第一章　计算机病毒概述

伴随着计算机技术的发展和普及，计算机流行病菌像生物病毒侵袭人类社会一样侵袭和威胁着计算机系统，这就是计算机病毒。当人们警觉到某种病毒在局围传播，不要多久，这一地区的大多数兼容计算机就会检查到同一种病毒，大量的存储介质被感染，数据被破坏，甚至计算机系统被摧毁等等。计算机病毒悄悄地、快速地传染开，使许多计算机工作人员感到吃惊和困惑。

第一节　什么是计算机病毒

由于计算机病毒发展早期的隐蔽性、传染的快速性和种类的多样性，往往使人们还来不及给计算机病毒以十分确切的定义。在人们逐渐了解和认识计算机病毒的过程中，许多计算机工作者才从不同的角度给出了计算机病毒的定义，从而帮助人们研究和防治计算机病毒。

我们认为，计算机病毒是一种侵入计算机内部、可以自我繁殖、传播、具有破坏性的计算机程序。

迄今为止，出现在计算机领域中的计算机病毒都是人为编制的一段程序编码。它被程序设计人员或操作人员有意无意地植入某个正常程序或计算机操作系统中，然后，该病毒就依照设计者给定的指令，不断地自我复制，进行繁殖。有的病毒又以磁盘、磁带和网络作为媒介进行传播和扩散，“感染”其它的程序或系统，在一定时期或地域内广泛地流行。计算机病毒可以通过不同的途径潜伏、寄生在计算机的系统或程序中，在一定的条件下，依照其程序指令，干扰计算机的正常工作、吞食计算机的资源、甚至破坏数据或文件，严重时使计算机系统完全瘫痪。

当前，计算机病毒种类迅速增加。不同的病毒有其不同的特征。小的病毒仅有20条指令，不超过56个字节；而大的病毒可由几万条指令组成；有的病毒一进入计算机系统就大量繁殖、侵占资源，肆意破坏；但有的病毒，却长期潜伏，仅当某一条件达到时，才突然发作。这些病毒的不同特征和破坏方式是与病毒制造者的主观目的紧密相连的。但是，有些病毒的传播范围和破坏程度却是病毒制造者没有预料到和无法控制的。尤其是计算机网络系统，由于病毒借助网络传播，其传播趋势是难以预料的。在几分钟内，网络中所有运行的计算机均可能被感染。

计算机病毒是计算机技术和以计算机信息处理为中心的社会信息化进程发展到一定阶段的必然产物。

由于计算机应用，尤其是微型计算机应用的迅猛发展，计算机与人类社会各种活动密切相关。计算机已深入到国民经济各部门，商业、企业的各个角落，乃至进入家庭。微机的广泛应用和信息的自动化处理，给计算机病毒的流行，提供了适宜的环境。

由于计算机在政治，经济，军事方面所起的作用日益增大，重要性逐日提高，因而利用计

算机犯罪的引诱力也就日见增加。计算机犯罪所使用的高技术，具有可瞬时完成及可远距离控制的特点，因而不易取证，风险小而效果却不可估量。计算机病毒是计算机犯罪的一种衍生形式。计算机病毒全球性的蔓延，已经给计算机系统及其数据的安全造成了重大的损害。

随着最近十几年微型计算机的普及，针对微型计算机的病毒也借机迅速地泛滥。这是微机系统本身脆弱性的暴露和信息共享机制安全管理上的缺陷所促成的。微型计算机操作系统简单明了，软、硬件透明度好，安全措施薄弱，能够透彻了解微机内部结构的人数日益增多。因而，一部分人就利用了它本身的薄弱环节和易于攻击之处，编制或修改某些计算机病毒，并使它流传，从而使计算机病毒日益泛滥。计算机病毒问题已超出了计算机技术领域，成为一个严重的社会安全和社会道德问题。

第二节　计算机病毒的产生

计算机病毒这一名词是由科普小说首先提出的。

1975 年美国科普小说作家约翰·布鲁勒尔(John Brunner)出版了一本名为："震荡波骑士"的幻想小说。该书以计算机蠕虫为主，描述了在信息社会中代表正义和邪恶的两种势力之间利用计算机展开的一场斗争。这个故事使计算机第一次成为幻想中相互攻击的重要工具。该书幻想新奇，描写生动，获得了广大读者的喜爱。继之，在 1977 年，另一个美国科普作家托马斯·杰·雷恩(Thomas·J·Ryan)的著作"P-I 的青春"更是轰动一时，在该书中作者设想出现了一种神秘的、能够自我复制的计算机程序，并称之为"计算机病毒"。该病毒在计算机之间流传，一时感染了 7000 多台计算机的操作系统，引起了极大的混乱。

科幻小说的出现是有一定的历史背景的。在那以前，许多人已发现了计算机程序可以自我复制和变异这一机理。

首先，计算机的创始人，冯·诺依曼(John Von Neumann)在世界上第一台计算机诞生后仅仅 4 年，于 1949 年就发表了"复杂自动机器的理论和结构"的论文，指出计算机程序可以在内存中进行复制即"程序复制机理"的理论。

在此之后，许多计算机人员在自己的研究工作或游戏中发展和应用了程序或软件自我复制的理论。1959 年美国 ATST Bell 实验室的 3 个年轻人，道格拉斯·麦克尔罗伊(Douglas Mcilroy)，维克特·维索特斯基(Vietor Vysottsky)及罗伯特·莫里斯(Robert Morris)利用公司机器中的核心存储器中的数据和程序来做游戏。他们通过改变磁心存储器中的代码来消毁其它的程序。这种游戏被他们称做"磁心大战"(Core war)。为此，他们设计出有自我复制能力、并在探测到敌方程序运行时能消毁其程序的程序。这个程序经过不断地改进，其威力逐渐增大，甚至发展到影响计算机 Xerox 530 机的正常运行。由于意识到这种能自我复制程序的潜在危险，磁心战被停止了，并在有关人员的默契中保守了这个秘密。直到若干年后，凯·汤普逊(Ken Thompson)在给计算机协会做的一次演讲中才泄露出去。而后，又在"科学美国人"上详细地探讨了 Core war 中可自我复制程序的原理。从此，美国有关学术界才开始了实质性的研究。

1983 年弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序，在全美计算机安全会议上提出并在 VAX 11/150 机上作了演示。在一周后，他又获准进行了实验演示，共演示了 5 个实验，由此，证实了计算机病毒的实际存在。伦·艾德勒

曼(Len Adleman)将它命名为"计算机病毒"。

随着计算机技术的发展,出现了一些热心于编制程序的计算机爱好者。尤其是年轻的学生,他们热衷于用计算机作一些恶作剧的游戏,并探索有自我复制能力的潜伏程序的奥秘。

1985 年,IBM PC 机上出现了恶意的特洛依木马(Jrojan Horse)程序 EGABTR,该程序在显示漂亮的图象效果的同时,删除磁盘上的文件。

1986 年在巴基斯坦的拉哈尔,一家出售 IBM PC 微型计算机的商店,年青的两兄弟阿姆加德(Amjad)和巴锡特(Basit),对社会上软件互相拷贝和交换产生好奇和兴趣,他们动手编制了一个计算机病毒程序,并在程序中注明了自己的姓名和地址,这就是所谓的巴基斯坦病毒。这是到目前为止,世界上唯一标注有编写者姓名和地址的病毒。该病毒程序运行时在屏幕上显示:

welcome to the Dungeon
(c) 1986 Basic & Amjad (pvt) ltd
BRAIN COMPUTER SERVICES
730 Nijam Block Allama Igbal Town
Lahore,Pakistan
Phone:430791,443248,2800530
Beware of this VIRUS
confact us for vaceination

他们把载有此病毒的软盘送给了一个朋友,至此造成了巴基斯坦病毒在全球的流传。

1987 年 5 月,帕金斯·坦尼电脑公司为了防止公司非法复制软件产品而制造的病毒在美国"普罗威斯顿日报"编辑部的计算机上显示信息:"欢迎进入土牢,请小心病毒……"

1987 年 12 月 IBM 公司的计算机网络由一份电子邮件传入了"圣诞节蠕虫程序"。每当用户显示内容时,病毒程序就以链式反应方式自我复制,最后导致网络拥挤,使部分计算机被迫停止运行。

1988 年 3 月,潜伏于苹果机中的病毒发作。被广泛感染的苹果机都停止了工作,并显示信息:"向所有苹果电脑的使用者宣布世界和平的消息",以此庆祝苹果机的生日。

1988 年 11 月 2 日美国康乃尔(cornell)大学研究生 23 岁的罗伯特·莫里斯(Robert Morris)制造的蠕虫事件,则是一起震憾全世界的"计算机病毒侵入网络的案件"。这个事件是计算机病毒演化过程中的一个重要转折点。该事件迫使美国政府立即作出反应,国防部成立了计算机应急行动小组。该事件发生后,美国报纸和电视台立即作了报导,使"计算机病毒"第一次成为国际社会的新闻热点。

莫里斯设计的病毒程序约有 6000 字节,可在 UNIX 环境下窃取口令字,并冒充合法用户将病毒程序拷贝到远程计算机中。病毒程序利用美国最大的计算机网络 Inter Net 网上的 Sendmail 程序进入计算机。这个病毒程序切断系统的安全功能,并把一段程序复制到另一台机器上,这段程序经编译和运行,再侵夺机器上的二进制命令和文件,连续复制和传播病毒程序。罗伯特·莫里斯设计的病毒实际上是钻了 UNIX4.3 的漏洞。根据 UNIX 专家的分析,病毒以 3 种途径侵入系统:

通过 Berkelgy UNIX 4.3 "Sendmail" 中的程序故障,使调试位呈通态;

在"Finger"程序中一部分使缓冲器过载,使它对病毒程序的另一部分进行编译和连接;

通过获取口令进入系统。

计算机病毒侵入后通过 Inter Net 网络不断扩散，直接影响 SUN 和 VAX 系统的运行。

莫里斯病毒侵入的 Inter Net 网络包括 5 个计算机中心和 12 个地区节点，连接着政府、大学和研究所共 250000 台计算机。该网中连接着 3 个主要网络：美国国防部高级研究计划局网络，军用网络和国家科学基金会网络。从 11 月 2 日上午 5 时病毒开始运行到下午 5 时，约有 6000 台与 Inter Net 网络连接的计算机，包括国家航天航空局，军事基地和主要大学的计算机停止了运行。直接经济损失达 9600 万美元。莫里斯本人被判 3 年缓刑，罚款 1 万美元，并罚做 400 小时的社会服务。

莫里斯病毒程序利用了 UNIX 操作系统的漏洞侵入系统。值得注意的是，该病毒程序虽然并不"恶意"地删除文件和破坏数据，但它无限制的繁殖抢占了大量的时间和空间资源。当发现网络超载后，莫里斯本人也失去了对程序的控制能力，已经没有办法制止机器上发展的状态。

莫里斯蠕虫事件引起了美国和世界计算机界的震惊，各国计算机专家及社会各界纷纷发表评论，至此，计算机病毒和计算机安全问题开始提到日程上来。

计算机病毒继续在世界上蔓延。尤其是一些恶性病毒的制造，更是对计算机系统的恶意攻击和破坏。

1987 年秋在以色列的希伯莱大学发现的"黑色星期五"病毒就是它们的代表。该病毒传染所有的可执行文件。按原计划黑色星期五病毒将在 1988 年 5 月 13 日（星期五）破坏该大学 1500 台微机系统的运行，恶意地破坏和删除磁盘中所有的可执行文件。该病毒因为快速侵占内存空间而在激活前被发现。但是，黑色星期五病毒程序的缺陷经过某些修改后成为目前在全球流行的恶性计算机病毒。它的触发条件仍是"13 日星期五"。1989 年 10 月 13 日，尽管国际社会已向各国发出了警告，一些国家的计算机仍遭到感染和破坏，国此，许多人称 10 月 13 日为世界计算机病毒流行日。

随着微型计算机在我国的普及，计算机病毒也逐渐流传开来。1988 年底在国家统计部门发现了小球病毒。该病毒侵入计算机后在屏幕上显示跳动的小球，发生跳荡后又不断地反射。它使机器运行速度明显地下降。尤其在 CCDOS 中文情况下它造成屏幕上下滚动，小球布满全屏幕，机器运行速度变慢，很快造成死机。由于缺乏防治措施，小球病毒迅速在我国流传。国家统计局下属省、市、县级的统计部门近 3000 台微机均受到感染。1989 年夏季，国家统计局召开病毒防治研讨会并采取检测、防治措施后，小球病毒仍禁而不止。更有甚者，在我国境内出现了大量小球病毒的变种。目前计算机病毒仍在中国大地蔓延，品种逐渐增多，病毒变种也逐渐增多，侧着破坏性大的恶性病毒发展。同时，由于软件输入的增加，国外流行的最新计算机病毒也在我国逐渐发现并且迅速蔓延。

第三节　计算机病毒的来源

从上面叙述的计算机病毒发展的历史可以看出，计算机病毒是人为制造出来的，是人们为着各种目的所编制的计算机程序。病毒制造者按着各自的意图，编制出一个能自我复制的、有不同破坏性的程序，并使其流传，造成了当今世界上方兴未艾的计算机病毒冲击浪潮。根据计算机病毒制造人员主观目的的自我表现和病毒程序传播中的客观效果，可将计算机病毒的来源分为几类：

1. 游戏和恶作剧

一些计算机爱好者和大学的学生们对计算机技术及其应用有着特殊的兴趣。一般说来，他们大多具有较好的计算机知识基础，为了开发自己的智能或者表现自己的才华，他们制造恶作剧的能力显自我复制的病毒程序，并使它在社会上流行，这类病毒程序在计算机屏幕上显示不同种类的图形或者玩笑性的警句。这种程序一般破坏性不大，也易于发现。但由于程序不断复制自己，从而侵占了系统的存储空间，因此也给计算机的正常运行造成一定程度的危害。

2. 软件自我保护

某些软件设计者或软件公司所开发的软件产品没有得到法律的正当保护，许多产品被非法拷贝，使其利益受到损害。为了保护自身的利益和给复制者以报复性的惩罚，他们在自己的软件系统中藏入可以自我复制、并带有破坏性的病毒程序。有的计算机俱乐部的成员将自己开发的应用程序公布在计算机网络中的公告板(BBS)上，欢迎大家选用，但使用者需邮寄使用费。否则，暗藏在应用程序中病毒程序机制就会像定时炸弹一样爆发，造成"占便宜者"的计算机系统的破坏。这种情况愈演愈烈，甚至发展到用计算机病毒来进行敲诈勒索。例如，1989 年 12 月肯尼亚一些银行和企业因使用了由伦敦寄来标有"爱滋病信息磁盘"字样的软盘没有付给要求的款项相继染上病毒，使计算机磁盘文件遭到严重破坏，有的计算机陷入瘫痪。

3. 蓄意破坏

某些组织和个人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，就是一种蓄意破坏行动。例如前面提到的，1987 年在以色列希伯来大学出现的黑色星期五病毒就是其雇员在被辞退时故意制造的。它针对该大学的计算机系统，一旦激活将彻底摧毁该系统，是破坏性极大的恶性病毒。由于计算机病毒潜在的威胁性被越来越多的人所认识，计算机病毒已成为某些人使用的新的恐怖手段。我国国内已发现破坏性很大名叫"中国炸弹"的计算机病毒，表明制造、传播计算机病毒已为成为计算机犯罪的衍生形式。

4. 军事目的

电子计算机已成为现代军事系统的重要组成部分。许多事实表明：武器的自动化程度越高，计算机所占的比重就越大。海湾战争是以计算机为中心的高技术武器的一次实战试验。海湾战争的经验使人们进一步认识到，在现代化军事系统的装备、指挥、控制、管理等等方面，计算机都起着影响全局的作用。其中计算机软件是最活跃的因素，甚至是决定一切的主要因素。为取得未来战争的胜利，军事对垒的双方，一方面要加强本营垒中计算机的安全性和可靠性；另一方面要千方百计干扰和破坏对方的计算机系统，包括使用计算机病毒破坏对方的计算机软件系统，削弱对方的战斗力。伴随着军队越来越依赖于电子武器及其指挥和控制系统，计算机病毒可以用来从事电子对抗战的说法逐渐被许多人接受。由于下一代武器和作战系统均是由计算机软件控制的，计算机病毒便成为一种巨大的威胁。而目标捕获、战场管理和有关作战的连网计算机系统，都将是未来"计算机病毒"的主要攻击目标。

根据 1990 年 5 月来自纽约的消息，美国军队悬赏摧毁敌人电子系统的计算机病毒研制者。军方对竞争军用计算机病毒获胜者将提供 55 万美元的研制费用。悬赏来的计算机病毒可以用来摧毁军用通信线路和控制系统，传递有意错报的信息，病毒可用来改变敌方向战斗部队传递信息的通信卫星软件，可通过无线电通信系统潜入敌方的计算机系统，等等。据此

人们预料，计算机病毒很可能在将来被用于军事目的，成为军事电子对抗战的重要手段和工具。计算机病毒将变为一种新式武器。

第四节　计算机病毒的特点

从上面讨论的几种主要计算机病毒的来源可以看出，计算机病毒是人们为了达到一定的目的，所编制并令它广泛传播的一段计算机程序。就目前所发现的计算机病毒来说，其主要特点是：

一、传　染　性

类似生物界的"病毒"，传染性是计算机病毒的一个重要特性。一个计算机病毒能够主动地将自身的复制品或变种传染到系统中其它程序上，也就是说，计算机病毒的传染性在于计算机病毒的强再生机制。病毒程序一旦进入系统，就与系统中的程序链接在一起。并在运行这一被感染程序时，在系统中开始搜索能进行传染的其它程序，并把病毒自身或变种复制到其它程序上，从而达到再生的目的。经过不断地传染，再生，该病毒的副本不断地增加，使该计算机病毒迅速地扩散到磁盘存储器和整个计算机系统。计算机病毒可以传染一个微机系统，一个局部网络，一个大型计算机网络以及一个多用户系统。

一台微型计算机一旦感染上计算机病毒，病毒不仅在本系统中很快地扩散并实施破坏作用，使系统丧失正常运行的能力，而且被感染的计算机即成为该病毒流行的一个传染源，构成对同类计算机或兼容系统的一个威胁。通过计算机系统数据共享的途径，如网络连接或磁盘拷贝，病毒会不断地扩散，波及整个地区乃至形成世界性的蔓延。

在大型信息系统和计算机网络的工作环境下，计算机病毒传染的速度越快，则病毒程序对系统的破坏性就越大。

病毒程序的传染性反映了病毒程序最本质的特征。严格说来，一个程序若没有传染、再生机制，就不能叫做计算机病毒。

二、破　坏　性

计算机病毒对计算机系统的正常运行都具有一定的破坏性。所谓破坏性，不仅仅是指破坏系统，删除或修改数据，而且也包括占用系统资源，干扰机器运行等等。

从计算机病毒设计者的主观意图和病毒程序对计算机系统的破坏程度来看，已发现的计算机病毒大致可分成恶作剧和恶性病毒两类：

1. 恶作剧类型

这类病毒的制作者一般仅为了取乐和炫耀自己的技巧，所编病毒程序不破坏系统和数据。如 IBM 圣诞树病毒，可令计算机在圣诞节时显示问候的话语，并在屏幕上显示圣诞树的图象。除占用一定系统开销外，对系统破坏性小。有些人将这种形式的病毒称为良性病毒，确切地讲，应称为破坏性较小的病毒。

2. 恶性病毒型

病毒设计者的目的在于明确地破坏系统中的某些目标，从而破坏系统的正常运行。因而，这些病毒对计算机系统的破坏力是很大的，所造成的后果是极其严重的。最常见的恶性

病毒往往是消除或破坏数据，删除文件，对磁盘进行格式化等。这类计算机病毒可以中断大型计算机中心的工作，使某个计算机网络处于瘫痪，造成灾难性的损失。

计算机病毒的破坏性反映了病毒设计者的目的。但是任何病毒都是一种可执行的程序，病毒程序运行时，均要占用 CPU 时间和内存空间，降低系统正常工作的效率。恶作剧类的病毒程序要表现自己，必然要干扰系统的正常工作，打乱屏幕的显示。病毒程序的传播又大量消耗系统存储资源。因此，广义而言，任何病毒都是有害的。

根据病毒大规模扩散的情况和计算机病毒频恶性病毒发展的趋势来看，强调指出病毒的破坏性是十分必要的。首先，任何类型的病毒都要占用系统的开销，干扰和破坏系统的正常运行。病毒对系统的破坏程度，不完全取决于设计者的目的，还取决于病毒运行的系统环境。例如前面叙述的，侵入美国 Inter Net 网络的莫里斯蠕虫程序，虽然该程序并不主动删除文件和破坏数据，却给美国最大的计算机网络造成巨大损失。再者，任何计算机病毒都是对计算机系统的非授权侵入，是对计算机系统安全工作的威胁，是一种违法行为。

三、隐 蔽 性

计算机病毒程序设计者为了使病毒程序达到非法进入计算机系统并进行广泛传播的目的，必须要在病毒程序表现之前设法隐蔽病毒本身。为了不被轻易的发现，一些广为流传的病毒都将自己隐藏在其它合法文件之中。病毒本身没有文件名，在列文件目录时也不被显示出来，尽量避免引起工作者的注意。

计算机病毒程序一般都短小精悍。因为病毒程序的设计者往往是程序设计技巧较高并且熟悉计算机内部结构的人员，他们能够设计出精致小巧的程序。由于程序短小，易于隐藏，病毒程序就不易被人察觉和发现。

当计算机病毒进入系统并进行传染时，源病毒经自我复制产生的病毒副本或变种往往使用前后链接或插入的方式隐藏在可执行文件或数据文件中。有的病毒能采取分散或多处隐藏的方式，而当病毒潜伏的程序体被合法调用时，病毒程序也合法投入运行，并将分散的程序部分在所非法占用的存储空间里进行装配，从而构成一个完整的病毒体投入进行状态。

四、潜 伏 性

病毒程序侵入系统后，一般不立即活动，需要等待一段时间，待外部条件成熟时才起作用。这就是病毒程序的潜伏性。一个编制精巧的病毒程序，可以在几周，几个月，甚至几年内进行传播和再生而不被发现。在此期间，系统的磁盘驱动器可能不断地复制病毒程序，制成病毒的副本或变种并传送到各部位，使它们感染病毒。因此，病毒的传染性与病毒的潜伏性有很大的关系。病毒程序编制得越精巧，它的潜伏期越长，则该病毒相对的传染性就越大。

所谓潜伏期是指病毒从外部设备(如磁盘驱动器)随寄生的合法程序进入系统，到病毒的破坏或表现部分开始作用时止的一段时间。病毒进入系统的时间，我们虽不能精确判定，但计算机病毒的潜伏期是可以判定的。因病毒所寄生的合法程序执行的时间可以精确判定。特定病毒的潜伏期越长，那么它的潜伏性就越好，这样病毒的传染作用可在较长的时间内发挥作用，其传染的范围也就相应地扩大。

五、寄 生 性

每一个计算机病毒程序都不能以独立的文件形式存在。它必须寄生在一个合法的程序之上。这个合法程序就是病毒程序生存的必要环境。这些合法程序包括引导程序，如主引导程序，DOS 引导程序；系统可执行程序，如 IBM PC 中的 IBM BIO·COM 文件，IBM DOS·COM 文件及 COMMAND·COM 文件；一般应用文件 如扩展名为 COM 或 EXE 等可执行应用文件。这些被病毒程序寄生的合法程序叫做该病毒的宿主程序或称为该病毒的载体。

一种病毒的寄生方式决定它的传染方式。计算机病毒的寄生方式可以分为覆盖型寄生方式，代替型寄生方式，添充型寄生方式，链接型寄生方式和转储型寄生方式。

覆盖型寄生方式是指病毒程序用自身的程序代码，部分地或全部地覆盖在寄生的宿主上使原宿主的部分功能或全部功能被破坏，如 512 病毒。

代替型寄生方式是指病毒用自身程序代码代替原宿主程序代码。病毒程序能完成或简单完成原替代程序代码的主要功能，如感染硬磁盘的主引导扇区的打印(Unprinting)病毒。

添充型寄生方式是指计算机病毒将自身的代码隐藏在寄生宿主内部未存有信息的空间的存储单元中，如勒海(Lehigh)病毒。被这种病毒传染的文件长度不变。

链接型寄生方式指病毒程序附加到寄生的宿主程序之上，并不破坏被寄生程序的代码。病毒程序可以寄生于宿主程序的开头、中间或尾部，计算机病毒程序附加到宿主程序的头部时，叫做头部链接式，如黑色星期五感染 COM 文件时属头部链接。病毒程序链接于宿主程序的尾部时，叫做尾部链接式。黑色星期五病毒感染 EXE 型文件时属于尾部链接。而中间链接式是指计算机病毒附加在宿主程序的中间。间接链接式是指病毒不直接与合法程序链接，而是存储于特定的存储空间，通过特定的功能在其宿主程序执行时获得控制权。

转储型寄生方式是指计算机病毒将其宿主程序部分或全部的代码转储到其它的存储空间，而病毒本身侵占该病毒宿主程序原来的存储空间。如小球病毒传染系统时将正常的 DOS 引导程序转移和存储在所寻找到的第一个空间簇中，而把病毒程序的前半部分存于 DOS 引导程序的原存储空间。

第五节 计算机病毒的分类

据统计，目前世界上出现的计算机病毒种类繁多，约有 2000 多种。为了便于分析和检测，需要将这些门类繁多的计算机病毒进行分类。

计算机病毒可以从不同的角度来进行分类。

一、按攻击对象分类

若按病毒攻击的对象来分类，可分为攻击微型计算机、小型机和工作站的病毒，甚至安全措施很好的大型机及计算机网络也是病毒攻击的目标。这些攻击对象之中，以攻击微型计算机的病毒最多，其中 90%是攻击 IBM PC 及其兼容机的，其它还有攻击 Macintosh 及 Amiga 计算机的。

二、按人侵途径分类

按计算机病毒侵入系统的途径，微型计算机的病毒大致可分为 4 类

1. 操作系统病毒

小球病毒和大麻病毒就属于典型的操作系统病毒。这类病毒用病毒本身的程序意图加入或替代部分操作系统进行工作。操作系统病毒是常见的计算机病毒，具有很强的破坏力。这是因为整个计算机是在操作系统的控制之下运行。该类病毒的入侵造成病毒程序对系统持续不断的攻击。严重时，可导致整个系统的瘫痪。

一般操作系统类病毒，当系统引导时就把病毒程序从磁盘上装入内存中，在系统运行时，不断捕捉 CPU 的控制权，进行计算机病毒的扩散。

2. 外壳病毒

这类病毒常附在宿主程序的首尾，一般对源程序不进行修改。外壳程序较常见，大约有半数左右的计算机病毒采用这种方式来传播病毒的。外壳病毒容易编写，也易于检测，一般测试可执行文件的长度就可找到。对于 IBM PC 机及其兼容机，外壳病毒一般感染 DOS 下的可执行程序。

3. 源码病毒

源码类病毒在程序被编译之前插入到用 FORTRAN，PASCAL，C 或 COBOL 等语言编制的源程序之中。源码病毒往往隐藏在大型程序之中，一旦插入到大型程序中其破坏力和危害性是很大的。

在当前国际上流行的计算机病毒中，源码病毒较为少见。编写源码病毒程序的难度较大，受病毒程序感染的程序对象也有一定的限制。

4. 入侵病毒

入侵类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。当入侵病毒进入到主程序后，不破坏主程序就难以除去病毒程序。

入侵病毒难以编写。这类病毒一般是针对某些特定程序而编写的。

三、按传染方式分类

按传染方式分类，微型机的病毒可分为下述 3 类。

1. 传染磁盘引导区的病毒

每种病毒都有自身特定的寄生宿主。传染磁盘引导区的计算机病毒的寄生宿主就是 DOS 的磁盘引导程序。对软盘来说，引导程序只有 DOS 的 BOOT 区引导程序。而对于硬盘，有传染硬盘主引导程序的计算机病毒和传染硬盘 DOS 分区中 BOOT 区引导程序。

2. 传染可执行文件的病毒

传染可执行文件的病毒又可分为：

①传染操作系统文件的病毒

这类病毒传染操作系统运行时所必须的文件，如传染 PC-DOS 操作系统中的 IBM BIO・COM，IBM DOS・COM 及 COMMAND・COM 等操作系统核心文件。如'中国炸弹'只传染 COMMAND・COM 文件。

②传染一般可执行文件的病毒

这种病毒寄生于一般以 COM 或 EXE 为扩展名的可执行文件中，或者扩展名为：OVL，OVR，SYS，OBJ 等可执行文件中。病毒传染可执行文件后，将自身链接于被传染程序的头部或尾部，这种病毒一般都要修改被传染程序的长度和一些控制信号，以保证病毒成为可执行程序的一部分。这类病毒的传染性很强。

③既传染文件又传染磁盘引导区的病毒

目前出现了一些病毒，它们不但传染可执行文件，而且还传染磁盘的引导区。如 Flip 病毒，新世纪病毒等。新世纪病毒不仅传染以 COM 和 EXE 为扩展名的可执行文件，而且还传染硬盘的主引导区。这类计算机病毒的消除工作更加困难。被这种病毒传染的系统用 FORMAT 命令格式化硬盘都不能消除病毒。

四、按寄生方式分类

按病毒的寄生方式分类，微型计算机病毒大致可分为 5 类。

在关于计算机病毒的寄生特性时，我们谈到：计算机病毒都要寻找自身赖以寄生的对象，以保证自己生存的环境。按照计算机病毒寄生于其寄生宿主的不同方式，计算机病毒可分为 5 种类型：

①覆盖型寄生病毒；

②代替型寄生病毒；

③链接型寄生病毒；

④添充型寄生病毒；

⑤转储型寄生病毒；

五、按破坏意图分类

按病毒的破坏意图和表现方式来分，计算机病毒可分为两种：

1. 恶作剧型

即所谓“良性病毒”。该类病毒一般不破坏系统和数据。但却能不断复制自己和快速地向外扩散，因而大量占用系统资源。严重时，也会使系统瘫痪。

2. 恶性病毒

有破坏目的的病毒。最常见的恶性病毒会破坏数据，删除文件或对硬盘格式化。这类病毒的破坏作用极其严重。

按照计算机病毒的各种特性，计算机病毒还有许多分类方法。如针对军事、政治、经济不同目的的病毒分类，等等。

第六节　计算机病毒的危害性

不管计算机病毒设计者的主观愿望是不是直接破坏计算机系统，病毒对系统的危害性都很大。仅仅为了表现自己的恶作剧病毒，由于它们占用系统资源，往往造成系统不能运行的恶劣后果。计算机病毒的危害性不取决于病毒程序的大小，而取决于病毒程序的再生能力。计算机病毒像生物病毒一样，只要条件合适就进行传染，并伺机破坏。一个计算机系统，凡是用软件手段能触及到计算机资源的地方都可能受到计算机病毒的破坏。一台典型 IBM

PC 机的病毒能在一个月内将整个地区的未联网的计算机感染。在已联网的系统中只要信息能被分享、解释和传递，病毒就能迅速扩散到整个系统。一旦条件成熟，即摧毁整个系统。

计算机病毒的主要破坏作用与危害性如下：

(1)破坏文件分配表

使用户在磁盘上的信息丢失。如微机系统若感染大麻病毒，大麻病毒将硬盘(20MB)的主引导程序移至后面物理第七扇区，从而破坏了硬盘的 DOS 文件分配表。此时若在长城 0520CH 机上打印时，虽 CCLIB24 字库文件存在，但屏幕却多次提示无字库文件。这是由于文件分配表的破坏，使文件名与文件的本体失去了联系。

(2)删除软盘或硬盘上的可执行文件或数据文件

在这种情况下，若删除的文件属于系统文件，如主引导程序，则该磁盘将不能导引系统。若在 13 日星期五在感染了黑色星期五病毒的计算机系统中运行的 COM 或 EXE 文件均会被病毒删除掉。

(3)修改或破坏文件中的数据

在一些企业和银行，系统文件数据被破坏，造成了极其严重的后果。

(4)减少磁盘空间

使磁盘中的坏扇区增多，可用磁盘空间减少。

(5)显示非正常信息和图象

屏幕显示特殊的信息和图象，影响正常工作的进行。如大麻病毒显示“Your PC is now stoned”，小球病毒在屏幕上出现跳动的小球，1575 病毒在屏幕上显示小毛虫等。

(6)不能存贮正常的数据和文件

病毒程序自身的多次复制，使系统存储空间异常减少，正常的数据和文件不能存贮。

(7)造成写错误

改变磁盘分配，造成数据写入错误。

(8)更改或重写磁盘的卷标

(9)影响内存常驻程序运行

(10)非法格式化

对整个磁盘或磁盘的特定的磁道或扇区进行格式化。

(11)破坏磁盘目录区

(12)计算机运行速度明显减慢

(13)打印机出故障

打印机或通讯端口异常；打印机速度明显降低或打印机失控。

(14)磁盘文件长度无故增长

(15)改变系统的正常运行过程

如小球病毒传染的系统运行 OFFICE 时不能正常打印汉字。

计算机病毒的种类目前仍在增加，因而病毒的破坏现象也是多种多样。再加上不同病毒同时传染整个计算机系统，形成不同病毒的交叉感染，使它们的破坏现象变得更加复杂。我们在检测病毒时应注意分析这些现象。

第七节　计算机病毒的状态及潜伏期

进入传播流行中的计算机病毒有两种状态，即静态病毒和动态病毒。

静态病毒指寄生于存储介质(例如软盘、硬盘、磁带等)上的计算机病毒。静态病毒没有处于加载状态，不能进入计算机内存，因而不能执行病毒的传染或破坏作用。

动态病毒是随病毒宿主的运行，如启动病毒寄生的软盘、硬盘，或执行染有病毒的程序时，病毒程序进入内存，处于运行状态或通过某些中断能立即获得运行权的计算机病毒。病毒的传染和破坏功能主要是动态病毒执行的。处于内存中的病毒时刻监视着系统的运行，一旦传染条件或破坏条件被满足，就调用病毒程序中的传染模块或破坏模块，使病毒得以扩散，使系统蒙受损失。

动态病毒在计算机内存中存在的时间称为动态病毒的生命期。动态病毒的生命期随病毒种类不同而不同。

常驻内存型病毒在其寄生的宿主程序执行时，计算机病毒就在内存中开辟一块"栖生地"常驻于内存之中，当其原宿主程序执行完毕退出后，病毒仍保留在内存中，并通过侵占的中断向量或修改的系统程序模块，监视系统的运行，伺机进行扩散或破坏。这类病毒的生命期较长，会一直延续到下一次重新启动或停机。黑色星期五，黑色复仇者等传染引导区的病毒均是这种常驻内存，生命期较长的病毒。

不常驻内存型病毒，如维也纳病毒，随着其病毒宿主程序的运行而进入内存，并在病毒宿主程序执行完之前根据传染或破坏的条件完成病毒要进行的传染或破坏作用。当宿主程序执行完时，随宿主程序一起退出内存。因而，不常驻内存型病毒的生命期较短。

计算机病毒进入内存、变成动态病毒以后，并不马上进行破坏或表现自己即显示一定的信息或图画，仅仅进行不断地传染、扩散活动。因而，我们很不容易发现它们。只有当病毒程、序破坏或表现模块的触发条件满足时，如某日某时病毒才破坏系统或显示信息，从而暴露自己。从病毒进入内存到其破坏或表现模块被触发，这段时间是病毒程序的潜伏期。显而易见，一种病毒的潜伏期越长，病毒程序的传染性可在较长的时间内得到发挥，其传染的范围也就大些。潜伏期和传染性之间的关系可用图 1-1 的曲线表示。

病毒的潜伏期越长，说明病毒隐藏自己的潜伏性越好。因而，病毒的潜伏性可用其潜伏期来衡量。

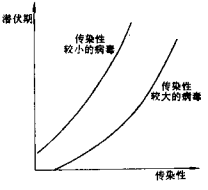

图 1-1　计算机病毒传染性与潜伏期的关系

计算机病毒进入内存，变成动态病毒后，一般不是无条件地进行传染和破坏的。而是需要首先判断传染条件或破坏条件是否满足。待条件达到时，才进行相应的传染或破坏活动。因而，计算机病毒的活动都是由条件触发来实现的。计算机病毒的传染活动的触发，是当系统工作条件满足病毒传染所需条件时，病毒即将符合条件的宿主进行传染。而病毒的破坏或表现活动的触发，是当系统条件满足时，病毒的破坏或表现模块被触发，或称之"被激活"，即开始破坏系统或在被传染的系统上表现自己。计算机病毒的一般工

作流程，可用流程图简单表示出来，如图 1-2。

计算机病毒在一定条件下触发病毒的传染模块或破坏和表现模块，也就是在满足一定条件下实行对病毒的传染模块或破坏和表现模块的调用过程。

计算机病毒传染活动或破坏和表现活动的触发条件可以是多种多样的。

首先，触发条件可以是单个条件或复合条件。

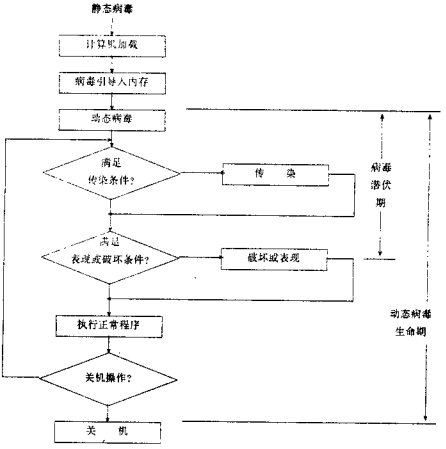

图 1-2　计算机病毒工作流程示意图

1. 单条件触发

仅仅需要一个条件即可触发的病毒活动是单条件触发。如：萨达姆病毒，每当中断向量 INT 21H 调用 8 次时，病毒的表现部分即被显示。

2. 复合条件触发

若干个条件经过逻辑组合后的条件称为复合条件。如：黑色星期五病毒的触发条件是某月 13 日，并且又是星期五。因而黑色星期五病毒是复合条件触发的，即两个条件的逻辑“与”(·AND·)。

再者，计算机病毒的触发条件一般有时间触发条件，功能触发条件，宿主触发条件等。

(1) 时间触发条件

以特定的时间进行触发的条件。计算机病毒以系统日期(某年某月某日)或系统时间(某时某分某秒)为触发条件,或作为触发的复合条件中的一个单条件。

(2) 功能触发条件

以计算机所提供的功能作为触发条件。这些计算机功能包括系统的软、硬件的特定功能实现,以及计算机的一些指令、命令的执行等。例如,一条 COPY 命令,某个中断向量的调用,或者一条指令等等。功能触发条件也可与时间触发条件或其它功能条件、宿主条件构成复合条件。

(3) 宿主触发条件

许多计算机病毒,尤其是传染可执行文件型的病毒,对于正在运行或当前目录下的程序或正在引导中的磁盘是有选择性的。如 4 月 1 日病毒仅传染扩展名为 COM 的可执行文件,而阿拉梅达病毒只传染软磁盘而不传染硬磁盘。

计算机病毒一般只传染未经病毒感染过的软盘和可执行文件。因此,在病毒进行传染前一定会校验被选中的宿主是否符合未曾被传染过这个条件。

第八节　计算机病毒的命名

当前,计算机病毒及其变种种类繁多,这些病毒都是秘密文件,在文件目录表中查找不到标识它们的文件名,而且往往病毒都是非授权侵入系统,又流传得十分迅速和广泛,因此很难找到它们的根源。为了更好地分析和检测并消除这些病毒,也为了互相交流检测和防治病毒的经验和方法,需要对流传较广、影响较大的病毒给予一个特定的名字,用以标识不同的病毒。

现在较为普遍的命名方法有以下几种:

1. 按病毒自己宣布的名称命名

某些计算机病毒的源代码中宣布了病毒的名称,如磁盘杀人病毒中有如下提示"Disk Killer version 1.00 by Ogre software April 1,1989.",则人们将它命名为"Disk killer"。如黑色复仇者包含有下列信息:"This program was written in city of Sofia (c) 1988－1989 Dark Averger",所以,被称为"Dark Averger"。

2. 按病毒程序显示标识的特征字符串命名

如大麻或石头病毒,在屏幕上显示:"Your PC is now stoned Legalize Marijuana",因而人们叫它 Marijuana 或 stoned。另外,如星期日病毒,显示中含有 Sunday";而萨达姆病毒,显示中含有 saddam 字样等等。

3. 按病毒最先出现的地点命名

如冰岛病毒于 1989 年在冰岛发现,而台湾病毒首先在我国台湾出现。

4. 按病毒的表现症状命名

如小球病毒运行时会在计算机屏幕上出现跳动的小圆点,因而得名,也叫做"圆点病毒"。

5. 按字节长度命名

以计算机病毒传染磁盘文件时文件所增加的长度而命名。如最近国内发现的病毒感染

文件时文件长度增加 2153 字节，故命名“2153 病毒”。

6. 按时间命名

按病毒特定的触发时间或病毒宣布的编写时间定名

如 4 月 1 日病毒，在 4 月 1 日该病毒激发，在屏幕上显示如下信息：“APRIL 1st HA HA HA，you have virus”(4 月 1 日，哈哈哈，你有一个病毒了)，然后系统死机。又如黑色星期五病毒，当某个 13 日又是星期五时，病毒破坏系统文件，于是人们将它定名为黑色星期五。

第九节　计算机病毒的标志

计算机病毒都有自己的标志特征。即病毒在对磁盘或文件进行传染后，都要在该磁盘宿主或宿主程序上做上自己的标志。以后病毒再要进行传染，首先要判断要传染的磁盘或程序是否已经传染过。病毒将从程序特定的位置提取字符串，如果该字符串是病毒自身的标志则放弃传染。

大多数情况下，病毒的标志是由 26 个英文大、小写字母和数字组成的字符串。病毒标志通常放在一个特定的位置：如引导型病毒，病毒标志多放在病毒程序的第一部分中，而文件型的病毒多放在被传染文件的尾部，等等。

病毒标志可以做为我们检测、判断病毒的特征字。如小球病毒在传染引导区后将偏移量 IFCH 和 IFDH 两处的位置为 57H，13H。若从这两处检查到 1357H，则可检测出小球病毒；1575 病毒在被传染文件的尾部标记有 OAOCH，则可用 OAOCH 标志检测出 1575 病毒，黑色星期五病毒在被感染文件的尾部加以标志“MsDos”，而 Liberty 病毒在传染 COM 文件时从文件头偏移 5EH 字节处置以病毒标志：Liberty，而在传染 EXE 文件时，从文件头开始偏移 02H 字节处为病毒标志 FFFFH。

设置病毒标志是病毒设计者的特意安排。这样，病毒既可以广泛传播，又可以做得隐蔽不容易被发现。如果被病毒感染的磁盘或程序没有置以特定的标志，则磁盘或文件就可能被同种病毒再次感染。而这个再次感染的过程在磁盘还有自由空间之前不会结束。解如，在磁盘引导区第一次感染时，病毒将原引导程序和病毒程序的第二部分放在一个被人为标以坏的空簇中。第二次感染时，病毒将在第一次感染时写到引导区的病毒程序的第一部分和病毒程序第二部分放到另一个标为坏簇的空簇中，以此类推，一个自由空间很多的磁盘不要很久就变得无可用空间，很快就会被用户发现和处理。对于启动盘，不仅磁盘空间被病毒占用，而且启动速度很快减慢。这是由于启动盘被无病毒标志的同种病毒感染了 n 次，则最后加载 DOS 前要把病毒程序在内存中安装 n 次，启动时间明显增长，因而很容易被检测出来。

第二章　有关计算机病毒的技术基础

第一节　磁盘结构

磁盘是微型计算机程序和数据广泛使用的存贮介质，也是计算机病毒传播、入侵的主要对象之一。因此，了解磁盘的结构及其数据组织的特点，对于检测和防治计算机病毒具有十分重要的意义。

一、软磁盘结构和存储方式

磁盘分为两种：软盘(Diskette)和硬盘(Fixed disk)。

目前，微型计算机使用最普遍的是5.25英寸和3.5英寸的软盘。

1. 软磁盘的结构

本节中以5.25英寸软盘为例，介绍软磁盘的结构。

软磁盘可分为单面可用(对应一个磁头)的单面磁盘和双面可用的(对应两个磁头)的双面磁盘。目前微型计算机采用较多的是双面双密度软盘(40道360K字节)和双面高密度软盘(80道，1.2M字节)。5.25英寸磁盘的外观和结构示意表示在图2-1和图2-2中。

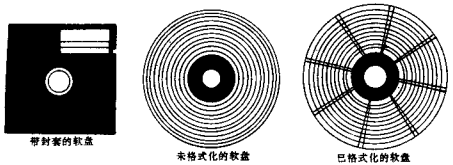

图2-1　5.25英寸软磁盘

一个磁盘，不是任何位置都可以贮存数据信息的。磁盘在使用前，必须先经过"格式化"，将其划成标准格式，使之符合DOS系统的规定。磁盘格式化时，以转轴中心为原点，把磁盘表面划分成一个个同心圆，称为磁道。数据是贮存在磁道中的。5.25英寸的软磁盘被划分成40个磁道，由外向内编号为0到39。对每个磁道，又以索引孔与圆心连线为起点，逆时针方向将圆周划分为若干个夹角相等的扇区(sector)见图2-2。5.25英寸软盘又分为8个或9个扇区，由操作系统决定。

每条磁道由首部，9个扇区和尾部构成。当磁盘驱动器检测到软磁盘上的索引孔时，这

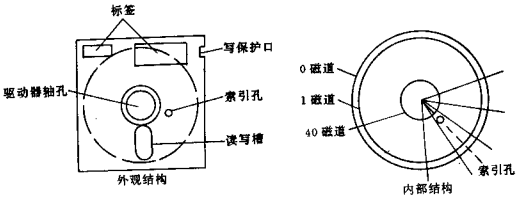

图 2-2　5.25 英寸软磁盘结构示意图

就是磁道的开始读写位置。考虑到，不同的驱动器对软盘定位时有一定的定位误差，所以格式上留有一定的允许误差间隔，这就是首部。在 IBM 软盘格式中，首部中写入软索引标记。同样，为了防护不同驱动器对软盘格式化时转速的变化，磁盘在依次设置好首部和各扇区以后，留有一段尾部。尾部的长度大于磁盘旋转一周时数据的变化量。

磁道中的每个扇区由 4 部分组成。依次为标识区(ID 区)、间隙、数据区和间隙组成，如图 2-3。

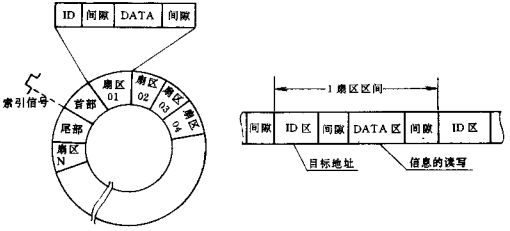

图 2-3　软磁盘的磁道与扇区

标识区用来标识扇区的开始和记录目标地址的信息，数据区用来记录数据，而两个区之间均留有间隙，以保护数据不受盘速变化，机械尺寸，延时误差等等因素的影响。

磁盘的面、磁道和扇区都有固定的编号。以 360KB(千字节)双面双密度软磁盘为例：面的编号是 0 和 1，相应磁头为 0 和 1。磁道的编号为 0 至 39。扇区的编号是 1 至 9。整个软磁盘共有 720 个扇区。

每个扇区不管其长度大小，均存储 512 个字节。所以整个磁盘的存储容量为：

720 个扇区×512 字节＝368640 字节