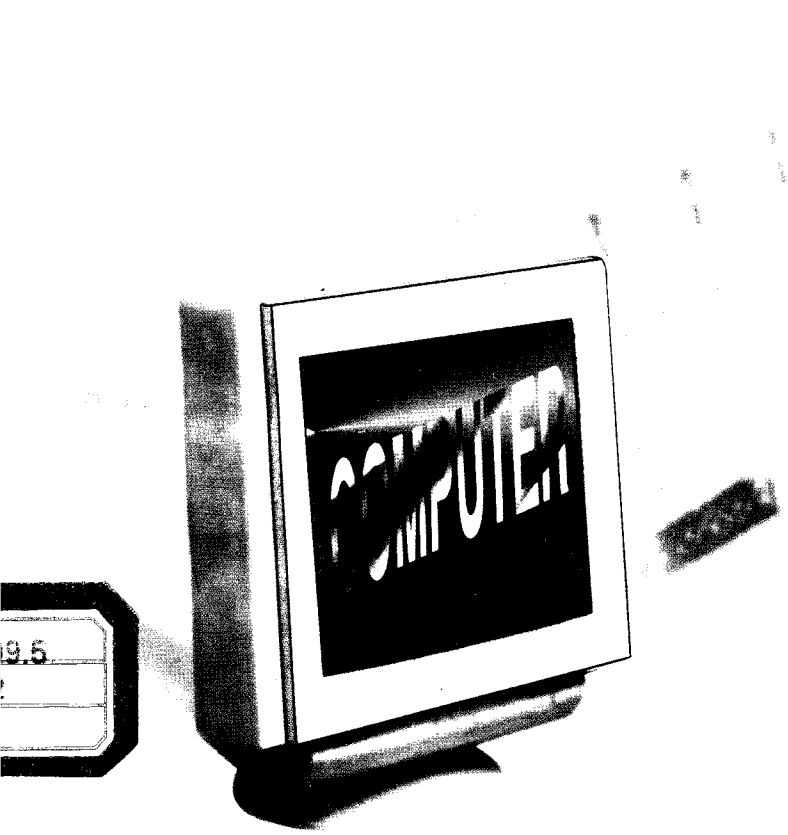
计 算 机 系 列 教 材

计算机病毒防治教程

陈宝贤 主编



中国商业出版社

国内贸易部部编计算机系列教材

计算机病毒防治教程

陈宝贤　主编

中国商业出版社

图书在版编目（CIP）数据

计算机病毒防治教程/陈宝贤主编．
－北京：中国商业出版社，1998.9
ISBN 7-5044-3502-3
Ⅰ．计…　Ⅱ陈．　Ⅲ．计算机病毒-防治-教材
Ⅳ．TP309

中国版本图书馆 CIP 数据核字（98）第 23094 号

责任编辑：陈李苓

中国商业出版社出版发行
（100053　北京广安门内报国寺 1 号）
新华书店总店北京发行所经销
北京星月印刷厂印刷
*
850×1168 毫米　32 开　5.625 印张　144 千字
1998 年 9 月第 1 版　1998 年 9 月第 1 次印刷
定价：8.00 元
*　*　*　*

编审说明

为适应建立社会主义市场经济新体制的要求，我部于1994年颁发了财经管理类5个专业和理工类7个专业教学计划。1996年初印发了以上12个专业的教学大纲。《计算机病毒防治教程》一书是根据计算机应用专业学生培养目标和教学任务的要求，结合我国科技进步和财税、金融等体制改革的情况重新编写的。经审定，现予出版。

本书由陈宝贤任主编，李中发、曹翌旺、高文义任副主编。具体编写分工是：陈仲培（第1章）、陈宝贤（第2章）、李中发（第3章）、曹翌旺（第4章）、高文义（第5章）、吴一凡（病毒问答）。最后由陈宝贤、李中发总纂定稿。

由于编写时间仓促，编者水平有限，书中难免有疏漏之处，敬请广大读者不吝赐教，以便于修订，使之日臻完善。

国内贸易部教育司

1996年8月

目　录

第一章　计算机病毒发展史及计算机犯罪

计算机技术的迅速发展，极大地促进了人类社会的现代化进程，20 世纪 80 年代以来计算机网络不断扩大，为人类社会的信息交流提供了便捷的途径。计算机应用已在社会各个领域广泛普及。计算机系统已能实现对生活、管理、办公的自动化，产生智能决策信息，从而使整个社会走向计算机化。各种各类的计算机信息系统亦逐步成为国家和政府机构运行的有力工具，成为社会活动信息处理的支柱。计算机信息产业已成为无形的巨大的新的社会资产，有的专家称之为计算机资产。

计算机技术发展，可谓一日千里，给人类社会带来了巨大财富。同时在这发展过程中，由于计算机系统本身的脆弱性，引出了必须十分注意的计算机安全问题。计算机病毒的产生、发展，对计算机系统的攻击，给广大用户带来了不可估量的损失。本章将简述计算机病毒的发展情况，以及相关的计算机犯罪与计算机安全问题。

第一节　计算机病毒的发展简述

至今计算机病毒的泛滥，给人类社会带来了巨大的心理压力。计算机新病毒的不断出现，真是形形色色，防不胜防，使得许多计算机使用者弄不准自己手中的软件是否已带上病毒，自己使用的计算机系统不知什么时候会有哪种病毒会发作。认识病毒，判断是否存在病毒，及时解毒杀灭病毒已成为计算机技术中一个重要课题。

一、计算机病毒的起源及发展趋势

计算机病毒的起源至今还没有一个被确认的说法，但是都一致认为计算机病毒的发源地是在美国。

1．科幻小说中病毒的构思

许多人都认为计算机病毒在1983年前已经存在，但现在我们所见到的在此以前仅仅是计算机病毒的设想。

1975年，美国科普作家John Bruner（约翰·布鲁勒尔）在其编写的一本名为《Shock Wave Rider》（《震荡波骑士》）的书中，以Worn和Virus描述了用电脑作为正义和邪恶双方斗争的工具的故事。

1977年，美国Thomas.J.Ryan（托马斯·简·雷恩）在其编写的一本名为《The Adolescence of P－1》（《P－1的青年》）的书中，构思了第一个计算机病毒，病毒能够自我复制，利用信息通道传播，能控制7000台电脑的操作系统，造成了人类社会巨大的恐慌与动荡。

2．实验演示证明计算机病毒的存在

早在半个世纪以前，计算机理论的奠基人冯·诺依曼提出了复杂机械的自动复制理论，指出了计算机程序能够在内存中自我复制的机制。

20世纪60年代初期，美国电报电话公司贝尔实验室的一些年轻研究人员，在工作之余，常常在实验室饶有兴趣地玩一种他们自己创造的计算机游戏。游戏的玩法是由每人编制一段小程序攻击对方的程序，设法毁掉对方的程序。这种被称为“达尔文”式的游戏的程序，后来有人认为就是计算机病毒的雏形。

1983年计算机界才确认计算机病毒存在。该年11月3日的美国计算机安全学术讨论会上，美国计算机安全专家Frederick Cohen博士首次提出计算机病毒的概念。就在这一天，专家们在运行UNIX操作系统的VAX11/750计算机系统上验证了计算机病毒的存在。在其后的一周内，在5次病毒试验中，病毒使计算

机系统瘫痪所需的平均时间仅为30分钟。由此确认了计算机病毒的存在，并且认识到计算机病毒可在短时间内实现对计算机系统的破坏，并具有迅速传染的特性。

3. 早期发现的计算机病毒

1987年美国和欧洲一些发达国家出现病毒对计算机系统入侵及引起破坏。1987年秋，计算机病毒开始受到新闻机构的关注和报道。在美国，仅1988年中，约有9万台计算机遭计算机病毒入侵。

1987年2月，美国东部一医疗中心计算机系统发现病毒，存储的全部病历突然莫名其妙地消失。

1987年9月美国加利福尼亚的阿拉梅达学院发现阿拉梅达(Alameda)病毒攻击计算机系统。

1987年11月宾夕法尼亚的利哈依大学发现利哈依病毒(COMMAND.COM病毒)。

1987年12月以色列希伯莱大学发现黑色星期五病毒和四月一日病毒（又称愚人节病毒)。

1987年12月IBM公司的国际电子信息网受IBM圣诞树病毒攻击，向计算机用户发出大量的节日祝贺信件，致使该大型计算机网络不堪重负而瘫痪。

1988年3月2日所有苹果（APPLE）牌号的微机开机后屏幕上自动出现一条和平信息，接着程序自动毁坏。

1988年8月苏联政府机构的计算机网络发现了3类病毒入侵。

1988年9月日本电气公司联网的PC－VAN网发生计算机病毒入侵用户计算机。

4. 计算机病毒流行

1988年11月3日，美国国防系统的洲际Internet网络遭到蠕虫病毒的攻击。该病毒利用UNIX系统中的电子邮件的脆弱性侵入网络，并在网络中不断自我复制，以闪电般的速度向整个网络蔓延，一夜之间网中的6200台VAX系列小型机及SUN工

作站都感染上病毒，致使整个网络系统遭到堵塞而瘫痪，损失约9200多万美元。为此，病毒程序的制作者Morris（莫里斯）作为被告而走上法庭。从此，在国际计算机领域掀起了一个谈论病毒的高潮，一时成为计算机界的热点。大家公认1988年为世界计算机病毒年。

自1980年以来，计算机病毒不断出现、泛滥，这些病毒以极快的速度传遍全球各地。据美国统计，1988年12月遭受计算机病毒攻击的用户数为30000户，1987年7月遭病毒攻击的用户数为50000户，1987年至1989年间发现的计算机病毒有80余种。

国外有人估计，目前计算机病毒的传染范围每两个月增加一倍，每3个月需对原有杀病毒软件升级一次。1989年MCAtee公司推出VIRUSSCAN抗病毒软件时声称，可检测并消除52种病毒。1997年又推出最新版本SCAN301.EXE。美国Central Point Software公司研制的CPAV杀防病毒软件，早期可检测和消除395种病毒，最近新版本可检测和消除1009种病毒。

1991年美国第一次将计算机病毒用于海湾战争，在空袭巴格达战争中，成功地破坏了对方的指挥通讯系统。

1994年5月，国际电脑安全协会主席大卫·斯丹博士在一次学术会上说，至今已发现的计算机病毒达5000多种。

目前，又有一些被称为“第二代病毒”的新病毒正在蔓延，它们不占用任何内存，也不盗用或修改任何系统数据和其他资源。例如，傻瓜病毒具有很强的传染性，既可传染可执行文件，又可传染隐含扇区，病毒标志很特别，不改写任何中断。计算机病毒的蔓延正朝着病毒变体和智能化的方向演变，已进入隐蔽状态，并有向恶性计算机病毒方向发展的趋势。

二、计算机病毒入侵我国及现状

1988年11月，《人民日报》就Morris事件3次刊载有关病毒的文章。

1989 年 4 月，我国西南部某铝厂的计算机首次发现小球病毒。同年夏天，上海一些单位的计算机也发现小球病毒及其变种。1989 年 8 月，福建发现小球病毒、硬盘病毒及其变种。

继发现小球病毒入侵以后，相继又发现大麻病毒、巴基斯坦病毒、维也纳病毒、1701/1704 病毒等几十种病毒。计算机病毒迅速蔓延至全国各地区。

1989 年在广州发现国产的计算机病毒“中国病毒 001 号”，在西安发现“中国炸弹”病毒。中国炸弹病毒侵入某省计委计算机系统，造成该计委计划经济研究室 1949 年以来有关计划指标及经济数据的破坏，带来不可弥补的损失。

1989 年 4 月以后，《计算机世界》、《计算机信息报》、《科技日报》等报刊相继载文报道计算机病毒的情况。据公安部计算机安全监察司的不完全统计，截至 1990 年 8 月底全国 40 万台微机约有 30 多万台受到过计算机病毒的感染，使许多单位蒙受了严重的损失。

目前，国外流入的计算机病毒已达百种之多，国产病毒也有数十种。据有关部门的统计，到 1995 年上半年我国发现的病毒已达 200 多种。

20 世纪 90 年代初，我国研究出多种防病毒卡，影响较大的有华星、瑞星、华能等牌号。1993 年发明硬卡在线升级技术，原电子工业部信息中心求真实验室开发了求真可升级消病毒卡。目前，广为使用的杀病毒软件有金辰安全实业公司开发的 KILL 杀毒专用程序。该软件具有较好的软硬件兼容性，受到广大用户好评。

第二节　计算机犯罪及相关社会问题

计算机技术的发展促进了社会的现代化、信息化，计算机已成为今日社会信息处理的现代化设备和重要工具，计算机信息系统已形成了一种新的社会资产，计算机资产是一个单位、一个国

家的重要战略资源。

一、计算机犯罪

计算机犯罪开始于计算机开始推广应用于社会的40年代末期。1966年首次对一起篡改银行数据的计算机犯罪案件提出起诉，引起社会对计算机犯罪的重视。80年代计算机病毒蔓延，给计算机系统及社会带来了严重危害，计算机病毒是计算机犯罪的一种衍化形式。

计算机犯罪是以计算机为工具或以计算机资产为对象实施的犯罪行为。计算机犯罪是高技术智能性犯罪，作案时间短、隐蔽性强、变化多端、破坏性大、蔓延迅速、地域广、涉及面宽。

二、计算机犯罪对社会的危害

计算机犯罪的手段从简单到复杂、高级，犯罪的手段有计算机病毒、非法访问系统、系统固有的弱点、系统支持软件的问题、电话窃听、电磁辐射等。计算机犯罪除了少数是计算机系统的硬件故障及软件技术造成的犯罪以外，大量是人为参与引起的。从构成犯罪的条件以及犯罪效果上看，计算机病毒是计算机犯罪中危害最严重的犯罪手段。

计算机犯罪对社会构成的危害主要有以下几个方面：

(1) 计算机系统及所在机房，由于抵御意外事故的能力较差，而发生对计算机系统设备损坏，数据丢失，造成不可挽回的损失。

(2) 计算机犯罪人员非法窃用计算机系统。

(3) 计算机犯罪人员非法获取数据，窃取机密，倒卖获利，损害合法用户以及计算机公司的资源权益。

(4) 采用恶劣手段，袭击破坏计算机系统。

(5) 研制、传播计算机病毒，干扰计算机系统的正常运行，危害计算机系统中信息资源。

(6) 采用非法手段，编制诈骗程序，篡改数据，输入假数据，非法获取利益。

计算机犯罪发案率的上升，危害领域已涉及金融、邮电、科研、生产、管理等各个领域。计算机犯罪的社会化，被一致认为已成为人类社会的一大公害。据有关方面统计，美国每年因犯罪而遭受的经济损失超过百亿美元；计算机犯罪正以400%的趋势高速发展。

三、计算机道德与安全教育

面对形形色色的计算机犯罪现象，在计算机时代和“计算机文化”的新时期，有必要形成一整套计算机道德规范。计算机道德包括如下内容：

(1) 加强对计算机人员以及计算机用户对计算机文化的正确认识，从根本上杜绝计算机犯罪行为的发生。

(2) 加强计算机安全意识的教育及计算机职业道德规范的训练，防止计算机犯罪的发生，阻止可能发生的蓄意犯罪行为。

(3) 尊重计算机工作人员的劳动，承认其社会价值，保持其合法权益。

(4) 提倡钻研业务，提倡奉献精神，正确对待个人、集体、国家利益。

(5) 建立计算机法律规范准则。

计算机文化的含义包括：计算机知识产权、计算机道德、计算机安全法律。因而开展计算机安全教育是使全社会计算机文明与社会发展相适应的一个重要方面。通过计算机安全教育，应达到以下目的：

(1) 要认识到计算机的先进性与高效性，又要看到计算机存在的脆弱性与危险性可能给社会带来的严重威胁。

(2) 使计算机人员及用户对计算机安全有全面的了解，重视发展计算机安全技术和计算机安全措施。

(3) 要充分认识到保证计算机应用系统取得效益的关键，是提高各级人员对计算机安全的重要性的重视。

(4) 要从管理上、技术上防止计算机犯罪行为发生。

第二章　计算机病毒概述

第一节　计算机病毒的定义及其特征、结构

一、计算机病毒的定义

目前，对计算机病毒尚未有一个公认的定义。在生物学中，病毒是指侵入动物体，具有传染性、潜伏性，并对动物体带来疾病的微生物。“计算机病毒”一词是人们联系到破坏计算机系统的“病源体”具有与生物病毒相似的特征，借用生物学病毒而使用的一个新的计算机术语。计算机病毒实际上是一种“带毒的程序”，它能在计算机系统中繁殖、生存、传播，对计算机系统资源及运行造成严重的破坏。

美国计算机安全专家 Frederick Cohen 博士于 1983 年首次提出计算机病毒存在。他认为：计算机病毒是一个能传染其他程序的程序，它靠修改其他程序，并把自身的拷贝嵌入其他程序而实现病毒的传染。1989 年，他进一步将计算机病毒定义为：“病毒程序通过修改（操作）而传染其他程序，即修改其他程序使之含有病毒的精确版本或可能的演化版本、变种或其他的病毒繁衍体。病毒可看作是攻击者愿意使用的任何代码的携带者，病毒中的代码可经由系统或网络进行扩散，从而强行修改程序和数据。”

美国计算机安全中心编制的《计算机安全术语汇编》中对计算机病毒的注释为：“计算机病毒是一种自我繁殖的特洛伊木马，它由任务部分、触发部分和自我繁殖部分组成。”

《计算机信息报》刊登的有关计算机病毒的描述为：计算机病毒是一种程序，一般包含引导模块、传播模块和破坏及表现模

块。引导模块将病毒由外存引入内存，使后两个模块处于活动状态。当病毒触发的条件满足时，传播模块将病毒传染到其他对象上，破坏及表现模块实施病毒的破坏作用。

二、计算机病毒的特征

计算机病毒的基本特征是具有传染性、破坏性、潜伏性和诱发因素。从本质上讲，任何一种计算机病毒均是一段较小的可执行的程序。这类病毒程序一般都不大于 4K 字节长，隐蔽在合法程序中，当计算机程序运行时，与合法程序争夺系统控制权，对计算机系统实施干扰和破坏作用。从第一例计算机病毒的发现，至今计算机病毒的流传、繁殖非常迅猛，形成了形形色色的、各种类型的病毒。计算机病毒具有以下一些共同特征。

1．传染性

计算机病毒的传染性是所有病毒程序都具有的重要特性，是衡量一种程序是否为病毒程序的首要条件。传染性是计算机病毒的再生机制，病毒程序通过修改磁盘扇区信息或文件内容，并与系统中的合法程序链接在一起达到计算机病毒的传染。运行被传染的程序，病毒就会很快地传染到计算机系统。计算机病毒的传染是指病毒由一个系统扩散到另一个系统，或由一个网络传入另一个网络系统等的过程。例如，病毒程序写入硬盘，就称该硬盘或这台计算机感染了病毒；如果病毒程序写入软盘，那么这张软盘也感染了病毒，带有计算机病毒的磁盘称为带毒盘。

计算机病毒的传染性与计算机系统的兼容性有关。一台微机带上病毒，能够很快传染给不同国家地区、不同单位的成千上万台微机系统。计算机病毒亦可以在一个局部网络上快速传染。

另外，计算机病毒的传染是有针对性的，目前发现的计算机病毒有针对 IBM PC 机及其兼容机的，有针对 Apple 的 Macintosh 系列机的，有针对 Unix 操作系统的等。

2．隐蔽性

计算机病毒程序都较小，而且一般都寄生在正常程序中，许

多病毒都采用特殊的隐身技术，传染正常程序时将程序文件压缩，留出空间嵌入病毒程序，这样使被感染病毒的程序文件的长度的变化很小，很难被发现。计算机病毒的传染过程一般不具有外部表现，大多数病毒的传染速度极快，这种传染的隐蔽特征使得病毒很容易侵入其他计算机系统而不被用户发觉。

3. 潜伏性

计算机病毒的潜伏性是指病毒依附于计算机磁介质而寄生的能力。计算机病毒侵入系统后，一般并不是立即发作的，而是具有一定的潜伏期，有的病毒潜伏期为几个星期，有的可以达几年。在潜伏期，只要条件许可，计算机病毒就会不断地进行自身复制、繁衍、传染。

4. 破坏性

计算机病毒的破坏性是指对计算机系统带来危害，其破坏性取决于病毒程序设计者的意图。所有的计算机病毒都会使计算机系统的工作效率降低，甚至瘫痪。有的病毒可以篡改系统的某些数据，使系统信息处理的结果面目全非；有的病毒可以毁掉系统内的部分数据或全部数据，给用户带来无法估量的损失；有的病毒虽不破坏系统内的数据，但干扰系统的正常运行。

由于计算机病毒具有破坏性，对于带病毒的计算机系统必须采取有效的检测措施，进行有效的杀毒工作，以最大限度地减少病毒给系统带来的损失。

5. 诱发性

计算机病毒的诱发因素是指触发病毒传染或触发病毒发作的控制条件。条件判断是病毒自身特有的功能，一种病毒一般设置一定的激发条件。病毒程序在运行时，每次都要检测激发（控制）条件，一旦条件成熟，病毒就开始发作。

三、计算机病毒程序的结构

从目前已出现的计算机病毒来看，计算机病毒一般包括三大功能模块，即引导模块、传染模块和表现/破坏模块。其中后两

个模块各包括一段触发条件检查程序段，它们分别检查是否满足触发条件和是否满足表现/破坏触发的条件。只有在相应的条件满足时，病毒才会进行传染或表现/破坏。当然，并不是所有的计算机病毒都包含了这三个模块。例如，维也纳病毒没有引导模块，巴基斯坦病毒没有表现/破坏模块。计算机病毒的一般结构可由图 2－1 表示。

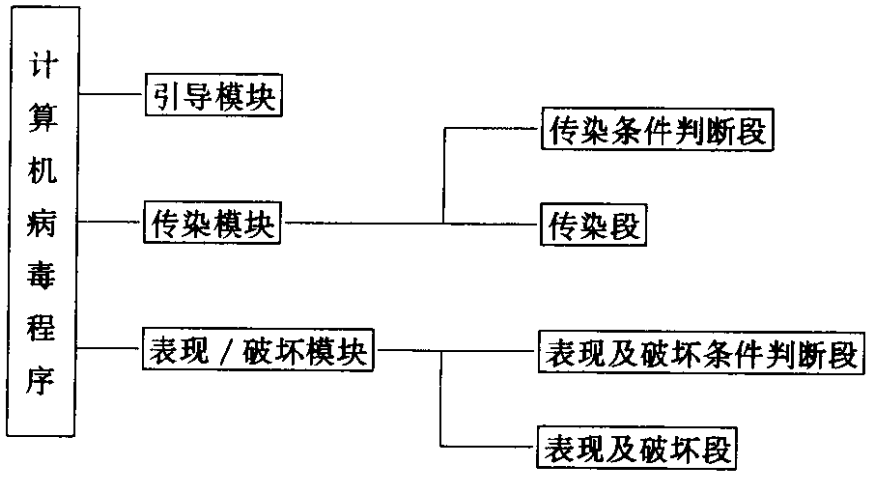


图 2－1　计算机病毒的一般结构

引导模块的作用是将病毒由外存引入内存，将静态病毒激活，使之成为动态病毒。静态病毒是指存储介质上如软盘、硬盘等的计算机病毒。静态病毒没有处于加载状态，不能执行病毒的传染或表现/破坏作用。动态病毒是指已进入内存处于活动状态的计算机病毒。动态病毒要么正处于运行状态，要么能通过调用某些中断而获得运行权。正是活动病毒时刻在监视着系统的运行，一旦传染条件或表现/破坏条件成熟，即调用其传染程序段或破坏程序段，使病毒进行扩散，系统蒙受损失。动态病毒在内存中存在的时间称为动态病毒的生命期。动态病毒的生命期有长有短，有些动态病毒只在运行宿主程序（即已被该病毒传染的程序）期间存在，宿主程序运行完毕即退出内存，例如维也纳病毒。大多数病毒则是从第一次被运行后即保留在内存中，一直延续到下一次重新启动计算机或关机。

计算机病毒的传染模块是计算机病毒的运载工具，其作用是