国家经委培训认定教材

《现代电子技术》增刊

微型计算机病毒防治手册

（修订本）

卢安国　编著

前　言

几年来，计算机病毒从无到有，在众多计算机系统和网络系统上迅速传播，如同艾滋病一样，构成了对计算机系统的极大威胁。因此，有效地研究、分析计算机病毒的发展动态、构成原理及其侵入系统的可能路径，将有助于防范计算机病毒的蔓延和对计算机病毒的清除。

本书从剖析微型计算机操作系统的角度入手，分析阐述了系统的组成及其固有的弱点，指出了可能受计算机病毒侵扰的部分。这一切将为读者防治计算机病毒提供有利的帮助和支持。

为让读者对计算机病毒有所了解，并能有效地阻止计算机病毒的侵入，作者使用了详尽的程序实例来说明病毒的传染、发作及破坏的方式，并针对各类计算机病毒给出了如何解决病毒传染的具体方法及源程序。

本书可以成为读者了解计算机病毒的材料，也可以成为计算机用户防止计算机病毒的良师，它提供的系统分析内容，亦可以成为计算机程序工作人员提高计算机使用技术的益友。

本书在编写过程中得到了陕西省经济信息中心诸多领导和同志的支持和帮助，在此我们谨向他们表示感谢，同时我们谨向陕西电子编辑部的全体编辑同志表示感谢，感谢他们对本书出版所做的大量辛勤工作。

由于本书编写时间短促，加之作者水平有限，书中错误在所难免，有不妥之处，敬请广大读者批评指正。

作　者

1990 年 9 月于西安

微型计算机病毒防治实用手册

目　　录

第一章　概　述

1.1　计算机的发展概述

自 1946 年第一台电子计算机 ENIAC 问世以来，经过 40 多年的发展，计算机系统开发应用水平已成为衡量整个世界各国政治、经济及军事发达程度的重要标准之一。当前，计算机软硬件技术更以惊人的速度发展。尤其是进入八十年代，计算机技术越来越广泛的被应用于各行各业，如目前的工业控制、各种辅助设计和辅助制造、科学计算、航天技术、地质勘探等领域的技术发展，都与计算机技术发展水平有密切联系；在商业流通、文字处理、办公自动化及通讯网络等社会活动领域已较为普及。随着计算机硬件价格的不断下降和计算机系统性能价格比的不断上升，一个应用和普及电子计算机，特别是普及微型计算机的浪潮正以不可阻挡之势，冲击社会生活的各个领域。可以预见，不久的将来，在我国计算机将步入社会的基本组成单元"家庭"，成为人们日常生活工作中必不可少的有利工具。

四十多年来，电子计算机硬件制造技术经过"电子管"、"晶体管"、"小规模集成电路"、"大规模集成电路"等阶段正发展到现在的"超大规模集成电路"。今后计算机硬件制造技术将朝着新的集成规模、新的体系结构等方向持续发展。

我国大量使用的微型计算机属第四代计算机产品。微型机产生的标志是 1971 年 INTEL 公司采用 PMOS 工艺制造的 4 位微处理机 INTEL4004。它的出现也标志着电子计算机在各学科、各领域广泛应用的开始。随着半导体技术的发展，INTEL 公司在 1972 年推出了 8 位 CPU 的微处理机 8008，其后各大公司又相继推出了 8080、M6800、Z80 处理机芯片，并推出了与之配套的种类繁多的外部设备控制芯片。在七十年代中期，由这样一批设备及与之配套的强有力软件组成的计算机系统，以它优越的性能价格比，冲击着电子计算机市场，也冲击着社会生活的各方面，随着这类微型计算机的大量销售，给电子计算机的应用工作开辟了广阔的天地。

进入 70 年代后期，由于采用 H-MOS 高密度集成半导体技术，使得速度更快的微处理机得以出现和生产（8088、8086），也使配套的系统更加多样化、系列化。跨入 80 年代，微处理机生产技术完全走上了系列化高速发展的道路，继推出 8088、8086 不久，又相继推出 80286、80386 和 80486 等寻址范围更强、运算速度更高、性能更完善的 32 位等微处理机芯片。随着制造技术的不断发展和提高，计算机的性能价格比日益上升，价格迅速下落，构造由几十个、上百个乃至上千个微处理机组成的阵列式计算机系统已成为现实。由几台、几十台乃至上千台各类电子计算机组成的计算机广域网络系统现已成为一个令人瞩目的发展领域。

1.2 DOS 系统的发展过程

一个完整的微型计算机系统由硬件和软件两大部分组成，自从 8 位微型机出现以来，计算机工作人员就开始追求着尽善尽美的软件支持环境——操作系统。一个优秀的操作系统能给计算机带来广阔的应用前途。

操作系统的功能是统一管理计算机的各种硬件设备和软件资源，如中央处理器、存储器和输入／输出等硬件设备；以及各类有关系统软件和应用软件的运转。总之，操作系统是计算机系统的指挥中枢，一个配有操作系统的计算机，当用户在使用时，无需过问各类资源的分配使用状况，也没有必要编写各种输入／输出设备驱动程序。用户只需正确使用操作系统提供的各种命令和系统调用功能，指定的软件程序就会在操作系统的调度控制下自动而协调地运行。

目前广泛流行的微型机操作系统有 XENIX、CP／M、DOS 等。在我国使用最广的微型机操作系统是由 MICROSOFT 公司为 IBM 公司研制开发的 MS-DOS。MS-DOS 配置在 IBM 公司研制的 PC 系列微型机上及其兼容机。

MS-DOS 是 MICROSOFT 公司在 SEATTLE COMPUTER PRODUCTS 公司开发 86-DOS 的基础上，对其进行了大量修改之后，被 IBM 公司在 1981 年选定为其当年推出的 PC 系列机的基本操作系统，命名为 MS-DOS1.0。这一版本是 MS-DOS 的第一个版本。

自 MS-DOS 诞生至今，它不断得到改进和提高。这些改进版不但保证了向前兼容，而且扩充了许多创新的和增强的功能，由下表我们可以看到，MS-DOS 目前的最新版本，以它崭新的面貌——前后台、多任务、多用户和超过 32MB 的寻址能力，引人瞩目地出现在全世界。MS-DOS 的最新版本能够充分发挥各档次处理机的已有功能。

MS-DOS 的发展过程

推出日期	版本号	主 要 功 能
1981 年 10 月	DOS1.0	支持单面软盘，IBM 的第一个微机操作系统。
1982 年 10 月	DOS1.1	支持双面软盘，并可实现错误定位。
1983 年 3 月	DOS2.0	支持带硬盘的 PC／XT 机，并在改进原有功能的基础上，增加了树状结构目录管理功能。
1983 年 6 月	DOS2.1	对错误精确定位
1985 年	DOS2.25	附加扩展的字符集
1984 年 8 月	DOS3.0	支持以 80286 为 CPU 的微型机，提供为 1.2MB 软盘服务的功能。
1986 年 3 月	DOS3.2	支持新的磁介质类型（3.5 英寸的软盘）。
1986 年 12 月	DOS4.0	除保留和增强以前版本的功能外，增加了前后台管理功能，多任务运行管理功能，多用户网络支持功能等。

回顾DOS系统发展的几年时间，可以明显的感觉到其自身已发生了巨大的变化，特别是在DOS2.1版推出后，微型机的应用和普及进入了空前发展的阶段。展望未来，DOS系统依然有很强的生命力，尤其是近一时期DOS系统的发展，突破了存储空间对它发展的制约，使有效地址空间已扩展至32M之上。

DOS在我国也产生了很大的影响，由于原版DOS系统不支持汉字功能，故我国于1983年首次推出了支持IBM PC系统的CCDOS。该系统的产生，使得PC及其兼容机具备了汉字处理功能，从而能在我国得以广泛推广。CCDOS在短短七年的发展过程中，已由仅支持16点阵汉字输出的基本系统，逐步发展到可支持24点阵的汉字、32点阵汉字、48点阵汉字等高级字模输出的汉字处理系统。输入方法也从原始的拼音、笔形、区位等低速方法上升到包括五笔字型、大众码、钱码等近百种高速输入方案。已经生产了图形处理、语音处理、排版印刷、文档管理等汉字处理系统。使微型计算机在我国各行业，诸如事务处理、办公室自动化、教育、通信、控制和工程设计等许多领域都得到了充分的应用。然而，正当我国计算机产业及软件行业呈现一派欣欣向荣的景象时，计算机病毒也已悄悄的侵入我国计算机领域。计算机病毒的侵入，使我国一些计算机系统的正常工作，都不同程度的受到了破坏，严重阻碍了计算机特别是微型计算机应用工作的顺利开展。

1.3 计算机病毒

医学中的病毒是一类没有细胞结构但有遗传、复制等生命特征的微生物。病毒多数要用电子显微镜才能观察到。各种病毒具有不同的大小、结构和形态，只能在一定种类的活细胞中增殖。

计算机病毒是那些能够在计算机内部反复地自我繁殖和扩散，危及计算机系统正常工作，浪费系统资源，破坏存储数据的一类计算机程序。此类程序一般能够在适当时机获得系统控制权，从而发挥其各种功能。当前计算机病毒的定义有狭义的和广义的两种。狭义的定义是：计算机病毒程序可以象生物学中的病毒细胞一样，通过一定的媒介在计算机系统内部或系统之间进行自我繁殖和扩散。本书所介绍的病毒程序选用此定义。计算机病毒的广义定义是：凡驻留于计算机系统内部，对系统原有功能进行非正确修改的程序或过程。常见的广义计算机病毒有逻辑炸弹（LOGIC BOMB）、陷阱入口、特洛伊本马(TROJAN HORSE)等。

在医学上将研究病毒的形态构造、感染、增殖、遗传、变异、复制、分类、生态以及病毒病发生、发展规律的科学称为病毒学，病毒学的目的是控制、改造有害病毒，利用有益病毒。计算机病毒研究属计算机安全防护范畴，它主要研究计算机病毒的构成、标志、加载、引发、传染及计算机病毒的各种特征，其主要目地是控制、消除各种有害病毒。实质上看，计算机病毒是具有破坏功能的一类程序，从计算机安全防护角度看，这类破坏程序，也就是说计算机病毒的产生目的不外乎有以下几个主要原因：

(1) 显示"超群智力"

(2) 利用病毒进行报复

(3) 对付非法拷贝

(4) 敲诈勒索

(5) 恶作剧等

凡此种种，可以看出计算机病毒都是人为制造的。要消除病毒，一要加强对计算机技术人员思想品德教育，二要在技术上采取相应的技术措施。

总之，计算机病毒可以破坏计算机内的数据和程序来导致整个目标系统的异常运行，从而达到制造者的各种目地。所以说研究计算机病毒的基理，制造有效的防治工具，已是当前计算机领域刻不容缓的重要任务之一!

据《计算机信息报》90 年 1 期登载"一九八九年我国计算机界十件大事"中的第五条说：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[illegible]成为重大课题。由此可见计算机病毒在我国蔓延的范围之大!

1.4 计算机病毒的发展

自从计算机病毒在 1983 年 11 月 3 日被弗莱德·科恩于计算机安全的一次研讨会上提出，并通过实验证明以来，人们已经开始逐渐意识到计算机病毒再也不只是科学幻想中的一个主观意念，而是实际存在于现实之中的、具有强大破坏潜力的、能够客观存在的一种计算机程序实体，它的产生、存在与消灭均受人的主观意念支配，因此，我们说计算机病毒会随着人类社会历史科学技术的进步而不断改进自身，且不断的采用各式各样的途径和方法侵扰并破坏计算机系统。

1946 年以来的计算机硬件系统结构大多为冯·诺依曼（Von Neuman）体系，也就是说：一个计算机硬件系统由运算器、控制器、存贮器和输入输出设备等组成。计算机的软件系统由操作系统和应用系统两大部分组成。操作系统是为了提高计算机的利用率，方便用户使用计算机以及提高计算机的响应时间而配备的一种软件。它是用户与计算机之间的接口，各种应用系统皆在操作系统控制下运行。应用系统是为完成专门工作而设计的一组互相联系的例行程序和子程序。

无论是操作系统、应用系统还是计算机病毒，均是由计算机程序设计人员研制和编写的。

至今发现的计算机病毒大都是针对选定操作系统的某一弱点进行设计产生，由于人类在一定时期内不可能设计出绝对完美无缺的产品，所以也就不可能彻底排除因各种因素引发的不安全现象，也就不可能完全避免计算机病毒的侵扰和破坏。

我国最先大面积出现的计算机病毒是"小球"I * *"巴基斯坦"、"犹太人"、"维也纳"、"美国佬"等等。分析现有各类病毒，可以将它们划分为两大类，一类叫系统病毒，一类叫过程病毒。

系统病毒是指存在于操作系统程序内部，随系统启动过程进行加载并发生作用的计算机病毒。这类病毒程序一般都很短小，常用于降底或修改目标计算机系统的功能。流传较广的有圆点病毒、STONED 病毒、银行盗窃程序等。

过程病毒是指存在于系统程序之外某个可执行过程体内的病毒，这类病毒的加载依赖于所存在的过程，它的大小不受系统程序的制约，随编制者的需求而定，这种病毒一般具有较强的破坏性，它使计算机的各类软件资源遭到破坏，前面提到的逻辑炸弹、陷阱入口、特洛伊木马用近来在我国出现的 Type-B 病毒等都属计算机过程病毒。过程是指被操

作系统直接运行的程序文件；在DOS系统中的过程文件有EXE和COM文件两种。每一个过程文件本身叫做过程体。

随着操作系统安全性能的不断提高，其可以用来攻击的薄弱点将日益减少，那么系统病毒的作用也将越来越小；另一方面，由于过程病毒具有人为的随机性，使其具有较系统病毒较强的潜伏性，从而也使其具有更大的破坏性，故今后计算机病毒类型发展的趋势将会偏向过程病毒。

病毒程序发生作用的前提是病毒程序驻留内存并获得当前系统控制权。

计算机病毒驻留内存储器的主要方法有：

①减少DOS管理内存空间

②利用DOS系统间隙

③高段驻留

④命令覆盖

⑤过程加载

病毒程序可以选用五种手法之一驻留内存储器，并在驻留期间获取特定时刻对系统运行的控制权。

已发现的获权方法有修改操作系统子功能、修改中断入口、修改过程体执行指针等。

(1) 修改操作系统子功能

利用DOS常驻内存部分做文章，比如修改COMMAND文件中的TYPE命令，使得当选用该命令时进行传染和破坏。

(2) 修改中断入口

利用DOS中断入口地址，用病毒程序入口替换选定中断口地址，如修改中断13H口地址，当调用中断13H指令便进行传染和破坏。

(3) 修改过程体执行指针

将病毒程序装入可执行文件内，将文件执行指针指向病毒程序，待系统调用此文件执行时就进行传染和破坏等功能。

简言之，未来计算机病毒除了将会被不断增强它的破坏性、隐蔽性、传染性、多样性及其灵活的表现性之外，还将最终受制于人，也就是说计算机病毒象人类自身机体的各种疾病一样，不可能将其从整体上彻底清除，但可以在了解其基理之后，从局部对其进行预防、治疗和根除。

1.5 计算机病毒的危害

计算机病毒的危害形式主要有已下几种：

1. 减少存贮器的可用空间
2. 使用无效的指令串与正常运行程序争夺CPU时间
3. 破坏存贮器中的数据信息
4. 破坏相连网络中的各项资源
5. 构造系统死循环
6. 破坏系统文件

7. 破坏系统I/O功能

8. 彻底毁灭软件系统

除了解上述的8种危害形式之外，更应当注意到计算机病毒在政治、经济、军事等社会各领域内造成的种种巨大破坏。

如美国高科技史上的"灾难"就是指1988年11月2日晚，ARPANET网上的所有运行计算机突然停止正常工作，屏幕显示一片混乱，这个连接全美三百所大学、私人公司、研究中心、军事基地的网络系统，及与之相连的全国军用、民用及其它计算机网络都同时出现了相似的故障，在整个网络瘫痪近二十四小时后，经过全美数千名电子计算机专家的共同努力，才于11月3日清除了由康奈尔大学二十三岁的罗伯特·莫里斯(Robert Morris)编写的病毒程序。

经有关部门统计，仅在此24小时内，全美共有六千台联网的电子计算机遭受病毒侵害，造成的经济损失达数百万美元之多。

除此之外，还有以下种种事例:

美国的某家计算机公司，一位程序员被辞退，决定采取报复，当天他返回公司输入了一个病毒程序，五年后，此病毒发作造成了该公司整个作业系统的混乱。

美国Lehigh大学1987年11月18日发生lehigh病毒，使得此大学在两天内，包括软、硬盘，总共有600个以上媒介受到感染。

1988年11月3日病毒袭击了全美的internet网络系统，在短短的两天内便有6000台以上的联网计算机系统感染了此病毒。

日本发生了窃取用户密码口令的网络病毒，该病毒系通过电子邮件发送一些实用程序，驻留选用人员设备，然后获得所需信息，再利用这些信息进行各式各样的非法活动。

1987年以来，美国的一些"计算机入侵者"采用"特洛伊木马"方式，以个人计算机通讯为媒介，引诱人们使用，最后破坏使用者的软件和整个计算机系统。

1988年台湾发现首例计算机病毒，该病毒发生在台北举办的1988年国际围棋赛中，该病毒使得参加比赛的Macintosh计算机系统瘫痪，迫使比赛无法进行。

1988年夏季，苏联政府机构的计算机系统发现了三种入侵病毒，经过专家们三个多月的努力，基本排除了病毒的危害。

1988年以来，我国先后在全国统计局系统及大部分地区发现病毒。据不完全统计全国近40万台微型计算机，约有11%以上的计算机设备受到病毒不同程度的侵入和破坏。

1990年3月初，陕西某单位清除其部门内流行的"小球"和"大麻"两种病毒，共查出受感染硬盘17台，受感染软盘574张，分别为其已有硬盘的68%，占有软盘的14.6%，占常用软盘的80.2%。

通过对以上事例的了解，不难看出，计算机病毒侵入造成的危害是无法预料的。据《计算机世界报》载，仅1988年之中，全美国因计算机病毒的破坏造成直接经济损失达1亿美元之多。在我国大多数病毒尚未造成严重的后果。但随着计算机技术在社会各领域的普及和深入，今后难免不发生利用计算机系统或网络进行犯罪的严重事件，特别是对那些军事国防或要害部门的计算机的侵入，一但出现后果将不堪设想。假如，某国的核武器计算机控制系统受到病毒程序的破坏，发出不该发出的命令，产生的后果将是十分危险的。

目前，全世界共发现病毒有100多种，在我国也已发现50多种计算机病毒。至今报

导的所有病毒，均在微型机之间传染，且多在使用 DOS 的 IBMPC 和其兼容机之间流行。

目前计算机病毒在我国还未形成较大的破坏力，但是随着对外开放和国际交流的增多，再加上国内有这样或那样原因制造病毒的人，计算机安全方面的问题必定会不断增多。我们都应知道一个构思精巧的几十条指令的计算机病毒可以使一台微型计算机系统、一台大型机系统或一个区域网络乃至大型的广域网络系统陷于因丢失数据、程序破坏等原因而造成的瘫痪这一困境之中。都应当充分了解在当今计算机系统起重要支持作用的信息社会里计算机病毒的危害性。可以说计算机病毒已经对计算机的安全构成了严重的威协。因此，在计算机用户中间普及这方面的防治，检测知识，让大家重视计算机领域中这一公害问题，并能够防治和检测，是十分重要的。

当前应当面对现实，从切实的工作中去解决这一问题。应要给使用的计算机系统以洁净的环境，一般来讲，通过各种渠道得到的软件都应当进行计算机病毒检测，只有这样才能较好的阻止病毒的入侵，为了大家的计算机系统，也为了计算机在我国的应用，必须十分重视对计算机病毒的防治。我们认为在防治中最重要的是防，而不是治，也就是说：重要的是阻止计算机病毒的侵入，而不是发现计算机病毒后的排除!

由于网络尚未在我国广泛使用，本书的重点将放在对微型计算机系统计算机病毒的研究和防治上。

第二章　DOS 系统

通过前面的叙述，我们已经了解到：计算机病毒大都是针对选定计算机和其所配操作系统的某一弱点进行设计产生的，它发生作用的前提条件是病毒程序利用系统功能驻留内存并获得当前系统控制权。因此，为了防治计算机病毒，首先需要了解和掌握操作系统的有关组成和其主要功能。可以说：从技术上对病毒防治的好与坏取决于技术人员对计算机操作系统结构功能了解的深与浅。

由于本书重点针对微型计算机病毒进行研究和防治，故我们将选择介绍 DOS 系统的组成结构、有关部分功能及其一般使用方法。

DOS 的主要功能是：利用内存控制块链表（MCL）结构对内存进行分配管理；利用文件目录表（FDT）结构对磁盘文件进行管理；利用文件分配表（FAT）结构对磁盘存取分配进行管理；利用程序前缀控制块（PSP）结构对被加载的程序进行环境控制；使用文件控制块（FCB）对磁盘文件的读写操作进行管理；通过 BIOS 模块提供的硬件设备驱动程序，实现对计算机外部设备的管理与使用；用户还可根据需要，通过 Config.sys 文件对系统进行重新配置，也可以通过选用网络器件来支持网络环境等。

2.1　系统组成

微型计算机是由硬件系统和软件系统两大部分组成。

微型计算机的硬件系统主要包含有：

(1) 中央处理器（CPU）
(2) 内存贮器（ROM+RAM
(3) 控制器及时序电路
(4) 电源
(5) 扬声器
(6) 标准键盘
(7) 打印机并行接口适配器
(8) 显示器／打印机适配器
(9) 显示器
(10) 存贮器扩展部件
(11) 软盘驱动器、适配器
(12) 硬盘驱动器、适配器
(13) 异步通讯适配器
(14) 同步通讯适配器

其中内存 ROM 部分固化的是硬设备的各类支持模块，它包括：

一、自检程序

开机后首先运行自检程序，对硬设备配置及设备当前状况进行检测，如无故障进入正

常启动过程。

检测的主要内容有:

处理器测试

8237DMA 测试

基本 16K RAM 测试

8259 中断控制器测试

ROS 检查和测试

视频存储器测试

8253 定时器测试

键盘测试

扩展 I/O 测试

RAM 测试

ROM 测试

磁盘连接测试

在前六个自检测试中若出现故障，系统死机，后面五个测试如不成功系统显示错误代码，最后一个磁盘连接测试出错，则进入 ROM BASIC。若测试通过，进入自举程序。

二、自举装入程序(INT19H)

它的功能是将 DOS 系统的软盘或硬盘引导记录装入(引导记录的位置在磁盘的 0 面 0 道 1 扇区内)到内存的 0：7C00H 偏移处，并将控制权转到 0：7C00H 处。

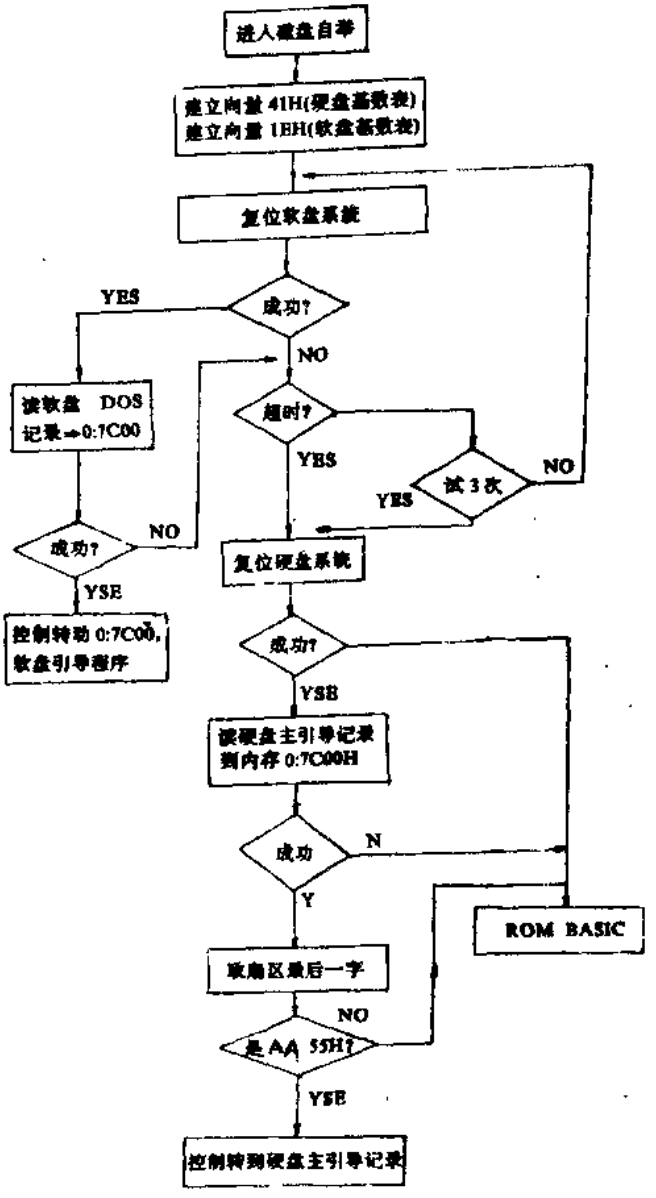
下面我们给出源程序和流程图，来具体说明它的作用。

执行程序及框图如下:

中断 19H 程序

```
C800: 01B0  B80000          MOV   AX, 0000                ; 置DS段为0
C800: 01B3  8ED8            MOV   DS, AX                  ;
C800: 01B5  B80000          MOV   AX, 0000                ; 置ES段为0
C800: 01B8  8EC0            MOV   ES, AX                  ;
C800: 01BA  FA              CLI                           ; 清中断
C800: 01BB  26              ES:                           ; 设置软磁盘参
C800: 01BC  C70604012902    MOV   WORD PTR [0104], 0229   ; 数指针到中断
C800: 01C2  26              ES:                           ; 41H口地址
C800: 01C3  8C0E0601        MOV   [0106], CS              ;
C800: 01C7  26              ES:                           ; 设置软磁盘参
C800: 01C8  C70678001E02    MOV   WORD PTR [0078], 021E   ; 数指针到中断
C800: 01CE  26              ES:                           ; 1EH口地址
C800: 01CF  28C0E7A00       MOV   [007A], CS              ;
C800: 01D3  FB              STI                           ; 置中断
C800: 01D4  B90300          MOV   CX, 0003                ; 置计数器为3
C800: 01D7  B200            MOV   DL, 00                  ; 选择软盘A
```

```
C800: 01D9  E82100          CALL  01FD                    ;软盘启动
C800: 01DC  7205            JB    01E3                    ;失败转移
C800: 01DE  EA007C0000      JMP   0000: 7C00              ;转交控制权
C800: 01E3  B0300           MOV   CX, 0003                ;置计数器为3
C800: 01E6  B280            MOV   DL, 80                  ;选择硬盘C
C800: 01E8  E8120           CALL  01FD                    ;硬盘启动
C800: 01EB  720E            JB    01FB                    ;跳转BASIC
C800: 01ED  26              ES:                           ;测试设备标志
C800: 01EE  813EFE7D55AA    CMP   WORD PTR [7DFE], AA55   ;
C800: 01F4  7505            JNZ   01FB                    ;跳转BASIC
C800: 01F6  EA007C0000      JMP   0000: 7C00              ;转交控制权
C800: 01FB  CD18            INT   18                      ;运行BASIC
C800: 01FD  B400            MOV   AH, 00                  ;磁盘启动过程
C800: 01FF  CD13            INT   13                      ;磁盘复位
C800: 0201  7213            JB    0216                    ;复位失败转
C800: 0203  B402            MOV   AH, 02                  ;将指定磁盘的
C800: 0205  B001            MOV   AL, 01                  ;第一物理扇区
C800: 0207  BB007C          MOV   BX, 7C00                ;读入内存的0
C800: 020A  51              PUSH  CX                      ;段7C00处
C800: 020B  B500            MOV   CH, 00                  ;并保存CX值
C800: 020D  B101            MOV   CL, 01                  ;
C800: 020F  B600            MOV   DH, 00                  ;
C800: 0211  CD13            INT   13                      ;
C800: 0213  59              POP   CX                      ;恢复CX值
C800: 0214  7307            JNB   021D                    ;读盘成功转
C800: 0216  80FC80          CMP   AH, 80                  ;比较超时标志
C800: 0219  E0E2            LOOPNZ01FD                    ;循环控制
C800: 021B  F9              STC                           ;清进位
C800: 021C  C3              RET                           ;返回
C800: 021D  C3              RET                           ;返回
C800: 021E  CF              IRET                          ;返回
```



三、I／O 支持模块:

a. 异步通讯 (RS-232C) (INT 14H)

b. 键盘 (INT 16H)

提供与键盘硬设备中断模块 (INT 9H) 接口

c. 磁盘 (INT 13H)

提供 DOS 系统对磁盘的支持途径

功能有：读、写、复位、检验、状态测试和格式化等。

d. 打印机 (INT 17H)

实现了对打印机的初始化和屏幕及文本输出等。

e. 显示器

(INT 10H)

提供了视频输出和终端接口等功能。作为PC系列提供的主要功能有：

- 显示方式设置
- 光标设置
- 字符显示
- 图形显示

四、系统配置分析：

a. 内存容量确定 (INT 12H)

b. 设备确定 (INT 11H)

五、日时钟 (INT 1AH)

该模块用于设置或读时钟当前值。

在以上五个模块中，除第一个自检模块之外，其余各模块均可以通过修改相关的中断口地址对其进行更换或功能修改，也就是说：除了自检模块，其它各模块都可能被病毒程序加以利用。

以上我们介绍了当前流行的IBM PC系列机的硬件系统组成及其固化在ROM中的部分设备支持模块，下面让我们谈谈PC系列机软件系统是如何较好的利用这些设备资源，组织整个计算机的正常工作，增强系统的处理能力和方便用户操作。

IBM公司为解决这一问题，选用了PC-DOS磁盘操作系统。该系统提供了较强的文件管理和系统资源管理功能。PC-DOS系统由以下四大部分组成。

1. 引导记录

DOS系统在做磁盘格式化时，作为特殊程序驻留在磁盘0面0道1扇区，在这里还保存有关系统信息。系统在加电启动时、第一个读取的就是这一位置，系统对它的读取不加任何校验，无论正确与否都将它装入内存并向它移交控制权。

一般称此位置为引导记录(BOOT)区。引导记录的作用是判别磁盘上有无IBMBIO.COM和IBMDOS.COM这两个系统加载文件，如果有则将它们依次装入内存；若没有则提示选定盘为非系统加载盘，在显示以下信息的同时进入等待状态。

Non-System disk or disk error

Replace and strike any key when ready

2. 基本输入／输出设备管理模块

在一个完善的系统中，不仅具有中断机构，还引入了通道和缓冲技术。虽然它们能显著提高CPU等的使用效率，但却给程序员直接使用设备带来了很大的困难和麻烦。为此，引入了设备管理模块，设备管理模块的基本任务是，按照用户的需求来控制I／O设备工作，完成用户希望的I／O操作，以减轻用户编制程序的负担。DOS操作系统的基本输入／输出管理模块是IBMBIO.COM，它提供了DOS需要的与硬件设备的低级接口。