适用IBM-PC及其兼容机

微机病毒预防和诊治

王路敬 编

中国科学院希望高级电脑技术公司

适用IBM-PC及其兼容机

微机病毒预防和诊治

王 路 敬 编

中国科学院希望高级电脑技术公司

一九九一年四月

★北京市新闻出版局

准印证号：3194-90194

★订购单位：北京8721信箱资料部

★电　　话：2562329

★电　　传：01-2561057

★地　　址：海淀影剧院北侧

★乘　　车：320、332、302路至海淀黄庄下车

★办公地点：希望公司大楼101房间

★邮　　码：100080

编 者 的 话

目前，计算机病毒正日益严重地侵害着计算机这一科学领域。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相继发现了计算机病毒的干扰，而且正不断蔓延，种类不断增加，就是同一种病毒的变种也在增多。据有关资料报到，到目前为止，世界上共有240种病毒在流行。

“计算机病毒大量流入我国，引起各方忧虑和重视，对计算机除毒防范的研究已成为重大课题”被选为一九八九年我国计机算界十件大事之一。自一九八九年上半年在我国部分地区发现圆点病毒以来，到现在据统计已有近70多种病毒在肆疟，流行较广的病毒也近20种。其中90%是攻击微型计算机的。随着微型计算机的普及和推广应用，DOS和应用软件的广泛交流，非法复制软盘的现象日益严重，加之机器的管理缺乏严格的制度，来自多方面的消息证实，计算机病毒尤其微型计算机病毒还在继续传播，其趋势有增无减。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。若任其发展、蔓延，其后果不堪设想。我们必须看到其危险性，当然也不能走到另一个极端看待计算机病毒。计算机病毒对计算机系统虽有一定的破坏性，但并不等于计算机病毒就是一种非常可怕的东西，以至“谈毒色变”，更不应有“草木皆兵”“人人自危”的错误认识。我们对待计算机病毒的态度还应遵从“在战略上藐视它，在战术上重视它”这一原则。

本书结合从一九九〇年以来，编者在中国农科院计算中心连续举办多期“微机使用技术与应用”培训班上有关“计算机病毒预防与清毒”授课的讲稿以及学员在学习这部分课程和我们检测消除计算机病毒操作中所遇到的问题，参阅了“计算机世界”报，“计算机世界”月刊、“中国计算机报”等以及有关计算机病毒的文献，结合我们检测消除各种病毒的实践，经过归纳整理编写了“微型计算机病毒预防与诊治”一书。

本书的突出特点是实用性强。因为受计算机病毒困扰的用户急需了解解除病毒威胁，以及如何免除病毒再攻击的实用技术，所以从内容上尽量避免过多的理论论述，而着眼于要解决的实际问题、能力和操作方法。全书共分四章：第一章计算机病毒概述。在明确什么是计算机病毒的基础上，进一步介绍有关计算机病毒产生、分类、特征、寄生方式，一般工作机理，传染途径及方式，表现形式等，最后落实到微型计算机病毒常用的预防、判别方法和处理的一般操作步骤。第二章检测和诊治微型计算机病毒的准备。该章内容包括：(1) 微机磁盘操作系统的基本知识。(2) 检测和清除病毒的必备工具软件的使用。第三章微型计算机常见典型病毒分析。该章着重对圆点病毒，大麻病毒，巴基斯坦病毒，黑色星期五病毒等流行最广的病毒进行了分析。第四章常用检测和消毒软件。第五章IBM-PC及其兼容机流行的129种病毒简介。

由于时间紧迫和实践的局限性以及水平所限，书中难免有一些错误和不妥之处，恳请读者不吝赐教，批评指正。

编者

1991.春节

目　录

第一章　计算机病毒概述

1.1　计算机病毒的概念

1.1.1　什么是计算机病毒

有关计算机病毒，可以从不同角度给出定义。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，另一种是计算机病毒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。还有的定义计算机病毒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，它会自身复制并传播，使计算机的资源受到不同程度的破坏等等。这些说法都是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相同的一面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、计算机病毒的根本特征就是潜伏性和破坏性。即计算机病毒可能在你不知不觉中侵入你的计算机系统潜伏起来，过一段时间再发作，进行破坏。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，达到某种条件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制者自己也无法控制。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。

当计算机正以日新月异的发展速度广泛地深入到社会生活的各个方面的时候，计算机病毒的出现不仅仅是计算机工作者，而且包括政府部门、法律部门、各级领导乃至普通工作人员提出了一个严肃的课题：在计算机功能日益增强的同时，如果计算机设计者，软件开发者，系统管理者之间不能有效地协作，不能增强计算机系统的安全性，那么计算机的使用会受到许多限制，这是一个很值得人们认真研究，认真对付的问题。

1.1.2 计算机病毒的产生

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之门。

（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机普及应用热潮，微机数量年年猛增，应用领域越来越广，其他国家也基本如此。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得越来越清楚，不同的目的可以截然不同的选择。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。

计算机病毒的来源：一是搞计算机的人员和业余爱好者的恶作剧寻开心创造出的病毒，企图显示各非凡的本领。例如象圆点一类的良性病毒。

二是软件公司及用户为保护自己的软件不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。典型的例子是巴基斯坦病毒的产生。巴基斯坦电脑病毒最早发源于阿姆扎德、法户普埃尔维和巴斯特、法卢普、埃尔维兄弟俩在拉奎尔电脑计算机服务部所卖的非法复制的磁盘。几年来他们的生意一直非常兴隆，他们拷贝美国最好的软件，例如WordStar字处理软件和Lotus1-2-3，他们以不到原始软件百分之一的价格出售。阿姆扎德毕业于旁遮普大学，是个优秀的软件设计者，具有讽刺意义的是，在他为顾客设计的程序被非法拷贝后，他设计了巴基斯坦电脑病毒作为对非法拷贝的警告和报复。当阿姆扎德和巴斯特自己也成为非法拷贝者时，他们便玩了个邪恶的游戏，他们把卖给外国旅游者尤其是美国人的非法拷贝磁盘涂上病毒，于是，巴基斯坦电脑病毒被带到了许多国家，尤其是美国。当这些购买者把他们以极便宜的价格从埃尔维兄弟那儿购买的专卖软件的假、冒复制品交付运行时，他们的系统上便被染上了病毒，这些最初购买感染了病毒的磁盘的人继续为他们的朋友拷贝非法复制的程序，从而引起了一连串的病毒感染，不久巴基斯坦病毒就通过磁盘交换传遍了整个世界。

三是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13号星期五病毒，就是雇员在工作中受挫或被辞退时恶意制造的，它针对性强，破坏性大，产生于内部，防不胜防。

四是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。

综上所述，可见计算机病毒都是人为制造的，有意或无意的进行传播。认识计算机病毒，了解计算机病毒，预防计算机病毒，检测计算机病毒，有了计算机病毒进行消除等等，都需要对计算病毒的产生有所了解，澄清一些模糊的认识。

1.1.3 计算机病毒的分类

计算机病毒可以从不同的角度分度。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。定时病毒仅在某一待定时间才发作，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。这种用它自己的程序意图加入或取代部分操作系统进行工作，这种病毒具有很强的破坏力，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，对源程序不做修改，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机及其兼容机的。

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分法。例如按破坏程度可分为以下几类：

无害型——这类病毒在系统中不产生明显的破坏作用。它们存在于不引人注目的区域，对软盘和其它与系统接触的媒体进行传染。这类病毒在传染时不腐蚀数据或程序，不干扰正常的系统处理。这类病毒造成破坏是偶然的，通常是由于病毒内的程序设计错误而引起的。

幽默型——这类病毒常显示幽默信息或图象，或导致一些恼火的事情发生，但不损失或修改数据。它们被其设计者视为玩笑而不是用来造成持久危害的。这类病毒最多使系统临时停车或短暂干扰屏幕处理，而恢复这一切一般都很简单。

更改型——这类病毒更改系统的数据。它们把数据文件置于数据库系统和其它应用程序中，修改数字信息，如把8改为3，给数字添上一个0或把小数点右移或左移。这类病毒还能改变两个数据元中的信息或把某一数据元中的数字顺序颠倒过来。它们能消除一个数字，以上这些以及与此类似的数据更改活动通常是随机的和偶发的，所以系统的用户可能几个月或几年都不知道病毒的存在。这类病毒具有最大的潜在破坏性，因为它们所进行的更改难以被发觉，然而累积起来却具有破坏性。

灾难型——这类病毒突然激活，立刻造成大范围的破坏。它们消除重要的系统文件，搅乱关键码信息表，有时甚至将硬盘和其它附属装置中的所有信息清洗掉。

若按存储的方式分：可分引导扇区及分区表病毒。该类病毒专门寄生在引导扇区和分区表，而将操作系统正常的引导扇区和分区表替换到磁盘另外的扇区中。寄在COMMAND.COM文件的病毒，该类病毒通过修改COMMAND.COM文件而附加到该类文件上，使其文件的长度加大。驻留于内存的病毒，该类病毒通过驻留内存感染.COM和.EXE文件；不驻留内存的病毒，此类病毒虽感染.COM文件，但不驻留内存。因此同一种病毒可以从不同的角度进行分类。

了解病毒的类型后，可以针对不同类型病毒的特征，表现症状等等现象，对缩小检测的范围，制定消除病毒方案，堵塞病毒传播的渠道，都是大有好处的。例如圆点病毒它是操作系统型的病毒，预防这种病毒的传染，对操作系统盘要严加管理，用无毒盘启动系统，固定从硬盘启动系统等等都是较好的方法。一旦感染了这种病毒，消除、免疫都从引导扇区着眼考虑问题，即可把问题缩小到一个较小的范围里。

1.1.4 计算机病毒的一般特性

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。表现为占用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、才表现。

(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。

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，例如感染黑色星期五病毒的.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，就必须不时调用驻留内存的消毒代码，作为长城系列或IBM-PC系列微机及其兼容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，这种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。

下面图1.1，1.2，1.3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：

```
-d 0000:0000
0000:0000   43 31 E3 00 3F 01 70 00 -00 00 00 00 3F 01 70 00
0000:0010   3F 01 70 00 54 FF 00 F0 -EC FE 00 F0 EC FE 00 F0
0000:0020   A5 FE 00 F0 87 E9 00 F0 -DD E6 00 F0 DD E6 00 F0
0000:0030   DD E6 00 F0 B7 01 00 C8 -57 EF 00 F0 3F 01 70 00
0000:0040   65 F0 00 F0 4D F8 00 F0 -41 F8 00 F0 C8 01 00 C8
0000:0050   39 E7 00 F0 59 F8 00 F0 -2E E8 00 F0 D2 FF 00 F0
0000:0060   00 00 00 F0 47 01 00 C8 -6E FE 00 F0 38 01 70 00
0000:0070   53 FF 00 F0 D9 45 00 F0 -22 05 00 00 00 00 00 00
-d
0000:0080   FB 0B E3 00 80 01 42 05 -42 02 0E 06 70 02 0E 06
0000:0090   E2 04 42 05 C4 14 E3 00 -21 15 E3 00 E7 27 E3 00
0000:00A0   07 0C E3 00 26 01 70 00 -00 00 00 00 00 00 00 00
```

```
0000: 00B0   00 00 0C 00 00 00 00 00—6D 03 42 05 00 00 00 00
0000: 00C0   EA 08 00 E3 00 00 00 00—00 00 00 00 00 00 00 00
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1.1 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：

```
-0000: 0000
0000: 0000   43 31 E3 00 3F 01 70 00—00 00 00 00 3F 01 70 00
0000: 0010   3F 01 70 00 54 FF 00 F0—EC FE 00 F0 EC FE 00 F0
0000: 0020   A5 FE 00 F0 87 F9 00 F0—DD E6 00 F0 DD E6 00 F0
0000: 0030   DD E6 00 F0 B7 01 00 C8—57 EF 00 F0 3F 01 70 00
0000: 0040   65 F0 00 F0 4D F8 00 F0—41 F8 00 F0 D0 7C 80 77
0000: 0050   39 E7 00 F0 59 F8 00 F0—2E E8 00 F0 D2 EF 00 F0
0000: 0060   00 00 00 F0 47 01 00 C8—6E FE 00 F0 38 01 70 00
0000: 0070   53 FF 00 F0 D9 45 00 F0—22 05 00 00 00 00 00 00
-d
0000: 0080   FB 0B E3 00 80 01 60 05—42 02 38 0E 70 02 38 0E
0000: 0090   E2 04 60 05 D4 14 E3 00—21 15 E3 00 E7 27 E3 00
0000: 00A0   07 0C E3 00 26 01 70 00—00 00 00 00 00 00 00 00
0000: 00B0   00 00 00 00 00 00 00 00—6D 03 60 05 00 00 00 00
0000: 00C0   EA 08 0C E3 00 00 00 00—00 00 00 00 00 00 00 00
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
0000: 0010   47 01 70 00 54 FF 00 F0—EC FE 00 F0 EC FE 00 F0
0000: 0020   A5 FE 00 F0 87 E9 00 F0—DD E6 00 F0 DD E6 00 F0
0000: 0030   DD E6 00 F0 B7 01 00 C8—57 EF 00 F0 47 01 70 00
0000: 0040   65 F0 00 F0 4D F8 00 F0—41 F8 00 F0 15 00 40 7F
0000: 0050   39 E7 00 F0 59 F8 00 F0—2E E8 00 F0 D2 EF 00 F0
0000: 0060   00 00 00 F6 47 01 00 C8—6E FE 00 F0 40 01 70 00
0000: 0070   53 FF 00 F0 D9 45 00 F0—22 05 00 00 00 00 00 00
-d
0000: 0080   07 0B EB 00 80 01 60 05—42 02 4D 0E 70 02 4D 0E
0000: 0090   E2 04 60 05 E0 13 EB 00—2E 14 FB 00 13 27 EB 00
0000: 00A0   13 0B EB 00 2E 01 70 00—00 00 00 00 00 00 00 00
0000: 00B0   00 00 00 00 00 00 00 00—6D 03 60 05 00 00 00 00
0000: 00C0   EA 14 0B EB 00 00 00 00—00 00 00 00 00 00 00 00
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 感染大麻病毒后系统中断向量表

注：上述中断向量表是在长城0520CH机，PC-DOS2.10，512K内存系统下获得的。

1.1.5 计算机病毒的寄生方式

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的文件形式存在，它必须是以现有的硬软件资源而存在的。

微机系统在目前来说永久性存贮设备即外存贮器主要是磁盘。磁盘包括硬盘和软盘。从存贮容量角度来讲，硬盘容量是一般软盘的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。微机系统所使用的文件存放于磁盘之中，所以微机的病毒是以磁盘为主要载体的。

计算机病毒的寄生方式主要有：

（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会被激活，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。

（4）寄生在文件分配表中。

从计算机病毒寄生在磁盘上不同的区域中来看，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。从目前入侵到我国的计算机病毒所造成的破坏情况，主要表现在：

（1）破坏操作系统正常的引导扇区和硬盘的主引导扇区，使得操作系统不能正常启动或不能启动。

（2）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CLIB24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CLIB24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。

（3）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。例如犹太人病毒于1987年某月13日又为星期五，运行.COM或.EXE文件将会删除该文件。4月15日北京晚报报导我国有些地方的计算机在4月13日激发感染上的“十三号星期五”病毒，计算机工作效率或程序受到不同程序的破坏。

（4）修改或破坏文件中的数据。

（5）改变磁盘分配，造成数据写入错误。

（6）影响内存常驻程序的正常执行。

（7）在磁盘上产生坏的扇区，使磁盘可用空间减小。

（8）更改或重写磁盘的卷标。

（9）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。

（10）对整个磁盘或磁盘的特定磁道或扇区进行格式化。

（11）在系统中产生新文件。

（12）改变系统的正常运行过程。

1.1.6 计算机病毒的一般工作过程

计算机病毒毒的完整工作过程包括以下几个环节：

（1）传染源

病毒总是依附于某些存贮介质，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贮介质，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

所谓病毒触发即计算机病毒一旦被激活，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。也可能是系统的一次通讯等等。

（5）病毒表现

表现是计算机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的数据。可以这样说，凡是软件技术能够触及到的地方，都在其表现范围内。

（6）传染

计算机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。计算机病毒传染的过程如图1.4所示。

从图1.4中我们可以看到，在磁盘被插入时，在受感染的磁盘上的病毒程序进入到计算机系统的存储器中。然后，病毒进行自身复制，存取在系统固定存储上的所有程序。如果这些程序提供了病毒能生存的环境，病毒将附着在上面。

1.1.7 计算机病毒传染途径及其方式

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，通过修改其他程序，把自身

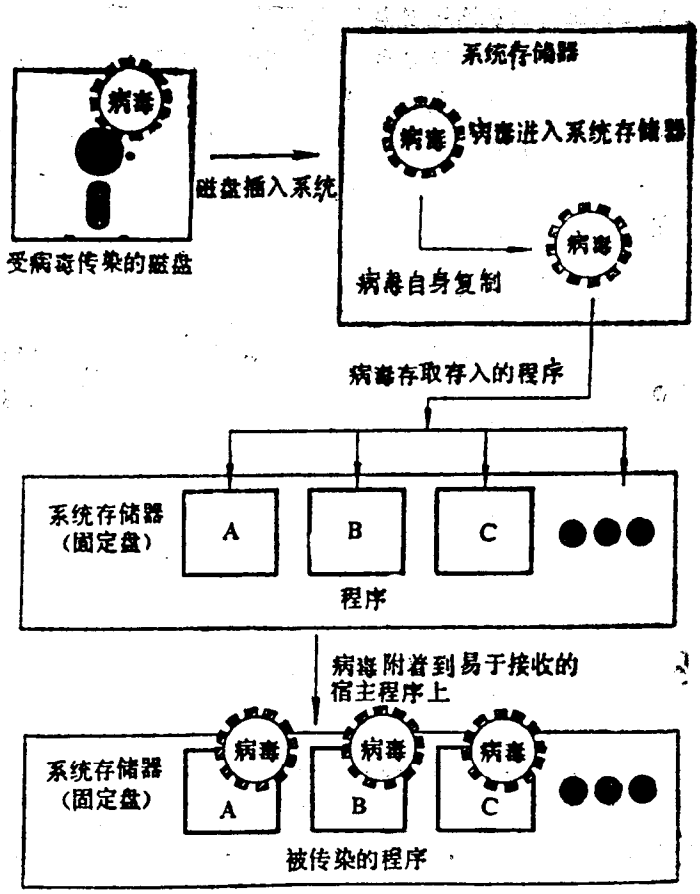

图1.4 计算机病毒传染过程

计算机病毒之所之为病毒是因为其具有传染性的本质，通过修改其他程序，把自身复制品包括在内，传染其他程序，传染渠道通常是以下几种.

(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。在网络中只要有一张受感染的磁盘，病毒就可以通过网络迅速扩散，一旦将受感染的盘插入工作站中，复制便开始了。寻

找可感染的网络文件，扩散到其他工作站上，一存取共享文件，就会受到感染。计算机病毒在网络中感染的过程如图1.5所示。

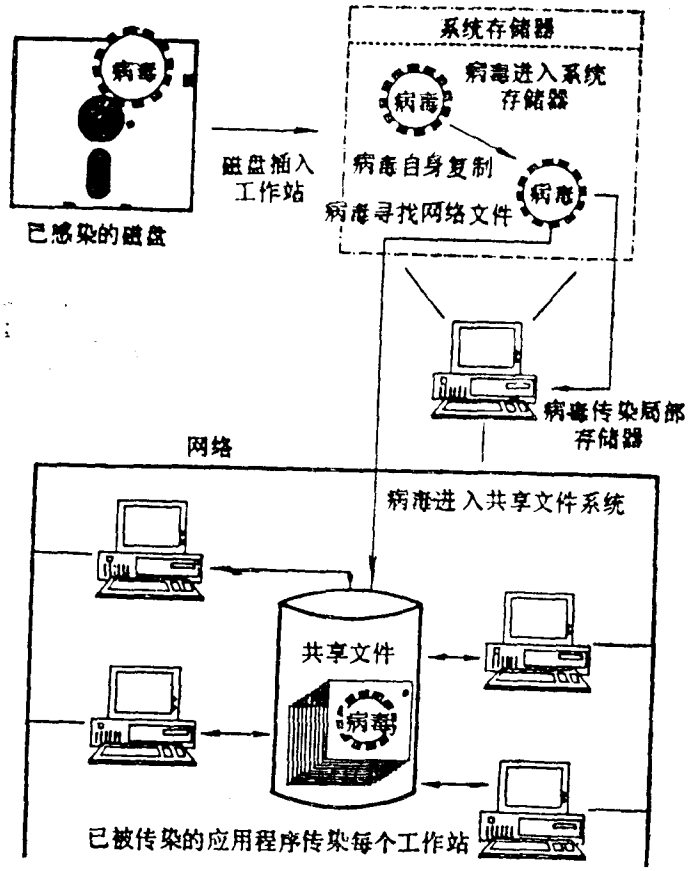

图1.5 网络感染过程

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到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。系统的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；当条件满足进行传染将病毒写入磁盘系统。

但是不同种类的计算机病毒其传染的方式不同。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为操作系统的某些文件，不是则不传染；若是，进一步判断是否满足条件，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512字节之中。这种病毒是在系统启动的时候进入内存贮器中，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，时刻监视插入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，病毒就将其传输到该软盘的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毒传染的主要途径。

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。

从目前蔓延传播的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的标识不一致，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。例如石头病毒可以感染硬盘，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。

计算机病毒传染的过程在PC系列机上是这样进行的：

在系统运行时，病毒通过病毒载体即系统的外存贮器进入系统的内存贮器，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。而病毒利用系统的INT 13H读写磁盘的中断又将其写入系统的外存贮器软盘或硬盘，再感染其他系统。

而操作系统类型的病毒，例如圆点、大麻、巴基斯坦等与感染可执行文件类型的病毒其感染的方式不同。

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，进行如下的操作：

（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。

操作系统类型的病毒的感染是在启动过程中进行的。正常PC-DOS的启动过程是：

（1）加电开机后进行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；