实 用

计算机入门丛书

吉林科学技术出版社

计算机病毒及防治基础

实用计算机入门丛书

计算机病毒及防治基础

崔广才　孙文生　　编著

吉林科学技术出版社

实用计算机入门丛书
计算机病毒及防治基础　　崔广才　孙文生　编著

责任编辑：赵玉秋　林先根　　封面设计：马胜

出版　吉林科学技术出版社　787×1092毫米 32开本 7.875印张 171,000
发行　新华书店总店北京发行所　1994年10月第1版　1994年10月第1次印刷
印刷　吉林电力职工大学印刷厂　印数：1—6000册　定价 6.00元
ISBN 7—5384—1384—7/TP·2

内 容 提 要

本书由浅入深地介绍了计算机病毒的历史、现状和危害性，系统地论述了预防计算机病毒的方法和技术等基本知识。包括计算机病毒起源、传播机制和预防措施，国内流行的病毒检测程序和消毒的软件，以及常见典型病毒的剖析与诊治实例。并对和病毒有关的 DOS 技术，磁盘结构等知识作了相应介绍，是广大微机用户了解病毒、检测病毒和消除病毒的必备书。

编写说明

随着微型计算机的普及，人们对计算机知识的需要也愈加迫切，而初学者对计算机又感到高深莫测，无从下手，怎样才能更好地帮助初学者尽快地掌握微型计算机的操作、使用，这是我们编写这套微型计算机入门丛书的宗旨。

对于初学者，要尽快地掌握微型计算机的使用与操作，最重要的是要对微型计算机有一个基本的了解，掌握计算机的"个性"与"脾气"，这就需要一位好老师，《微型计算机入门丛书》能帮助您尽快与微机交上朋友。本套丛书以实用为其特点，从微机基础知识，到各种软件的使用，都讲得通俗易懂，一看就会，就能在微机上实现，特别适合初学者自学，是计算机初学者的良师益友。

微型计算机已开始进入办公室和家庭，它是现代化办公与现代化家庭的标志，掌握微型计算机知识，也是未来现代化社会的需要，所以说，微型计算机知识是有识之士必备的知识，是现代化社会的必修课。《微型计算机入门丛书》由著名计算机专家、吉林大学教授庞云阶主编，每个分册的编写者都是多年从事微机教学的有经验的老师，因此，这是一套非常实用的初学者的教材，相信它会对你掌握微机有很大帮助。本书由于编写时间仓促，编者水平有限，缺点和错误之处在所难免，恳请广大同行与读者批评指正。

编　者

1994年8月

前　言

计算机病毒在全球大规模泛滥，对计算机的使用造成了巨大的威胁，尤其是随着微型计算机的发展，电脑已走入千家万户，对计算机病毒的诊治和预防，更成为迫切而重要的问题。

本书共七章组成：前两章介绍了计算机病毒的起源、发展及其基本原理；第三章从实用的角度介绍了国内常用的几种清毒和检测程序；第四章和第五章从理论基础和实用原则结合的角度介绍了解析计算机病毒的技术基础和一些实用工具软件；第六章提供了一些简单的计算机病毒的预防方法；最后一章给出了几个剖析病毒程序的实例。

陈玉文同志对本书的编写给予了大力的支持，曾凡永同志和刘宇同志对本书的录入和校稿做了大量的工作，在此一并表示感谢。

因作者水平有限，本书有错误和不妥之处，请读者批评指正。

编著者

1994 年 4 月

目　录

第一章　计算机病毒概述

§1.1　计算机病毒的起源和发展

1.1.1　计算机病毒的起源

随着计算机的普及，计算机的应用已从科学计算、过程控制、数据处理等方面，逐步深入到人类社会生活的各个领域，计算机给人类进步和社会文明所带来的巨大冲击，就像当年蒸汽机和电的发明所带来的震憾一样。正当计算机事业向前迅猛发展的时刻，计算机病毒悄然出现了，并迅速传播，计算机病毒以其在全球的大规模疫情，造成了极其严重的经济和社会损失。计算机病毒的影响和破坏在我们身边经常可以看到，尤其在微机上。但究竟计算机病毒是如何形成的呢？关于这个问题，众说不一。下面是关于计算机病毒起源的几种主要说法：

（1）科学幻想小说

1975 年，美国科普作家约翰·布鲁勒尔（John Brunner）写了一本名为《震荡骑士》（Shock Wave Rider）的书，该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事，令人耳目一新，成为当年最佳畅销书之一。

1977 年，另一位美国科普作家托马斯·捷·雷恩

(Thomas. J. Ryan) 推出轰动一时的《P-1 的青春》(Adolescence of P-1)。雷恩构思了一种神秘的、能够自我复制的、利用信息通道传播的计算机程序，并称之为计算机病毒。这些病毒在计算机之间相互传染，最终控制了 7 000 多台计算机的操作系统，引起混乱和不安。

计算机病毒从上述的科幻小说到大规模泛滥仅用了 10 年时间。

(2) 恶作剧

一批从小熟悉计算机并对计算机技术有浓厚兴趣的年轻人，特别是像美国这样计算机普及率很高的国家里，他们自恃自己有高超的技术和过人的智慧，认为世界上没有做不到的事，他们凭借自己对计算机软件特别是操作系统的深入了解，编制了隐藏在计算机系统内部，能通过载体进行传播和复制，并在一定条件下激发和表现的程序，这就是计算机病毒。编制这些病毒程序的初衷，无非是想显示一下自己在计算机方面的才华，并且从同伴的计算机资源遭到破坏中寻求乐趣。一般来讲，这类病毒多属于所谓的“良性”病毒。例如像“小球”病毒和“Yankee Doodle”病毒，前者在屏幕上显示一个跳动的小球，后者则演奏一首美国民歌。

曾经轰动美国乃至世界的 Internet 网络事件，就是 23 岁的美国青年罗伯特·莫里斯 (Robert T. Morris) 出于恶作剧制造的蠕虫病毒 (Tap worm) 引起的。它使 6 000 多台计算机被病毒感染，造成了美国历史上最大的计算机网络 Internet 不能正常运行。这是一次非常典型的计算机病毒侵入计算机网络的事件，迫使美国政府立即做出反应，国防部成立了计算机应急小组。这位学生设计该病毒的目的是攻击 SUN 微机系统公司和数字设备公司 (DEC) 的计算机系统。这次

事件中遭受计算机病毒攻击的 Internet 网包括 5 个计算机中心和 12 个地区节点，连接着政府、大学、研究所和拥有政府合同的 250 000 台计算机。在 Internet 网络中有三个基本网：美国国防高级研究计划局网络、军用网络和国家科学基金会网络。罗伯特·莫里斯设计的病毒实际上是钻了 UNIX4.3 的漏洞。蠕虫病毒入侵后通过 Internet 网络不断扩散，直接影响 SUN 和 VAX 系统的运行。由于这次病毒事件的影响，计算机系统直接经济损失达 9 600 万元。罗伯特·莫里斯设计的病毒程序利用了系统中存在的弱点，从而使他成为入侵 APPANET 网的最大的电子入侵者，并由此获准参加康乃尔大学的毕业设计和哈佛大学 Aiken 中心超级用户的特权。

据美联社 1990 年 5 月 5 日消息，根据罗伯特·莫里斯设计的病毒程序，造成 1988 年 11 月 2 日约 6 000 台与 Internet 系统连的计算机，包括国家航空和航天局、军事基地和主要大学的计算机停运的事故，他因此而被判 3 年缓刑，罚款 1 万美元，并被命令进行 400 小时的新区服务。

（3）程序员的软件权利保护

计算机软件是一种知识密集的高科技产品，是软件工作者付出巨大的劳动的结晶。但因为软件资源（软件产品）的保护还没有适当的法律依据，许多商业软件被非法拷贝和复制，使软件程序员和软件制造商的利益受到严重损害。为了保护自身利益，也为了惩罚和教训那些不尊重软件程序员劳动成果的人，程序员和软件制造商在他们的软件产品中加入计算机病毒，并在一定的条件下引发和破坏。

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。×××与×××敬

上，帕金思坦尼电脑公司”。当专家进一步追查时，发现这个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。事后了解到，这个病毒是帕尼斯公司防止非法复制的自卫性病毒。

另外典型的还有 Pakistain Brain 病毒，据说这种病毒由巴基斯坦程序员阿尔维兄弟编写的，其本意是为了追踪对他们的软件产品的非法拷贝者，并无恶意。这种病毒最初只是修改磁盘的卷标，把卷标打上标记，后来被人修改后，已具有巨大的破坏力。

受病毒感染的软磁盘文件，在程序运行时屏幕上显示的内容是：

Welcome to the Dungeon

(c) 1986 Basit & Amjad (pvt) Ltd.

BRAIN COMPUTER SERVICES

730 Nizam Block Allama Igbal Town

Lahore, Pakistan

Phone: 430791, 443248, 2800530

Beware of this VIRS

Contact us for vaccination

在 1986 年初，他们编写了这个病毒程序，随后将这个病毒程序的磁盘拷贝文件送给了一个朋友。不久，这个病毒在美国出现。最先发现 Pakistan 病毒的报告是由特拉华大学提供的，随后在匹兹堡大学、乔治·华盛顿大学、宾夕法尼亚大学等高等学校陆续出现。并且每次出现的病毒在表现形式上都略有不同。

(4) 计算机犯罪

在当今的国际社会里，由于计算机病毒潜在的破坏性，使

它成为一种新的恐怖犯罪活动，并且正演变成军事系统电子对抗的一种进攻性武器。

1989 年 12 月，肯尼亚的一些大公司、银行、国家机关的计算机系统相继感染上计算机病毒，有的计算机系统磁盘文件遭到破坏，有的计算机系统陷于瘫痪。这种病毒来自标有“艾滋病信息磁盘”字样的软盘，磁盘由巴拿马的一家自称“西布格公司”制作，由伦敦免费向欧洲、北美、远东、东非各大公司和银行邮寄，截止 1989 年 12 月该公司寄出至少 1 万张磁盘。随盘的信说，这种磁盘的程序专为艾滋病预防者和医务人员编制的，使用者可查阅各种有关艾滋病的资料，但又警告说，凡使用本磁盘的人必须向西布格公司支付 378 美元，否则该公司将使用现有程序机制中断该程序，计算机中原有的程序也将受到破坏。肯尼亚的一些银行、企业由于使用这种磁盘，使计算机系统受到破坏。英国、南非等国也相继发现了这种病毒，计算机系统也受到了严重的破坏。

经调查，这种病毒是一个名叫鲍伯的美国人编制的，事后，美国联邦调查局指控他利用计算机病毒对许多国家进行敲榨、勒索，并逮捕了他。

1989 年美国军方一架完全由计算机监控的的隐形战斗机试飞时坠毁。根据警方调查，怀疑是计算机病毒造成的恶果，属于人为的事故。

1990 年 5 月，日本一家公司利用计算机病毒破坏夏普公司微机计算机系统数据文件。这是日本第一次发现公司之间利用计算机病毒作为竞争手段。警方已着手调查此事。

上面只是几种主要说法，关于计算机病毒的起因，也许是兼而有之，我们也不必认真的追究，我们重点要说明的是如何预防和清除计算机病毒等实际问题。

1.1.2 计算机病毒的发展

计算机病毒在国际上大规模传染始于1987年，但当时新闻媒介对计算机病毒侵害的反应是冷淡的。而1988年11月3日在美国发生的INTERNET网络遭受计算机病毒攻击事件震惊了世界后，从此一个崭新的名词“计算机病毒”闯入了新闻报道领域，并且逐步由陌生到熟悉闯入了千万个计算机用户的大门。人们由惶恐到冷静，开始积极研究与之斗争的策略和方法。

计算机病毒种类从1988年至今已有700余种。这还不包括形形色色的小批量病毒变种，从INTERNET网络至今，计算机病毒已传遍了全球，引起了世界范围内的惶恐和惊慌，可以说计算机所到之处也是病毒所达之处，计算机应用面越是拓宽，计算机病毒的传播面也就越扩大。许多国家和地区，如美国、日本、印度和中国等许多国家都曾发生过计算机病毒的恶性事件。

即使在苏联也发现了多种病毒，这些病毒包括：扬基、星期天、磁盘杀手、乒乓、维也纳、耶路撒冷、黑色星期五、Ascsina、Microsoft88（543）等以及各种其它病毒的变种。

计算机病毒的攻击对象是有针对性的，不同种类的病毒攻击不同的计算机种。由于IBM PC及其兼容机占了计算机的主导潮流，则攻击它的计算机病毒也特别的多，约占60%。

在我国，西南铝加工厂计算中心，于1989年3月首次发现计算机病毒程序，并把它命名为“001”号病毒程序，这就是今天大家所熟悉的小球病毒。随后《计算机世界》等一大批报刊和杂志相继发表了有关报道，从此拉开了我国计算机病毒热的帷幕，随着时间的推移，各种计算机病毒通过不同

渠道传入我国，同时计算机界的有识之士开始研究剖析病毒程序，并提出了各种检测和诊治病毒的软件，为控制计算机病毒的蔓延，为减少病毒所造成的损失起到了巨大的作用。

在我国已经相继发现了小球、大麻、DIR-2、Torch 等多种国外流行的病毒，其中小球、大麻、DIR-2 流传最广，危害最大，几乎遍布全国城乡各地。特别是二者的交叉传染，使常用的解毒软件无能为力。值得注意的是国内也发现了各种变种病毒，甚至于完全由国内制造的国产病毒，如：中国炸弹（CHINESE BOMB）、6.4 病毒等。

最近在国内流行的 DIR-2 病毒，Torch 病毒以及其它国产病毒，如 6.4 病毒等又呈流行之势。特别是 Torch 病毒，由于其隐蔽性好，传染性强，发作时破坏硬盘主引导扇区，因此危害性更大。

病毒的种类和变种正呈不断上升的趋势，而解毒软件和检测软件也在不断的完善：魔高一尺，道高一丈，两军对垒正呈犬牙交错、交替上升之势。

和计算机病毒作斗争，将是长期的、艰巨的任务。

§1.2 计算机病毒的概念与特性

1.2.1 什么是计算机病毒

计算机病毒可以在很短的时间里席卷全国甚至于全世界。究竟什么是计算机病毒？是很多人其中包括一部分计算机专业人员无法解答的问题。事实上，在计算机界，对病毒的定义也只是描述性的。下面给出几种定义：

· 自我繁殖和向无毒计算机扩散的加密性指令集。

· 不断滋长且危及越来越多计算机工作的程序或指令集。

· 一种在计算机系统运行过程中能把自身精确拷贝或有修改地拷贝到其它程序体内的程序。

· 隐藏在计算机系统内的一种破坏性程序，能够利用系统数据资源进行繁殖、生存，并通过系统数据共享进行传染。

· 计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。(中华人民共和国计算机信息系统安全保护条例)。

· 人为编制的一段程序，其隐藏在计算机系统内部或依附在其它程序上，通过复制自身达到扩散之目的，并破坏或干扰计算机系统的正常工作。

1.2.2 计算机病毒的特性

随着病毒开发者的目的、水平和应用技巧的不同，可以产生各种各样的计算机病毒。一般而言，计算机病毒通常具有以下几个特点：

(1) 隐藏性：计算机病毒通常具有小巧玲珑的特点。指令代码比较少，隐藏在数据或文件中（或潜伏在系统中），不易被发觉，而当病毒程序潜伏的程序体合法调用时，病毒程序也“合法”投入运行，并可将分散的程序部分在所非法占用的存储空间进行重新装配，从而构成一个完整的病毒并投入运行状态。

(2) 潜伏性：计算机感染病毒后，并不立即发作，表现出中毒的症状。往往要等到一特定的条件成立时，才会有所表现。

(3) 可激发性：当满足某特定条件时，可激发表现出中毒的外观症状，激发的本质是一种条件控制，一个病毒程序可以按照设计者的要求，在某个点上激活并发起攻击。攻击的时间可以与多种情况联系起来，包括指定的某个时间或日期、特定的用户标识符的出现、特定文件的出现或使用、用户的安全保密等级或者一个文件使用的次数等等。计算机病毒的可激发性，本质上是一个逻辑炸弹。由于病毒可受外界条件控制激发过程，从而使潜伏在计算机系统中的病毒不易被人发现。

(4) 可传染性：计算机病毒具有强再生机制，可以在运行过程中根据病毒程序的中断请求随机读写，不断进行病毒体的扩散。病毒程序一旦加到当前运行的程序上面，就开始搜索能进行传染的其它程序，从而使病毒很快扩散到磁盘存储器和整个计算机系统上。

个人用计算机系统一旦感染上计算机病毒，可以在系统内扩散病毒，破坏磁盘文件的内容，并可以使系统丧失正常运行的能力。在大型信息系统和计算网络的工作环境下，计算机病毒的传播更为迅速，其病毒程序对系统的破坏性就更大。

需要指出，计算机病毒在系统运行过程中不断进行扩散和传播，因而可以明显降低计算机系统的运行效率，细心的用户可以从计算机运行速度的变化来察觉系统是否感染上计算机病毒。

(5) 危害性：由于病毒具有上述特性，发现难、传染快，且通常有一定的危害能力，轻者影响系统正常工作，重者破坏系统资源，因此具有极大的危害性。