良、价格便宜、发展潜力大，所以深受广大计算机用户的欢迎。但是，由于 IBM-PC 系列微型计算机系统自身的弱点，尤其是 DOS 操作系统的开放性，给计算机病毒的制造者们提供了可乘之机。因此，装有 DOS 操作系统的微型计算机成为其攻击的主要对象。

到 1987 年，即经过 10 年的时间，计算机病毒的幻想终于变成了现实。

1987 年 10 月，在美国本土，世界上第一例电脑病毒(Brain)被发现，并以强劲的势头迅速蔓延。随后，其它病毒也相继出现。

1988 年，各种病毒开始大肆流行。

以色列希伯莱(Hebrew)大学的计算机曾受到黑色星期五病毒的攻击。

“评分”(Scores)病毒感染了美国许多政府机构的计算机，并扩散到美国国会办公系统和包括波音航空公司、福特航空公司在内成百上千个公司的计算机系统。

8 月，在前苏联发现了三种计算机病毒，经多名计算机专家的共同努力，方将其消除。

9 月，与日本电气公司联机的日本最大的计算机网发生了计算机病毒入侵用户终端的事件。

11 月 2 日，世界上有史以来最严重的一次计算机病毒侵袭事件发生在美国康乃尔大学。该大学的一年级研究生罗特. 莫里斯(Robbet. T. morris)制作了一个蠕虫计算机病毒(Tap-Worm)，并将其投入到美国 Internet 计算机网络中。该病毒从 11 月 2 日上午 5 时开始发作，到下午 5 时已使美国军事系统计算机网络中的 6000 多台计算机工作站受到感染，许多联网计算机被迫停机。直接经济损失达 9600 万美元，造成了不可收拾的局面。莫里斯也由此受到了法律的制裁。莫里斯的蠕虫事件引起了美国全社会和计算机界的震惊，专家们在法律、道德、反病毒技术等方面发表了大量的评论，许多公司、研究所纷纷发表道德宣言，表示要教育职工、学生不得制造也不得传播计算机病毒。

1989 年初，日本《朝日新闻》评选 1988 年十大科技新闻，其中第二条便是：“计算机病毒入

侵日、美、苏计算机网络”，美国科学家也将“计算机病毒在欧美流行”作为1988年重要国防科技十大新闻之一。

## 二、国内计算机病毒发展状况

1. 国内计算机病毒的来源

国内计算机病毒主要有两个来源：一个来源为国外，主要是一些出国技术人员回国时带来的应用软件或游戏盘等，这些软件大多带有病毒。如小球病毒(“Bauncing ball”病毒)，在我国发现之前，在国外和香港就已有报道；“FLIP”病毒在兰州首次被发现时，国外已有消除该病毒的软件，可见“FLIP”病毒早已在国外流行；再有，“DIR-2”病毒在1992年3月份传入我国，而在此之前国外有关资料也已有报道。

国内病毒的另一个来源就是国内某些人改写国外的计算机病毒或自己制造病毒。如“广州一号”病毒即为修改“大麻”病毒而形成的变种。而Bloody病毒则为土生土长的国产病毒。

2. 计算机病毒在国内蔓延情况

1989年年初，大连市统计局的计算机上发现有小球病毒。3、4月间，重庆西南铝加工厂也有了关于计算机病毒的报道。从此以后，计算机病毒以其迅猛之势，在中国大陆蔓延。

9、10月间，北京、上海、福建等地有关部门都开展了计算机病毒的情况调查。结果表明，大约有50%以上的计算机染毒，这些病毒均针对IBM PC/XT、AT及长城286、东海、浪潮等PC系列兼容机。

1989年11月，第四次全国计算机安全技术交流会在昆明召开，与会代表专门讨论了“计算机犯罪、计算机病毒研究”等问题。

“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”被选为1989年我国计算机界十大事件之一。

据1989年11月份《中国日报》报道，我国40多万台计算机系统中，约有十分之一以上机器染有病毒，而且在沿海各省市传播的范围远比内地要广泛得多。

与此同时，许多高等院校、科研机构纷纷组织技术人员，研究反病毒软件。其中最具权威者当属中华人民共和国公安部的SCAN系列扫描病毒软件和KILL系列的清除病毒软件。

此后，计算机病毒的发展并未受到明显的抑制。“大麻”病毒、“黑色星期五”病毒先后侵入我国，造成的破坏也越来越大。

1991年，计算机病毒已经到了“家喻户晓，人人皆知”的地步。有的人对计算机会感染病毒这一问题感到困惑，更有甚者，则谈计算机病毒色变，从而对计算机也丧失了信心。为此，《计算机世界》月刊、《计算机信息报》、《计算机用户》、《科技日报》等报刊纷纷载文介绍计算机病毒的情况，同时也发表了大量的分析、解剖病毒的文章及防范病毒应采取的措施，从而使广大计算机用户对计算机病毒有了一定的认识，为以后采取措施预防病毒、诊治病毒打下了良好的基础。

1992年初，“黑色星期五”病毒、“米氏”病毒袭击了国内多个单位的计算机，损失较大的应属某民航飞机订票处的计算机网络。在某个星期五(又是13号)，病毒发作的当天，计算机中所存储的航班资料受到严重损害，造成一片混乱。

7、8月间，从国外传染的“FLIP”病毒又开始在兰州一些单位的计算机中传播，这是一种危害性很大、传播相当迅速的恶性病毒。在当时，国内还尚无相应的消毒软件可将其有效地清除。不久“FLIP”病毒又蔓延至其它地区。

12 月 3 日,《软件报》载文,题为"DIR-2 病毒首次骚扰上海",据此可以认为,DIR-2 病毒已在较大范围内传播。

上海《文汇报》报道:在上海又发现"乞讨"病毒,该种病毒危害大、传播快。

由此可见,在未来的日子里,计算机将不断面临"病毒"的挑战。因此,如何完善广谱防病毒技术,从根本上杜绝病毒的危害,已成为目前亟待解决的问题。

## 第二节　计算机反病毒技术的发展

计算机病毒在种类不断增加,破坏性不断增大的过程中,迅速向全世界蔓延,成为威胁计算机安全的主要"敌人"。这就促进了计算机安全领域中的一个重要分支——计算机病毒学的形成。

从 1987 年世界上第一例计算机病毒——Brain 出现开始,广大研究及应用计算机的人员就与计算机病毒的制造者展开了针锋相对的斗争。哪里有计算机病毒出现,哪里就有破译病毒、消除病毒的产品出现。

几年来,国内外很多专家、学者利用各种手段,宣传计算机反病毒技术的理论,介绍防毒、消毒的方法的很多专著也不断问世。

从国内外专家研究计算机反病毒技术成果看,目前对付计算机病毒的重要方法有两种:一种方法是利用工具软件消毒;另一种方法是利用微机防病毒卡防毒。

1. 利用扫描清除病毒软件消除病毒

几年来,国内外的计算机专家开发了很多优秀的清除计算机病毒软件,如国外的 CPAV 软件、SCAN 系列软件等,均可扫描和消除部分病毒。尤其是我国公安部不断推出的扫描和消毒软件,给计算机用户提供了很大的帮助。

但是,用消毒软件进行消毒是一种被动方式并带有滞后性。即计算机已经感染了病毒或者已经造成了损失再去消除病毒,就象人得了病再去找医生看病和打针吃药一样,总是处于被动状态。由于这些病毒检测和清除软件都是在具体地分析了某一种病毒后编制的,因而只能清除有限的已经被识破的病毒。而计算机病毒的种类极其繁多,各种新病毒又在不断地出现,原有的计算机病毒还有各种变种,均将导致消毒软件失效,甚至出现系统死机、文件丢失、数据被破坏等现象,那么可否象人讲卫生一样,采取以预防为主的方法呢?有关专家认为这是可行的。在这一思想的指导下,国内外产生了众多的软件、硬件相结合的防病毒产品。

2. 软、硬件相结合的抗病毒产品

(1) 防病毒卡。防病毒卡的基本工作原理是在充分地分析计算机病毒的机理、DOS 操作系统的内部结构以及微型计算机软、硬件资源和用户使用习惯的基础上研制的。在预防计算机病毒领域里,这类产品充分显示出了其优势,深受广大计算机用户的欢迎。

当然,防病毒卡也有其局限性,如存在假报警现象、不能消除文件型病毒等问题。防病毒卡要解决的问题主要是"预防"微型计算机被病毒感染,而消毒软件主要解决的问题则是当微型计算机被病毒感染后,如何"消除"病毒。将二者有机地结合,即可构成一个既能防范又能消除病毒的计算机安全系统。

(2) PC-CILLIN。微机病毒免疫锁 PC-CILLIN,其中包含硬件免疫锁和检测病毒软件两部分,检测病毒软件放在软盘上,所以它基本上还是一个软件系统。

总之,在短短的两三年内,众多的防毒、消毒产品已经出现,尽管这些产品还存在许多不

足，但可以相信，随着时间的推移，计算机反病毒技术必将不断地发展、不断地完善。

## 第三节　计算机病毒的基本概念

### 一、计算机病毒的定义

1. 定义

对计算机病毒的定义，至今尚未统一，较为普遍的定义是："病毒"是一种人为制造的、寄生于应用程序或系统的可执行部分，并且能够自我复制的程序。在宿主程序执行的某个阶段，它能够取得控制权。"病毒"程序不仅能够附着在系统启动区(BOOT 区)、操作系统的某些可执行文件以及设备驱动程序中，而且能够附着在任何应用程序上。因此，必须把计算机病毒和程序错误严格区分开来。程序错误被称之为"臭虫"(BUG)。根据程序错误的定义，程序错误不是蓄意制造的，而计算机病毒则是蓄意制造的。

2. 计算机病毒的特性

(1) 传染性。计算机病毒一旦驻留内存，就等待时机寻找适合其传染的磁介质或文件作为宿主，并将自己的全部代码复制在宿主中，从而达到感染之目的。

(2) 破坏性。计算机病毒均具有破坏性。破坏是其目的，感染是其手段。病毒程序一旦进入 DOS 系统，就会对系统造成不同程度的影响。轻者占用系统资源，影响运行速度，重者破坏系统文件和数据，甚至使系统瘫痪，给用户造成无可挽回的损失。

(3) 多样性。不同的病毒在发作时，呈现不同的症状。有的可直接观察，有的在表面上无任何异常现象，而在系统内部造成异常；有的病毒在不同条件下呈现出不同的症状。这些现象体现了病毒程序的多样性。

(4) 隐蔽性。为了不让用户发现计算机病毒，其编制者均巧妙地把病毒隐藏起来。在系统或文件被感染后，并不立即发作，也就是说，它有一定的"潜伏期"，在达到引发条件时才发作。

### 二、计算机病毒的分类

计算机病毒的分类方法有多种，可以按破坏程度分为良性病毒和恶性病毒；可以按攻击的操作系统分为攻击 DOS 操作系统的病毒和攻击 UNIX 操作系统的病毒等；也可以按攻击的机种分为攻击微型机的病毒，攻击小型机的病毒和攻击工作站的病毒。在本书中，采用按传染方式分类的方法，即分为引导型病毒、文件型病毒和混合型病毒。

1. 引导型病毒

磁盘经过格式化后，在引导扇区建立起操作系统的引导记录。对硬盘而言，有两个引导区，一个是主引导区，一个是 DOS 引导区或称逻辑引导区；对于软盘而言，只有一个引导区。但无论是对于硬盘还是对于软盘，引导区内所存储的内容都应建立正常的引导记录。引导型病毒主要是用病毒程序的全部或部分逻辑来取代正常的引导记录，而把正常的引导记录隐藏在磁盘的其它存储空间内，有的进行保护，有的不进行保护。由于磁盘的引导区是磁盘能够正常工作的先决条件，所以这种病毒在系统启动时，就获得了控制权，其传染的可能性很大、危害也极大。

2. 文件型病毒

文件型病毒是指那些专门感染 EXE 和 COM 等可执行文件的病毒。这种病毒与可执行文



此为试读，需要完整PDF请访问：www.ertongbook.com

件进行链接。一旦系统运行被感染的文件，计算机病毒即获得了控制权，并驻留内存监视系统的运行，寻找可传染的宿主程序以便进行传染。这类病毒也包括能传染 COMMAND.COM 文件的病毒。这些病毒当前广泛地存在，如 DIR-2 病毒、V2000 病毒、FLIP 病毒等等。

我们知道，计算机病毒几乎是无孔不入的，病毒程序的制造者的手段也越来越高明，不可能完全按上述模式来编制病毒程序。实际也是如此，有的病毒既感染引导区也感染可执行文件，有的病毒还重复感染可执行文件，其手段也是五花八门的，必须对具体问题进行具体分析，方可解决问题。

## 三、计算机病毒的基本弱点

为了有效地防治计算机病毒，首先必须分析计算机病毒的一些基本弱点。只有这样，方可有针对性地采取相应的措施。

(1) 计算机病毒是一段程序，而不是一个完整的程序。因此，其不能独立运行。若要运行则必须首先找到一个宿主(即病毒程序的载体)。

(2) 病毒程序的宿主必须是计算机系统的可执行部分。也就是说，它只能感染系统引导程序，或应用程序，而不能感染数据文件，表格信息，或系统的其它原始数据。

(3) 病毒的任何感染行为总是要改变宿主，或完全替代宿主的一部分代码，或修改一部分代码。如果病毒附加到一个宿主程序上，则将改变程序的开头、结尾或程序中间的某部分。如果病毒隐藏在磁盘的空扇区，则将改变这些扇区的标志；如果病毒将原引导记录转移到其它空的位置，也会改变系统。总之，病毒程序的任何感染操作均会留下一些痕迹。

(4) 如果病毒要存活、繁衍，其程序代码就必须能够执行。即病毒至少在初次感染后，使自己常驻内存，以持续潜伏，或者立即执行病毒的感染过程。

以上四点是病毒程序存活的基本共同点，也是其共同弱点。这些弱点可被反病毒工具充分地利用。

## 四、病毒程序的组成及工作过程

通过对计算机病毒程序的剖析，我们可以得出结论，计算机病毒主要由四部分组成：引导部分、选择时机部分、传染部分和表现部分。其工作过程如下：

1. 病毒程序的加载

在计算机系统中，“加载”即为将程序、数据等信息从磁盘介质读到内存，并置于操作系统管理之下的过程。

在操作系统把病毒程序的载体加载到内存时，通常要读入病毒程序的引导部分，并把系统的控制大权交给它。病毒程序的引导部分的主要任务是把整个病毒程序读入到内存并安装好。然后，再按照不同病毒的设计思想完成其他工作。病毒程序的加载过程，分以下三步：

(1) 驻留内存。病毒程序若要发挥其破坏作用，就必须要驻留内存。为此，就必须先开辟所用内存空间或覆盖系统占用的部分内存空间。

(2) 窃取控制权。在病毒程序驻留内存后，必须使其有关部分取代或扩充系统的原有功能，并窃取到系统控制权。此后，病毒程序依据其设计思想，隐蔽自己，等待时机，在条件成熟时，再进行传染和破坏。

(3) 恢复系统功能。病毒程序为了隐藏自己，驻留内存后还要恢复系统，使系统不会死机，而继续运行。只有这样，才能达到其等待时机成熟，进行感染和破坏的目的。

2. 病毒的触发

病毒程序加载到内存后，为了达到传染和破坏的目的，必须隐蔽自己，隐蔽得越深，也就越不容易被发现。病毒发作需要一定的条件，而这种条件也是各种各样的。计算机病毒中极少不进行任何条件判断而随意发作的。否则，这种病毒的隐蔽性就不强，也就很容易被用户识破。

一般情况下，有如下几类触发条件：

(1) 以时间、日期作为触发条件。这种触发条件与系统时钟有密切的关系。常表现为修改与时钟有关的中断和功能，如 INT 1AH、INT 1CH 等等。

(2) 以计数作为触发条件。当满足制造者的设定值时，病毒将发作。

当然，病毒程序的制造者还会设计出其它各种条件触发病毒的发作。但无论如何，所有的触发条件，均为在病毒程序驻留内存，并取得了系统控制权后方能使用。

3. 病毒的感染

计算机病毒加载到内存后。该病毒在内存中常驻并隐蔽自己，同时监视系统的运行。当发现攻击的目标后，在触发条件满足时，病毒便把自身的代码连接到目标，从而达到感染健康"机体"的目的。此后，病毒又利用磁盘读写中断 INT 13H，重新返回到软盘或硬盘，以便再感染其它系统。

4. 病毒的表现

计算机病毒的表现存在多样性。不同的病毒在发作时呈现不同的症状，有的可直接观察，有的则无表面现象，而在系统内部造成破坏；有的病毒在不同条件下呈现出不同的症状。如雨点病毒的表现是屏幕上的字符象雨点一样向下落；"1575"病毒发作时，则有一个小爬虫，把屏幕上显示的字符向右推移；而"Bloody"病毒的表现部分只是一句英文等等。

## 五、病毒的传染媒介

计算机病毒的传染媒介主要有两个：一个是磁介质，主要是软盘和硬盘；一个是计算机网络，对于微机而言，主要是局域网。由于我国目前计算机网络的开发利用还不普遍，因此二者比较，计算机病毒的传染媒介又以软盘、硬盘为主。

在微机系统中，由于硬盘容量大，读写速度快，所以用户读写文件主要是在硬盘上，因此硬盘就成了病毒的载体，也就成了再次传染病毒的媒介。

由于软盘具有携带方便及存储容量大等特点，因此其成为传染病毒的主要媒介。目前很多单位互相交流应用软件、汇总数据资料等均使用软盘。如果将带有病毒的软盘在其它系统中使用，病毒就传染给使用该盘的系统。

计算机网络是在网络操作系统的支持下，采用某些计算机技术，以实现资源共享的环境。其中包括中心机服务器、工作站、用户终端等设备。在共享资源时，需要网中的通信系统传输数据和文件，如果被传输的文件染有病毒，那么这些病毒就会通过局域网传播到四面八方，因此，计算机网络也是病毒传染的一个媒介。目前，计算机网络传染病毒的现象在国内还不多见。

## 六、如何判定系统是否被病毒感染

无论计算机病毒隐蔽得多么巧妙，它总会要露出一些马脚。在病毒发作时，总是会产生破坏作用，造成一些异常现象。因此，我们总是能够根据一些表面现象，再结合更深入的技术分析方法，正确地判定病毒的存在与否，并采取相应的防范措施。判定计算机系统是否染有病毒的方法主要有现象观察法和技术分析法：

1. 现象现察法

用户在使用机器过程中，如果发现下列一些现象，则可怀疑有病毒存在：

① 当运行某一程序时，运行速度明显变慢；

② 一些可执行文件的长度增加(文件的长度可用 DIR 命令列表看出)；

③ 用户使用的基本内存空间变小；

④ 用户运行的程序没有读、写磁盘的操作，但软盘或硬盘的指示灯却闪动；

⑤ 时常出现莫名其妙的死机现象；

⑥ 系统经常出现“写保护错”提示信息；

⑦ 在排除硬件故障的情况下，打印机无故不联机；

⑧ 显示屏上出现一些杂乱无章甚至不可辨识的显示内容；

⑨ 磁盘上出现了用户不能识别的文件；

⑩ 系统出现了文件分配表错的提示信息；

⑪ 命令处理文件 COMMAND.COM 被修改；

⑫ 硬盘不能引导系统；

⑬ 磁盘上文件的内容被修改；

⑭ 磁盘上的文件突然消失。

如果以上现象发生，很可能是计算机病毒所为，但还应该结合技术分析法或者用扫描软件进行进一步分析检查以作出最后的判定。

2. 技术分析法

采用技术分析法不仅取决于技术人员对系统的熟悉程度，还取决于技术人员对计算机病毒的熟悉程度。如果平时对计算机病毒剖析的较多，积累的经验较丰富，又能熟练地使用某些工具软件，如 PCTOOLS、DEBUG 等，结合出现的现象，便能很快地能确定系统是否染有病毒，并能够进一步确定病毒的类型和性质。

技术分析法的具体实施方法将在第三、四、五章节中详细介绍。

下面简要地介绍两种工具软件：DEBUG.COM 和实用软件包 PCTOOLS。

(1) DEBUG.COM。所有的 DOS 系统版本均提供 DEBUG.COM 文件，此程序的主要功能是：

① 可以监视、控制被调试程序，发现问题可以立即改正，即时运行，无须重新汇编程序，就可以证实修改的程序是否正确。使用该程序可节省时间，提高程序的调试效率。

② 可以直接读写磁盘各扇区的内容及数据，并且可以修改扇区的内容，这一点在排除磁盘故障时非常有用。

③ 可以直接修改、显示、运行内存中的程序或数据。

DEBUG 程序的主要命令如下：

.A ASSEMBLE(汇编)命令。用于把汇编语言语句直接加载到内存中，输入给汇编命令的所有数值，均为十六进制数。输入的汇编语句被汇编到内存中去。

.C COMPARE(比较)命令。用来比较内存块的内容。

.D DOMP(卸出)命令。用于显示内存中某一部分的内容，被显示的卸出内容有两部分。内容前一部分为十六进制部分，以十六进制形式显示每一个字节。后一部分为 ASCII 码部分，字节被显示为相应的 ASCII 码字符。

.E ENTER(输入)命令。用于替换从指定地址处开始的一个或多个字节的内容。以顺序

方式显示和修改字节的内容。

.F FILL(填充)命令。用于将特定数值填入到所指定范围的内存单元中。

.G GOTO(转移)命令。用于执行用户正在调试的程序。当程序执行到指定的地点(断点)时。停止执行,并显示寄存器、标志和下一条将执行的指令。

.L LOAD(装入)命令。用于将一个文件或一个完整的磁盘扇区装入内存。单个的装入命令所能装入的最大扇区数是十六进制的 80H。

.N NAME(命名)命令。

.R REGISTER(寄存器)命令。主要有三个功能:

① 显示一个寄存器的十六进制内容,可根据任选项改变这些内容;

② 显示所有寄存器的十六制内容,以及标志状态和下条将被执行的指令;

③ 显示 8 个双字母的字母标志状态,并根据任选项更改其中的任一个或全部。该命令显示并设置的寄存器名(Rigister Names)是:AX、BX、CX、DX、SP、BP、SI、DI、DS、ES、SS、CS、IP、PC、F。其中 IP 和 PC 均为指令指针。

.T Trace(跟踪)命令。用于追踪程序的执行。

.U Unassemble(反汇编)命令。用于对指令进行反汇编(将内存中的内容转换为汇编语言的语句),并显示反汇编后的汇编语句及其地址、十六进制内容。

.W 写(Write)命令。用于将调试结果写入磁盘。如果发生写盘错误,DEBUG 则显示出错信息。

以上是 DEBUG 用于检测病毒,清除病毒时常用的一些主要命令,它们都是非常有用的,必须熟练掌握。

(2) PCTOOLS 实用软件。PCTOOLS 实用软件是 Central Point Software 公司的产品,它包括了几乎所有的 DOS 系统命令,尤其是对于磁盘的操作,是其它软件无法相比的。因此也是一种有效的检查病毒的工具。

PCTOOLS 所提供的 F 命令和 E 命令对检测病毒十分有用。

F Find(查寻)命令的功能是在整个磁盘上查找某一字符串。它可以根据一种病毒的标识和病毒的特定字符进行查寻。

V/E View/Edit(查看/编辑文件)命令的功能是查看/编辑指定驱动器上磁盘的内容。

M Map(映象)命令的功能是显示整个磁盘被占用的情况。检查磁盘上被损坏的簇的位置及各文件在磁盘上的存储位置。某些坏扇区为病毒程序所制造。

I Info(系统信息显示)命令的功能是显示系统的资源信息,其中包括机器的型号、系统配置、内存分配等信息。

# 第二章　DOS 系统的组成及其弱点

到目前为止，我们已经了解到，计算机病毒程序大都是针对所要攻击的计算机及其配置的操作系统的某些弱点进行设计的，病毒发挥作用的前提条件是病毒程序利用系统功能驻留内存，并取得当前系统控制权。也就是说，为了防治 PC 系列微机病毒，必须要了解和掌握 DOS 系统的有关组成和主要功能。因此，对计算机病毒防治水平的高低，在很大程度上取决于技术人员对 DOS 系统结构功能理解的深浅程度。

由于本书的重点是针对 PC 系列微型计算机病毒的防治，所以我们将介绍 DOS 系统的组成结构、与病毒相关部分的功能及其使用方法，还将向读者指出 DOS 系统在安全性方面存在的弱点。

## 第一节　DOS 系统的层次结构及系统组成

PC 系列微型计算机上的操作系统有两个主要版本，即 IBM 公司的 PC-DOS 系统和 Microsoft 公司的 MS-DOS 系统，本文所涉及的 DOS 系统系指 PC-DOS 系统。

DOS 系统提供了较强的文件管理和系统资源管理功能。它采用层次模块结构，由一个引导记录和三个层次模块组成。

### 一、引导记录

DOS 系统在使用 FORMAT 命令格式化磁盘时，将引导记录作为一个记录驻留在软盘的 0 面 0 道 1 扇区上，在该扇区上还保存系统有关信息。对于硬盘，引导记录驻留在 DOS 区段的第一个柱面的第一个扇区上。系统在加电启动时，第一个读取的就是这一位置，并用其查找和加载 PCDOS 的两个隐含文件（IBMBIO. COM 和 IBMDOS. COM），并把控制权交给 IBMBIO. COM。该程序首先检查驱动器 A 中是否插入了系统盘，若插入了系统盘，则引导 DOS 进入内存，若插入的是非系统盘，将显示下述提示信息，并进入等待状态：

Non--system disk or disk error

Replace and strike any ker when ready

### 二、DOS 系统的模块结构

DOS 系统是由 3 个相互独立而又有联系的程序模块所组成。它们是：

① 命令处理模块，文件名为 COMMAND. COM；

② 文件管理和系统调用模块，文件名为 IBMDOS. COM；

③ 基本输入输出设备管理模块，文件名为 IBMBIO. COM。

1. 命令处理模块

该模块是整个 DOS 系统的最外层，直接同用户打交道，作为用户和操作系统之间的接口。其主要功能是解释并执行用户输入的 DOS 命令，命令处理模块由两部分组成：

① 在内存中的常驻部分 CCPR；

② 在内存中的暂驻部分 CCPT。

其常驻部分由 IBMDOS. COM 模块的初始化程序加载到内存的低端。此外，常驻部分还包括重新加载暂驻部分的加载程序。

暂驻部分 CCPT 是命令处理程序的本身，系统启动时被加载到内存的高端。其中包括全部命令解释程序、内部命令的处理程序、批命令文件处理程序和外部命令的加载程序等。该部分还产生系统提示符，如 A>。在系统屏幕上出现提示符后，等待用户从键盘上输入命令并解释执行之。因此，命令处理程序不仅负责内部命令的解释和处理，同时也负责外部命令的加载和执行。凡是用户从键盘上输入的命令，均要首先经过其的处理。之所以称其为暂驻部分，是因为其驻留的内存高端地址可以被应用程序所覆盖。一般情况下，应用程序加载执行时，CCPT 的内容将不再被使用。DOS 的这种处理方式有助于较大的应用程序加载执行。

常驻部分 CCPR 包括 DOS 本身专用的 3 个中断处理程序。即程序结束处理 INT 22H、INT 23H 和严重错误处理 INT 24H 以及重新加载暂驻部分的程序。这部分之所以必须常驻的原因在于：DOS 系统在接受控制时，要利用这 3 个专用中断程序，对用户使用 DOS 命令或执行应用程序时所遇到的正常结束、强制中断或严重错误的情况，及时作出相应的处理。还有，当某一应用程序退出时，需要调用暂驻部分时，应立即调入这部分程序中的重新加载程序，完成暂驻部分的再次加载，使屏幕上重新出现 DOS 提示符“>”，等待用户输入命令。

2. 文件管理和系统调用模块

此模块是操作系统的核心部分。为整个 DOS 的中间一层，其任务是提供一套独立于硬件的系统功能调用子程序，为系统软件和应用软件调用。

这一套子程序集中在 INT 21H 软中断服务程序中，在调用时，只需在 AH 寄存器中设置调用功能号，并将指定的入口参数放入其它有关寄存器，随后即可执行。

INT 21H 完成的主要功能是：

① 管理磁盘文件；

② 管理磁盘空间和其它系统功能调用；

③ 负责操作系统和外层模块的联系。

在系统启动开始时，控制转入到 IBMDOS 模块后，首先进行初始化工作。初始化所要完成的任务是：初始化内部工作表、文件分配表、为中断 20H-27H 填写中断向量表、为 COMMAND. COM 程序建立一个程序段前缀等。IBMDOS. COM 初始化的最后一项任务是为 IBMBIO. COM 提供加载地址，一旦 COMMAND. COM 被加载后，IBMBIO. COM 将控制权交给命令处理程序 COMMAND. COM。

3. 基本输入/输出设备管理模块

IBMBIO. COM 模块是 ROM 中的 BIOS 的低级接口模块。在系统启动过程中，负责确定内存容量、测定系统中设备的状态、初始化附加设备、复位磁盘系统、设置低序号的中断向量、解释 CONFIG. SYS 文件并设置系统环境，加载可安装的设备驱动程序，并给引入内存的 IBMDOS. COM 模块重新定位等。其中系统定义的驱动模块由一组 6 类共计 11 个设备驱动程序所组成。在加电过程中，由 DOS 引导模块将其加载至内存并常驻，故称之为常驻的设备驱动程序。

综上所述，若不包括引导程序，DOS 系统层次结构为：最外层是命令处理程序，即 COMMAND. COM 模块；第二层是功能调用和文件管理层，即 IBMDOS. COM 模块；第三层是基



此为试读，需要完整PDF请访问：www.ertongbook.com