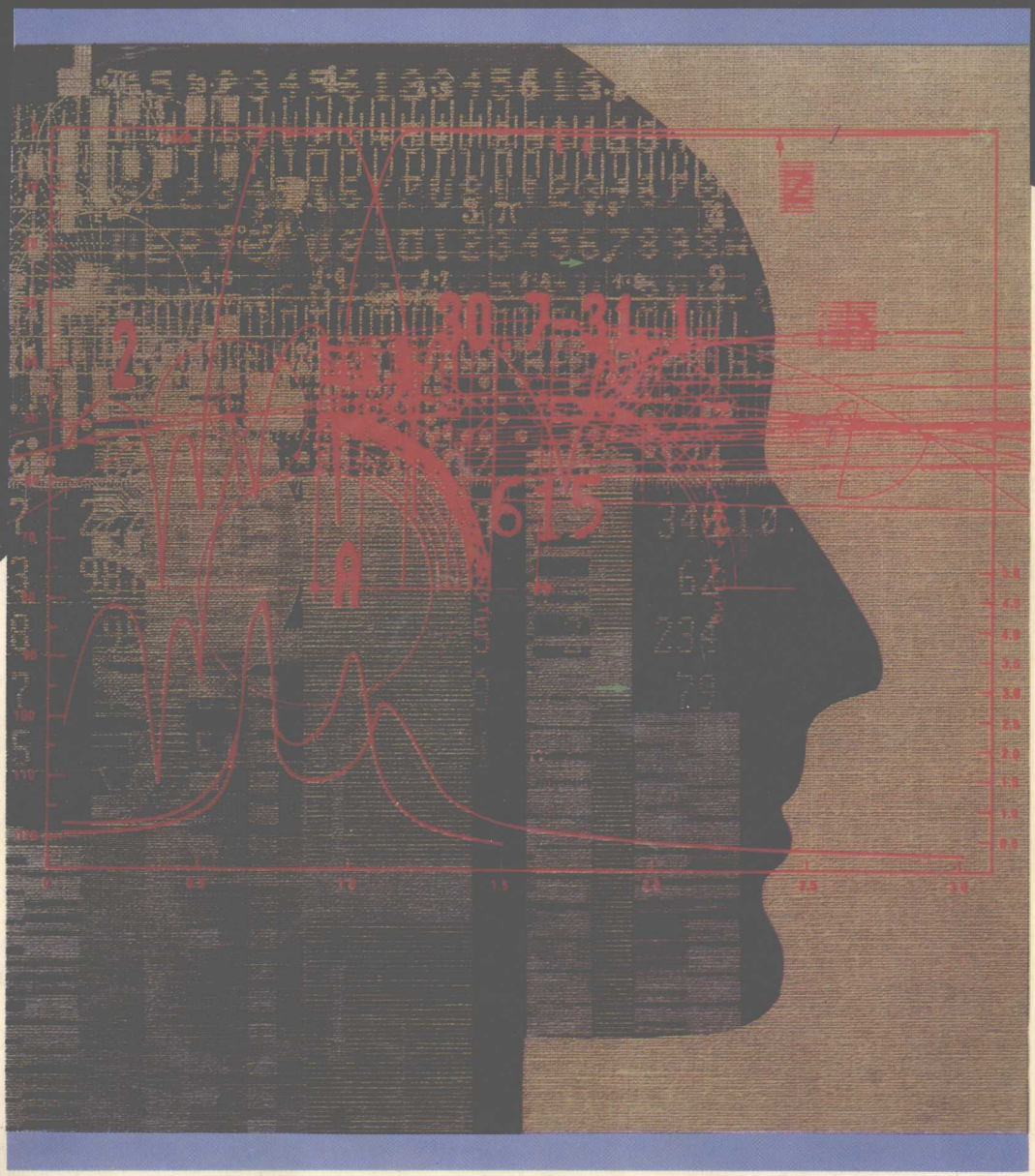
JISUANJI BINGDUDE ZHENZHI JISHU

计算机病毒的诊治技术

● 朱根良 编著



杭州大学出版社

计算机病毒的诊治技术

朱根良 编著

杭州大学出版社

内 容 提 要

本书是一本关于计算机病毒诊治技术的实用手册，主要介绍了计算机病毒概述、常见计算机病毒的症状及其检测和消除工具、计算机反病毒软件技术原理及国内常见反病毒软件的使用方法、计算机反病毒硬件技术原理及国内常见防病毒卡的功能。

本书适合于计算机操作和管理人员、计算机科研人员及大中专师生使用，可以作为了解、预防、检测和消除计算机病毒的参考用书。

计算机病毒的诊治技术

朱根良 编著

*

杭州大学出版社出版发行

（杭州天目山路 34 号）

*

杭州大学出版社电脑排版部排版

杭州余杭人民印刷厂印刷

787×1092 毫米 1/16　12.25 印张　283 千字

1996 年 3 月第 1 版　1996 年 3 月第 1 次印刷

印数：0001—5000

ISBN 7-81035-883-9/TP・034

定价：15.00 元

前　言

计算机病毒自80年代后期出现至今的短短的几年时间里，以其种类、数量出现之多、发展蔓延速度之快、编制技术和手段之高、对各行各业信息所造成的危害之严重，受到了国内外计算机界专业人士的重视，并引起了各行各业计算机用户的关注，纷纷投入大量人力物力进行计算机病毒防治的研究，而且确实也出现了许许多多防治计算机病毒的方法。

为了使广大计算机用户了解计算机病毒，消除他们对计算机病毒的神秘感和恐惧感，而且能使他们掌握一些预防和消除计算机病毒的技术方法，有必要编写一本有关计算机病毒的书籍，以达到以上目的，这就是编写本书的指导思想。

尽管目前已有几本计算机反病毒方面的书籍出版，但由于这些书大多数是从纯技术角度来剖析计算机病毒、并用手工编程的方法来消除病毒，而这对一般的计算机用户专业性要求太高，不易掌握，而且在计算机反病毒软硬件技术发展到一定程度的今天也是不现实的。本书正是从这点出发，从实用的角度介绍了计算机病毒的一些基本知识、计算机反病毒软件的使用方法及反病毒硬件产品的功能。因此，本书一定能对普通的计算机用户带来较大的帮助。

本书共分五章：第一章，计算机病毒概述，介绍了计算机病毒的产生和发展概况；第二章，介绍了计算机病毒的基本概念及其预防、诊断、消除、免疫的一般方法；第三章，常见计算机病毒介绍，介绍了计算机病毒的具体表现症状及可用以检测和消除相应病毒的工具等；第四章，计算机反病毒软件技术及产品介绍，介绍了有关计算机反病毒软件的一些概念，并详细介绍了目前国内常见的一些反病毒软件的使用方法，如Scan/Clean、CPAV、NAV、TNT、F－PROT、KILL、KV200等；第五章，计算机反病毒硬件技术及产品介绍，介绍了计算机防病毒卡的概念及一些国内常见防病毒卡产品的功能。

本书适用于计算机操作和管理人员，也可供大中专学生参考。

本书在编写过程中参考了大量的相关书籍，在此谨向这些作者致谢！

由于作者水平有限，加之编写时间仓促，书中错误和遗漏以及不当之处在所难免，恳请广大专家、同行及读者给予批评指正。

编著者

1995年11月

目　录

第一章　计算机病毒概述

电子计算机自1946年诞生至今已近半个世纪。正当计算机，尤其是80年代初问世的微型计算机及个人计算机在人类各行各业中得到广泛应用，成为人类从个人生活、经济建设到国防事业等不可缺少的工具的时候，计算机"病毒"的降临，对各国造成了不可估量的损失，使计算机用户甚至计算机专业人士产生相当程度的神秘感和恐惧感，也引起计算机界及各国政府的担忧和重视。今天，对计算机病毒的研究已成为重要的课题。

1.1　计算机病毒的产生和发展

1.1.1　计算机病毒的起源

1949年，计算机的创始人、著名数学家冯·诺依曼发表了题为《复杂自动机器的理论与结构》的论文，在世界上第一次描述了程序复制机制的理论，即程序能够在内存中进行繁殖。1957年，冯·诺依曼在由耶鲁大学出版社出版的他的遗著《计算机与人脑》中，又详细讨论了复制程序的理论。但这个理论在当时并没有引起人们的注意。

1959年在AT&T贝尔实验室及加利福尼亚Xerox公司的研究中心，美国麻省理工学院(MIT)的一些研究人员为了娱乐，通过改变公司计算机核心存储组中的代码，设计出具有自我繁殖能力且能在探查到敌方程序运行时销毁敌方程序的程序，这种程序设计方法称为核心战(Core War)。有人认为这是计算机病毒的雏形。后来由于这种程序影响公司计算机的正常运行，于是这种Core War游戏被终止。当时知道这种程序设计方法的人很少，而且这些研究人员也认识到这种具有自我复制能力的程序对计算机应用具有潜在的威胁，因此核心战的概念从此逐渐"沉睡"了。但在1983年，这种程序具有自我复制机理的秘密，被组织Unix操作系统研制和开发并获得图灵奖的Ken Thompson在给计算机协会成员的一次演讲中泄露出去。1984年出版的《科学美国人》杂志详细探讨了Core War及有关编写自我复制程序的信息。这样，有关计算机病毒实现的可能性及原理和设计方法基本上公开化了。这使得一些恶作剧者及恶意攻击者将这种理论付诸于实践，于是就产生了计算机病毒。

在60年代，美国计算机专家John Conway确信能够创建一种具有电子复制机制的"活的软件"(Living Software)，使其能在计算机中活动，并且作了初步的工作。Conway的努力提高了人们对于计算机的利用，这可以说是计算机发展史尤其是软件发展史上的一大成就。但是，Conway的工作又使计算机病毒的发展向前推进了一步。

1975 年，美国科普作家约翰·布鲁纳(John Brunner)出版了一本名为“Shock Wave Rider”(《震荡波骑士》)的幻想小说，该书以 Worm(蠕虫)和 Virus(计算机病毒)为主，第一次描述了信息化社会中计算机作为正义和邪恶双方斗争的重要工具的故事。1977 年，美国著名科普作家托马斯·J·雷恩(Thomas. J. Ryan)出版了一本轰动一时的名为“The Adolescence of P－1”(《P－1 的青春》)的科幻小说。作者构思了一种神秘的、能够自我复制并利用信息通道进行传染的世界上第一个计算机“病毒”。1984 年，威廉·吉伯森(William Gibson)在他出版的小说《Neuromaner》中首次提出了计算机流氓(Cyber punk)的概念。这一概念和弗雷德·科恩(Fred Cohen)对计算机病毒的定义几乎是同时出现的。从此，科学幻想中的计算机病毒在作家的笔下和计算机的现实中得到发挥和实现。

1983 年夏天，美国计算机专家弗雷德·科恩(Fred Cohen) 在完成其博士论文时首次通过实验证明了计算机病毒传染性的可实现性，并于 1984 年在美国国家计算机安全会议上演示了他设计的病毒，并正式将这种具有自我复制能力的程序定名为“计算机病毒”。同年他将病毒演示过程及结果整理成文发表在《国际信息处理联合会文集》中，1987 年 2 月，美国的“Computer & Security”(《计算机与安全》)杂志第一期转载了这篇题为“Computer Viruses: Theory and Experiments”(《计算机病毒：理论和实践》)的论文。

以上是几个对计算机病毒的产生和发展具有代表意义的事件。尽管此时计算机病毒已从科幻走向现实，但绝大多数的计算机专业人士和用户仍认为计算机病毒是个神秘深奥的未知物，不会降临到他们面前。可出乎人们的意料，计算机病毒从科学幻想到大规模泛滥仅用了 10 年时间。

1.1.2 计算机病毒生存和蔓延的原因

计算机病毒的产生是计算机技术及以计算机为核心的社会信息化技术发展到一定阶段的必然产物，其主要原因可归结为以下几项：

1. 计算机软硬件产品具有先天的脆弱性，容易受到病毒的攻击。

电子计算机自 1946 年诞生以来，其硬件系统结构大多采用冯·诺依曼体系，即：一个计算机硬件系统由运算器、控制器、存贮器和输入/输出设备五个部分组成。在这种体系结构中，命令和数据被同等对待，并可动态地对它们进行修改，以满足变化的需要。计算机硬件是电子产品，具有易于修改和更新的特点，在输入、存储、处理和输出数据的过程中极易发生误入、篡改、丢失、作假和破坏等问题。至于计算机软件，它不但容易被修改、删除，而且有了错误很难发现。大多数程序都是手工编制的，而且往往相当复杂，难以保证没有错误，而尤其令人遗憾的是至今还没有一种方法可以查出程序中的所有错误。另外，现在的计算机系统往往结构庞大，且由于采用超大规模集成电路使得构造复杂，隐藏几个错误或者说病毒可以说是大海里藏针，很难发觉和查找。

2. 简单透明的微型计算机的普及诱发了计算机病毒的流行。

70 年代末 80 年代初问世的微型计算机，尤其是 IBM PC 系列微型计算机，由于其性能优良，价格便宜，发展潜力大，深受广大计算机用户的欢迎，也将计算机的应用推向一个高潮。但是由于 IBM PC 系列微型计算机及其兼容机系统自身的弱点，尤其是它所采用的操作系统 IBM PC DOS (MS－DOS)的开放性，使有计算机技术基础的人几乎无需花费多

大力气即可透彻地了解其内部结构，给计算机病毒制造者提供了可乘之机，从而使 IBM-PC、AT286、386、486 等兼容计算机成为计算机病毒攻击的主要对象。又由于操作系统程序和用户程序及数据在计算机内存中均被当作数据处理，并可以动态地对他们进行修改，使得计算机病毒利用这个特性来达到传染的目的，于是酿成了计算机病毒的大流行。

众所周知，DOS 操作系统是安全性与易操作性的一种折中。从计算机用户的角度来看，DOS 是一个相当友好的系统，它赋予用户极大的自主权力——用户可以修改 DOS 操作系统，从而便于用户扩展系统功能。DOS 的 FAT(文件分配表)，FDT(文件目录表)，中断向量表等对用户都是透明的，DOS 为用户提供了一些便于用户编程的中断服务程序。利用它们用户可以编写程序使其常驻内存，甚至用户可以修改 ROM 的中断功能；用户可以编写 SHELL(外壳)程序代替 DOS 的命令解释程序 COMMAND. COM；如果用户具有更高的技术层次，甚至可以修改 IBMBIO. COM 和 IBMDOS. COM 两个低层模块。因此，从安全性的角度来看，DOS 结构的各个层次均可以受到攻击，DOS 不是一个很好的安全操作系统。正是由于 DOS 操作系统本身存在的这些固有的脆弱性成为当今计算机病毒攻击的一个原因。也正因为此，计算机病毒与微型计算机几乎同步流行决不是时间的巧合，而是由于它们本来就有着密不可分的内在联系。

3. 一些国家和地区不尊重软件产权，没有软件产权保护法，或是有法不依，私自复制他人软件程序，促进了计算机病毒的产生和传播。

软件是计算机公司花费了大量人力和物力而编制成的程序，凝聚着软件开发人员的辛勤劳动。由于软件产品得不到适当的法律保护，软件制造商设计和开发的软件产品被大量地非法拷贝，使其利益蒙受巨大损失。为了防止自己开发的软件被非法拷贝，他们在自己开发的软件系统中加入了用以惩罚非法拷贝者的，可以传染并具有一定破坏作用的计算机程序。后来人们猜测，可能是软件开发者为保护自己的利益而从事的恶作剧性的工作，逐渐演化成了危及社会的计算机病毒。因此，有些计算机用户在窃取了他人程序时千万不要自以为得计，一旦染上了计算机病毒，轻则浪费了自己的计算机系统资源，重则使自己的系统全面崩溃。

4. 计算机犯罪日益猖獗，计算机病毒巨大的破坏力对惟恐天下不乱的歹徒有着强烈的诱惑力。

计算机犯罪本来就是一种高技术犯罪，具有隐蔽、不易取证和不易侦破等特点。而利用计算机病毒犯罪是一种最严重的计算机犯罪，它风险小，破坏力大，从而更刺激了某些高技术罪犯的犯罪意识，成了这些人恶作剧和报复心态的表现方式。当今世界上传染、流行的计算机病毒已有几千种，虽然计算机用户已摆脱了对计算机病毒的神秘感，却又陷入了被计算机病毒的困扰之中。通过计算机病毒进行犯罪的手段主要有诈骗、勒索、实施政治及人身攻击、泄愤等。据《参考消息》1989 年 8 月 2 日刊登的一则评论称：计算机病毒将成为 21 世纪国际恐怖活动的五种新手段之一，并名列第二。另外，计算机病毒还有可能被应用于军事目的，成为现代战争的实用武器。总之，计算机病毒已成为计算机犯罪的一个主要工具，从而刺激罪犯制造和传播更多的计算机病毒。

1.1.3 计算机病毒的来源

1. 显示超群智力

有些计算机专业人员和业余爱好者，为了炫耀个人“非凡”的本领，恶作剧地设计和制造了一些病毒。例如像圆点一类的良性病毒就是这样产生的。

2. 对付非法拷贝

软件公司或用户为了保护自己的软件不被非法拷贝，设计了一些报复和惩罚性的病毒。他们发现对软件加锁不如在其中隐藏病毒，这样对非法拷贝者打击大，于是就在自己的程序中有意制作病毒。典型的例子是巴基斯坦病毒的产生。

3. 利用病毒进行犯罪

如前所述，计算机病毒已成为计算机犯罪的一个重要工具。这种具有犯罪目的性的计算机病毒以后会越来越多。

4. 利用病毒从事政治、军事目的

国家、部门和个人为了摧毁敌国、敌方或他人的计算机系统，蓄意制造了某些病毒。1989 年 11 月在澳大利亚军方举行的一次军事演习中，红方使用了新西兰病毒来破坏对方计算机系统的正常运行，并在演习中占尽优势。这是人类历史上第一次有关计算机病毒用于军事目的的报道，从而揭开了软件形式的计算机战争的序幕，人类也终于将面对计算机战争的威胁。

据 1990 年 5 月 8 日来自纽约的消息称：美国国防部悬赏 55 万美元征集可以用于摧毁敌方计算机系统的病毒。

1991 年海湾战争中，美军第一次将计算机病毒用于实战。在空袭巴格达的战斗中，成功地破坏了对方的指挥通讯系统，并使之瘫痪，保证了战争的顺利进行直至取得最后胜利。

5. 其他来源

有些人为研究或出于有益目的设计的计算机程序，不慎由于某种原因失去控制而演变成了病毒。不过这种病毒一般为良性病毒。

1.1.4 计算机病毒发展概况

1.1.4.1 国外计算机病毒发展概况

在 1977 年至 1987 年的 10 年间，计算机病毒从科幻变成现实。

1977 年，美国科普作家 Thomas · J · Ryan 的科幻小说《P－1 的青春》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，并控制了 7000 台计算机的操作系统，最终酿成一场灾难。

1980 年，深受广大计算机用户欢迎的 IBM PC 系列微型计算机，由于其采用的 DOS 操作系统自身的弱点，成为计算机病毒攻击的主要对象，也成为造成计算机病毒大流行的主要原因。

1985 年，巴基斯坦拉哈尔(Lahore) Brain Computer Service 商店的两兄弟 Amjad Farooq Alvi 及 Basit Farooq Alvi 为保护自己的软件产品编制成功了巴基斯坦智囊病毒，到

1986 年该病毒在全世界广泛传播。

1987 年 5 月，美国罗德岛《普罗威斯顿日报》编辑部发现存储在计算机中的文件变成了如下字符串："欢迎进入土牢，请小心病毒，如需疫苗，请与我们联系。XXX 与 XXX 敬上，帕金斯坦尼电脑公司。"当专家进一步追查时，发现该病毒程序早已广泛传播，遍布于该报社计算机网络系统的各个结点。

1987 年 10 月，在美国本土发现 Brain 电脑病毒，并以强劲的势头迅速蔓延。同时在 Lehigh 大学发现 Lehigh 病毒。同年 12 月，一份电子邮件给 IBM 公司传送了一份能自我繁殖的圣诞祝贺程序。每当用户显示内容时就以链式反应的方式自我复制到用户的收件人目录下，最后导致网络拥挤，部分停机。这就是 IBM 圣诞树蠕虫病毒。

1988 年，各种计算机病毒开始大肆流行。3 月 2 日，早已潜伏并广泛散布于苹果机的 MacMag 病毒发作，被感染的苹果机均显示"MacMag 的出版人及其全体同仁，借此机会高兴地向所有苹果机用户转达世界和平的信息"，以庆祝苹果机的生日。5 月 13 日，黑色星期五病毒于以色列被发现。该病毒是为抗议于该日举行的以色列国成立 40 周年而设计的具有政治目的的病毒。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的康乃尔大学。该大学年仅 23 岁的一年级研究生罗伯特·T·莫里斯(Robert·T·Morris)制作了一个蠕虫计算机病毒(Tap Worm)，并将其投入美国重要的计算机网络 Internet 中。该病毒从 11 月 2 日上午 5 点开始发作，到下午 5 点已使联网的 6000 多台计算机工作站受到感染。虽然该病毒程序并不删除文件，但无限制地繁殖抢占了大量的计算机时间和空间资源，使许多联网计算机被迫停机。据报道，该事件造成的直接经济损失达 9000 多万美元，莫里斯也因此受到法律的制裁。莫里斯的蠕虫事件引起了美国全社会和计算机界的震惊，专家们在有关法律、道德、反病毒技术等方面发表了大量的评论，许多公司、研究所也纷纷发表道德宣言，表示要教育职工、学生不制造也不传播计算机病毒。翌年初，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。

1989 年 10 月 13 日，星期五，"黑色星期五"病毒在长期潜伏、广泛传播后，在全世界数十万台运行 DOS 的微机上发行。在这天，每运行一个文件，则被删除一个，许多微机用户被迫停机，所造成的损失难以估计。因此，对计算机界人士而言，这是灾难性的一天。

1.1.4.2　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：

(1)出国技术人员回国时带回的应用软件或游戏盘带入。

(2)由国内某些计算机界人士改写国外的计算机病毒或自己制造病毒。如"广州一号"即为修改"大麻"病毒而形成的变种，而"Bloody/6.4"及"大连"等病毒则是土生土长的国产病毒。

2. 计算机病毒在国内蔓延情况

1989 年上半年，小球病毒在我国计算机上被发现，从此计算机病毒以其迅猛之势在中国大陆蔓延。

1989 年秋，北京、上海、福建等地有关部门开展了计算机病毒的情况调查。结果表明，大约有 50%以上的计算机染有病毒，而且这些病毒主要的攻击对象为 IBM PC 系列微机及其兼容机。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“计算机犯罪及计算机病毒研究”等问题。同月，《中国日报》报道：我国约有 4 万台以上的计算机系统染有病毒，而且在沿海各省市传播的范围远比内地广泛得多。

“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”被评为 1989 年我国计算机界十大事件之一。

与此同时，国内许多高等院校、科研机构纷纷组织技术人员，研究反病毒软件，其中最具有权威性的为中华人民共和国公安部的 SCAN 系列病毒扫描软件及 KILL 系列的病毒清除软件。

此后的几年中，计算机病毒的蔓延没有受到明显的扼制。“大麻”、“黑色星期五”、“米氏”、“FLIP”、“DIR－2”等病毒先后侵入我国，给我国的计算机应用造成很大的破坏，给我国的经济造成很大的损失。

随着国外软件的大量引进和计算机技术的日益普及，计算机病毒正以惊人的速度在国内扩散。由于国情所限，非法复制的软件大量流传，给计算机病毒以相当大的传播机会。目前，全世界计算机病毒的总数已达几千种甚至可能已超过一万种，而流入国内的病毒也已超过千种，且多为传染性强、隐蔽性好、破坏力大的恶性病毒。由此可见，在未来的日子里，计算机将不断面临“病毒”的挑战。

第二章　计算机病毒的基本概念

2.1　计算机病毒的基本概念

2.1.1　计算机病毒的定义

任何一学科中的任何一个名词一般都有其特定的内涵和外延，计算机病毒也不例外。由于计算机病毒与生物学（或医学）中的病毒具有相似的一些特性，于是人们就认可了Len Adleman从生物学（或医学）中借来的“病毒”这个名词，在计算机领域确立了“计算机病毒”这一概念。但由于计算机病毒是一组程序编码，有其特定的内涵和外延及自身的特性，其定义应该反映其所有特性，因此在给计算机病毒下定义时应该注意以下几点：

（1）包含有计算机病毒的一组指令可以有不同的形式，通常它能包含软件中的程序指令、硬件指令，或包含远程通讯信息中的控制字符参数或作业控制语言等等，因此计算机病毒的定义不应局限于传递病毒的某种特定的介质之上。

（2）由于病毒可以在少数或许多软件系统中进行自我复制，繁殖出与先前版本形式相异内容不同的指令集合，也即计算机病毒能够随时间的推移而发生变化，因此，计算机病毒的定义不应局限于病毒所采取的繁殖形式上。

（3）有些计算机专家把破坏系统资源或严重影响系统运行环境的病毒称为“恶性病毒”，反之则称为“良性病毒”。也就是说，他们试图根据病毒所造成的危害程度来区分病毒的“良性”和“恶性”。但实际上，即使是所谓的“良性病毒”也要消耗系统的存储空间并占用系统的运行时间，做一些令人难以对付的事情。尤其由于在已有的病毒程序中添加一些代码比编制一个新的病毒程序更加容易，因此病毒程序的设计者可以在现有的一些“良性”病毒中添加一些有较大危害性的代码，使病毒发生变异，从而使病毒的破坏性发生根本变化，使计算机病毒内所谓的“良性”转化为“恶性”，而且新生成的病毒给系统所造成的后果往往比原版病毒所造成的后果更为严重。因此，计算机病毒的定义不应局限于病毒的表现形式和破坏程度上。

（4）计算机病毒的传染性是计算机病毒的一个主要特性。病毒对不同的传染对象可以采用不同的形式或方法。因此，计算机病毒的定义也不能仅着眼于病毒的传染形式或方法上。

（5）应区分计算机病毒与程序错误（即臭虫BUG）的概念。根据程序错误的定义，程序错误一般不是蓄意造成的，而是由程序本身、程序运行环境及误操作等造成的，而计算机

病毒一般总是人为故意制造用来破坏某个或某些计算机系统的。

对计算机病毒至今尚未有一个统一的定义。综合以上各点，我们认为一个比较科学的定义应该是：计算机病毒是一种人为制造出来的寄生于应用程序或系统的可执行部分，并等待时机利用它们进行自我繁殖和传染，危及计算机系统正常运行、浪费系统资源、破坏所存储数据的计算机程序。

2.1.2 计算机病毒程序的基本结构

通过对计算机病毒程序的剖析，我们发现计算机病毒在其结构上存在着共同性，它主要由以下几部分组成：

(1)引导部分：这部分程序随着宿主程序的执行使病毒进入内存而获得系统控制权。

(2)传染部分：这部分程序一般包括传染的判断条件和完成病毒与宿主程序连接的病毒传染主体部分。病毒是否要传染由传染的判断条件决定。通常病毒的判断条件中还包含有判断病毒自身是否已传染了病毒自身的病毒标识。一旦传染的判断条件满足，传染部分则通过一系列的非法操作将其自身感染到宿主程序，使之成为新的传染源。这部分反映了病毒最本质的特征，因为离开传染机制就不能称之为病毒。

(3)破坏和表现部分：这部分包含有破坏或表现的判断条件部分(用以判定是否破坏、表现及什么时侯破坏、表现)及破坏被传染系统或在被传染系统的设备上表现特定现象(如在系统的显示器上显示特定的信息或画面，蜂鸣器发声等等)的程序部分。这部分是病毒程序的主体，它在一定程度上体现了病毒设计和制造者的目的。

综合以上三部分，我们可以构画出计算机病毒程序的整体结构，如图 2-1 所示。

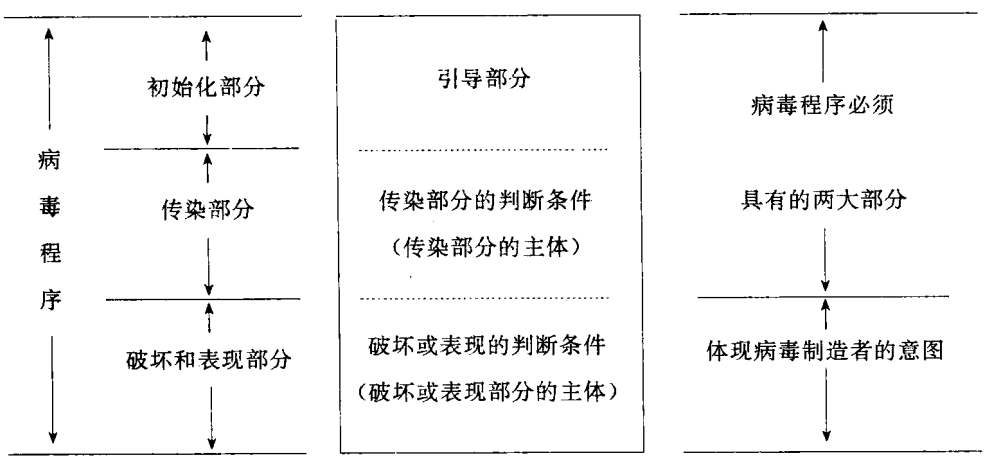


图2-1 计算机病毒的整体结构

2.1.3 计算机病毒的寄生及其寄生环境

为了便于读者理解，本书采用寄生概念，它和读者在其他书上所看到的宿主概念的意义完全一样。