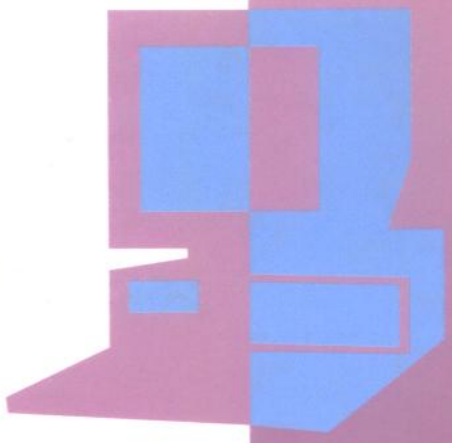
●鲁沐浴 主编

计算机

病毒大全



電子工業出版社

计算机病毒大全

鲁沐浴　主编

電子工業出版社

内 容 提 要

本书简要阐述了计算机病毒的基本概念；列举了计算机用户自己开发的检测、消除病毒的若干程序实例；介绍了3个常用工具软件的使用说明；目前国内几种常见反病毒软件的特点及使用注意事项；列出了国内外2000种病毒的特征、感染过程、感染后果、检测和消除方法；还给出了部分计算机病毒相关词汇英汉对照。

本书适用于计算机应用、开发、操作、爱好者和计算机病毒研究者。

计算机病毒大全

鲁沐浴　主编

责任编辑：张荣琴　特约编辑：雨寒

*

电子工业出版社出版

北京市海淀区万寿路173信箱(100036)

电子工业出版社发行　各地新华书店经销

电子工业出版社计算机排版室排版

北京大中印刷厂印刷

*

开本：787×1092毫米 1/16　印张：46　字数：1201千字

1996年5月第一版　1996年5月北京第一次印刷

印数：5,000册　　定价：66.00元

ISBN 7-5053-3478-6/TP·1381

前　言

自1989年春计算机病毒入侵我国以来，以惊人的速度蔓延开来，虽然通过多方努力使之得以控制，但新的病毒层出不穷，而且技术水平不断提高，隐蔽性越来越强。时至今日世界上已有4988种病毒的记载，继续威胁着计算机系统的安全，严重扰乱着计算机工作人员的正常工作。因此，计算机病毒的预防、检测和消除仍是计算机界所关注的热门话题之一。

本书列出了国内外2000种病毒的特征、感染过程、感染后果、检测和消除办法，并按英文字母顺序排列；列举了计算机用户自行开发的检测、消除病毒的部分程序实例，在编辑过程中每个程序都上机调试通过；对国内目前几种常见的、并已商品化的反病毒软件的特点和使用注意事项做了简单介绍，以期对广大计算机用户和计算机病毒的研究、开发者能有所帮助。

本书由鲁沐浴主编，参加编写工作的有张慧英、殷峰、海燕、张如恩、鹿翠兰、岱东、赵芳启、亓靖涛等。在第二部分"计算机病毒的检测、消除实例"中参与编写的原作者有：

贺朝晖　王有翦　陈乃强　李　志　于信涛　陈诗帆　邹肇辉　刘晓风　王　可　罗　辉
宋正荣　陈立波　江　文　陶为民　赵江声　邱大钧　颜岳军　杨　林　陈　清　张治民
薛炳如　谭克宁　龙爱兵　秦　旭　施来法　孙　伟　张兴福　胡筱罡　张钟保　张　研
万学军　王志红　黄　铮　张　方　等34人。请与编者(100854北京市142信箱406分箱张慧英)联系。

在第四部分"国内几种常见反病毒产品简介及使用说明"中的超级巡警KV100、200反病毒软件简介由王江民编写，DB95反病毒平台中通用病毒检测程序——VCHECK.SYS简介由帝霸计算机技术研究所提供。全书由鲁沐浴统稿，并由俞志清、徐秀荣、郑伟审校。

编　者

1995.12

目　录

第一部分　计算机病毒的基本概述

1.1　计算机病毒的由来

可以肯定地说：计算机病毒发源于美国。计算机病毒是随着计算机技术的发展而产生的一种畸形怪胎。由于计算机的硬件和操作系统的不尽完善而使得计算机病毒层出不穷，并迅速蔓延。

1970 年出现了 CREEPER；

1974 年出现了 RABBIT 病毒；

1980 年美国远景规划局的计算机网络上出现了 DEDUX 病毒；

1981～1982 年在 APPLE Ⅱ 微机上出现了 ELKCLONER 病毒；

1985 年巴基斯坦拉哈尔(Lahore) Brain Computer Service 商店的两兄弟 (Amjad Farooq Alvi, Basit Farooq Alvi)为了保护自己的软件产品而编制成功了巴基斯坦智囊病毒；

1986 年巴基斯坦智囊病毒广泛传染；

1987 年秋 Lehigh 大学发现了 Lehigh 病毒；

1987 年 12 月 IBM 圣诞树蠕虫传染 IBM 的 BITNET 网络；

1988 年 3 月 MacMag 病毒被发现；黑色星期五病毒在以色列发现；

1988 年 11 月 2 日由美国 Cornell 大学年仅 23 岁的研究生 Robert T. Morris Worm 编写的程序攻击美国最大的 Internet 网络，使网络上的 6200 多台计算机不能正常运行。称之为 Internet 网络事件，轰动了世界整个计算机界。

在此以后，计算机病毒就广泛蔓延开来，新的病毒层出不穷，时至今日已达 4,988 种。(这个数字是美国安全网络公司 1995 年 2 月公布的)1989 年 3、4 月间小球(Bouncing Ball)病毒传入我国，从此计算机病毒便在我国大陆蔓延开来。继小球病毒之后，相继出现了巴基斯坦智囊(Pakistani Brain)病毒、大麻(Marijuana)病毒、黑色星期五(Black Friday)病毒、维也纳(Vienna)病毒、洋基(Yankee Doodle)病毒、磁盘杀手(Disk Killer)病毒、打印(Unprinting)病毒、1575/1591 病毒、音乐(Music)病毒、1701/1704 病毒、1554 病毒、Bloody/6.4 病毒、星期天(Sunday)病毒、黑色复仇者(Dark Avenger)及其变种 V2000 病毒、Flip/OPB(Omicron by PsychoBlast)病毒、Liberty 病毒、世纪(Century)病毒、Storytellor 病毒、Exciting Day 病毒等等。不仅如此，我国的一些恶作剧者或恶意攻击者还修改病毒版本制造了一些病毒变种甚至编制了一些新病毒，如中国一号病毒、中国炸弹(Chinese Bomb)病毒、中国炸弹-B(Chinese Bomb-B)病毒、Traveller 病毒、新世纪(New Century)病毒等。

也可以肯定地说：计算机病毒的种类、花样会继续增多，技术水平也会不断提高。而反病毒技术同样会日渐完善，但任何一种反病毒技术和以此技术开发的各种反病毒产品都不能彻底预防、完全检测和消除已知或未知的计算机病毒。

1.2 什么是计算机病毒

美国计算机安全专家 Frederick Cohen 博士对计算机病毒给出了一个早期的定义，即：计算机病毒是一个靠修改其它程序，并把自身复制品传染给其它程序的程序。

现在可以简单地说：计算机病毒是人为的一种计算机程序，这种程序隐藏在计算机系统的可存取信息资源中，利用计算机系统信息资源进行生存、繁殖，影响和破坏计算机系统的正常运行。

1.3 计算机病毒的定名

现在人们对计算机病毒的定名有以下几种方法：

(1) **以计算机病毒自身宣布的名称定名** 计算机病毒的源码中宣布的病毒名称，如原始的大麻病毒中含有 Marijunana 及 Stoned 字样，于是人们定名这种病毒为 Marijunana 及 stoned；Disk Killer 病毒有如下提示："Disk Killer version 1.00 by Ogre Software April 1，1989"，于是人们将其定名为 Disk Killer 及 Ogre 病毒；Traveller 病毒也是计算机病毒自身宣布的名称。

(2)**以计算机病毒触发时间定名(传染触发尤其是表现或破坏触发)** 这种定名取决于计算机病毒表现或破坏系统的触发时间，这种病毒的表现或破坏部分一般为一种定时炸弹，如黑色星期五，即每月的 13 日且为星期五时病毒破坏系统文件，于是人们将其定名为黑色星期五计算机病毒；又如米开朗基罗病毒，该病毒之所以如此定名是因为其触发时间为 3 月 6 号，而 3 月 6 号是著名意大利画家米开朗基罗的生日，于是人们将这种病毒定名为米开朗基罗病毒。

(3)**以计算机病毒表现症状定名** 即根据计算机病毒的表现症状定名计算机病毒，如黑色星期五在一定的情况下，系统屏幕上出现一块长方形亮块，于是国内有人曾定名它为长方块病毒。

(4)**以计算机病毒传染方式定名** 即根据计算机病毒的传染方式定名计算机病毒，如黑色星期五病毒，由于其传染 .EXE 文件时不作标志，所以反复传染，于是又有人定名它为疯狂拷贝病毒。

(5)**以计算机病毒发现地定名** 以计算机病毒首先发现的地点定名计算机病毒，如黑色星期五又称 Jerusalem 病毒、Hebrew 病毒等等。

(6)**以计算机病毒字节长度定名** 以计算机病毒传染文件时文件的增长长度来定名，如黑色星期五又称 1813 病毒；幽灵病毒也可成为 3544 病毒。但由于计算机病毒传染病毒宿主程序时，不同的病毒连接于宿主的长度可能一致，所以这种定名方法并不很科学。

(7)**以计算机病毒宣布的编写时间定名** 用病毒在其病毒代码内部记载的或发作时显示的计算机病毒的编写时间来定名，如 4 月 1 号病毒等等。

(8)**以计算机病毒宣布的编写者定名** 用病毒的其病毒代码内部记载的或发作时显示的计算机病毒的编写者的名称来定名，如 Ogre 病毒(Disk Killer)。

(9)**以计算机病毒中出现的字符串定名** 用病毒在其病毒代码内部记载的或发作时显示的字符串的全部或部分来定名，如 Saddam 病毒、Sunday 病毒。

(10)**以计算机病毒标识定名** 即根据计算机病毒中病毒的标识定名计算机病毒，如 Lib-

erty 病毒。

以上是计算机病毒定名的几种常见的方法，根据这几种方法可以定名一种计算机病毒。

1.4 计算机病毒的分类

目前有关计算机病毒的分类方法很多，如按病毒的寄生方式、按攻击方式(这种分类方法将病毒分为：源码病毒——攻击高级语言编写的程序、入侵型病毒——将自身侵入到现有程序之中、操作系统病毒——操作系统运行时，病毒用自己的逻辑部分取代部分操作系统的合法程序模块、外壳型病毒——将自身包围在主程序外，对原有程序不做修改)、按破坏情况(这种分类方法将病毒分为"良性"病毒、"恶性"病毒)、按是否驻留于内存分类等等。但就攻击微机系统的病毒而言，分类方法应以传染方式、寄生方式及是否驻留内存来分较为妥当。因为之所以称为病毒就在于它具有传染性，而寄生方式又决定着消除病毒的方法，病毒是否驻留内存也关系到病毒的传染、预防、检测和消除。

这里仅对微机系统的计算机病毒按其传染方式分为以下三大类：

1. 引导型计算机病毒

引导型计算机病毒是指既传染硬盘主引导区，又传染 DOS 的 BOOT 区的计算机病毒。就一般而言，引导型的计算机病毒出现的传染情况如下：

(1) 硬盘 BOOT 区引导程序；

(2) 软盘 BOOT 区引导程序；

(3) 硬盘分区表(主引导程序)。

传染情况是(1)+(2)；(1)+(3)；(1)+(2)+(3)。

2. 文件型计算机病毒

文件型计算机病毒是指：

(1) 能传染操作系统文件的病毒，即(以 PC-DOS 为例)传染 IBMBIO. COM、IBMDOS. COM、COMMAND. COM 等操作系统运行时所必须的文件的病毒；

(2) 能传染扩展名为 .COM 文件的计算机病毒；

(3) 能传染扩展名为 .EXE 文件的计算机病毒；

(4) 能传染 .COM 及 .EXE 文件的计算机病毒；

(5) 能传染覆盖文件等其它可执行文件的计算机病毒；

(6) 能传染 COMMAND. COM 文件、. EXE 文件、. COM 文件，甚至两个系统隐含文件的计算机病毒。

3. 混合型计算机病毒

混合型计算机病毒是指既传染磁盘的引导区又传染可执行文件的计算机病毒(即引导型和文件型计算机病毒)。

以上这三类计算机病毒包括了目前出现的各种微机病毒。

1.5 计算机病毒的构成部分

就一般而言，计算机病毒由以下三部分构成：

1. 引导模块部分

此部分将病毒由外存引入内存，使传染模块和表现模块(破坏模块)处于活动状态。

2. 传染模块部分

传染模块是将病毒传染到其它对象上去。

3. 表现模块(破坏模块)

实施病毒的破坏作用，如删除文件、格式化磁盘、显示或发声等。

计算机病毒的一般工作流程是：当通过第一次非受权的加载，病毒的引导模块被执行后，病毒由静态转为动态。动态的病毒通过某种触发手段不断地检查是否满足传染条件，一旦满足则执行相应的传染功能或破坏功能。

静态病毒是指存在介质(如软盘、硬盘、磁带等)上的计算机病毒。动态病毒是指已进入内存、正处于运行状态或立即获得运行权的计算机病毒。病毒的传染或破坏主要是由动态病毒进行的。

1.6 计算机病毒宿主

计算机病毒和生物病毒一样，也有自己的病毒体(病毒代码或病毒程序)生存环境。而病毒自身和病毒的寄生体是两个概念，前者必须找一个赖以生存的环境，后者是前者的生存环境。当一种计算机病毒传染系统之后，病毒所寄生的环境则称之为这种病毒的宿主或宿主环境，而存储染有此种病毒的程序的介质则称之为这种病毒的存储介质宿主。染有此种病毒的程序在计算机系统中运行时或运行后，病毒驻留内存中，这时计算机系统称之为该病毒的宿主系统，一台计算机系统可同时成为多种病毒的宿主系统。当病毒在内存中占据中断进行传染或破坏时，被病毒占据的中断程序称之为该病毒的内存宿主或传染宿主。所以每一种病毒都有自身的宿主系统、存储介质宿主、内存宿主或宿主程序。

1.7 计算机病毒的特征

1. 计算机病毒的寄生性

计算机病毒的病毒码必须寄生在外部存储介质中，否则在系统运行中止后无处藏身。病毒码常常寄生在磁盘的引导扇区、可执行程序中或为独立的程序。一种病毒的寄生性决定了这种病毒的传染方式。计算机病毒的寄生性又可分为覆盖式寄生性、代替式寄生性、添充式寄生性、链接式(及间接链接式)寄生性和转储式寄生性 5 种。

(1) 覆盖式寄生性是指病毒程序用其部分或全部代码部分或全部地覆盖被攻击的合法宿主，使原宿主的部分或全部功能被破坏。

(2) 代替式寄生性是指病毒用自身代码代替原合法程序的代码，但病毒自身的代码能够完成(或简单地完成)原合法程序的主要功能，如 Unprinting 病毒(2708 病毒)传染硬盘的主引导区。

(3) 添充式寄生性是指计算机病毒将自身的全部代码隐藏在合法程序内部未存有信息的“空闲”存储单元中，被这种病毒传染的文件长度不变，如 Lehigh 病毒。

(4) 链接式寄生性是指病毒程序寄生在合法的宿主程序之上，不破坏原合法程序的代码。链接式寄生性还可以分为头部链接式、尾部链接式和中间链接式。头部链接式是指计算机病毒

程序链接于宿主程序的开头；尾部链接式是指病毒程序链接于宿主程序的尾部；中间链接式是指计算机病毒链接于宿主程序的中间。如黑色星期五病毒传染 .COM 时属头部链接，传染 .EXE 文件时属于尾部链接。间接链接式是指病毒不直接与合法程序链接，而是存储于存储介质的特定位置，通过特定的功能在其宿主程序执行时获得控制权。

(5) 转储式寄生性是指计算机病毒将其宿主程序部分或全部转移存储到该病毒宿主程序所在的存储介质的其它存储空间，而病毒侵占该病毒宿主程序所在的原存储空间。转储式寄生性又可分为保护型转储式寄生性和非保护型转储式寄生性，前者是指计算机病毒对其转移存储的系统合法程序(或部分程序)进行保护，后者则不保护转移存储的程序。例如小球病毒传染 BOOT 区属于这种寄生方法的前一种——保护型转储式寄生。该病毒传染系统时将正常的 DOS 引导程序转移并存储在病毒找到的扇区中，并对这些扇区进行保护，而病毒的一部分存储在 DOS 的引导区中；而大麻病毒传染系统(无论是硬盘的主引导程序还是软盘的 BOOT 区程序)则属后者——非保护型转储式寄生。

2. 计算机病毒的传染性，传染的广泛性和隐蔽性

病毒一词来源于生物学，传染也相应成了计算机病毒的一个重要特性。传染性是衡量一种程序是否为病毒的首要条件。计算机病毒的传染性是计算机病毒的再生机制，病毒程序一旦进入系统并与系统中的程序链接在一起，它就会在运行这一被传染的程序之时或之后开始传染其它程序，从而达到再生的目的，使得一种病毒产生之后该病毒的副本不断地增加。计算机病毒可以传染一台(多台)微机、一个(多个)局部网络、一个(多个)大型计算机系统或者一个(多个)多用户系统。应当指出的是，对于一个个人计算机系统来说，一旦传染上病毒，不仅系统本身可能丧失正常运行的能力，同时(应该着重强调的是)由于计算机病毒的传染性，被传染的计算机系统可能成为对计算机界中每一个与该被攻击的系统兼容的系统的一个攻击者，这样通过计算机系统数据共享的途径，病毒会不断地蔓延开来，乃至于波及整个计算机领域，影响整个社会。传统的计算机病毒传染系统一般都是通过抢占系统合法中断的方法来实现的，病毒抢占合法中断的方法一般又都是通过修改合法中断的中断向量来实现的，即修改后的中断向量指向病毒传染部分，病毒的传染部分通过病毒保存的合法中断向量指向合法中断服务程序。这样病毒的传染和执行合法的中断是联系在一起的，使得病毒的传染貌似系统正常的合法中断服务程序的执行，所以计算机病毒传染系统都具有一定的隐蔽性。

3. 计算机病毒的多重传染

对于一个计算机系统而言，它可能是多个病毒攻击的对象，可以同时是多个病毒的宿主系统，则称多种或多个计算机病毒共同寄生于同一个宿主系统的传染现象为计算机病毒的多重传染。这种情况在计算机病毒如此众多的今天是一种较为常见的现象。并且计算机病毒的多重传染所导致的表现症状、破坏方式及对系统所造成的后果是很难判定的。若形成了这样两种现象：

第一，已经被一种病毒传染的计算机系统可能又被另一种或多种病毒传染；

第二，已被传染且未消毒的特定病毒的宿主程序可能又被另一种或几种计算机病毒传染，也就是说，同一程序在某个时间段内可能成为多种计算机病毒的宿主程序。

第一种现象是针对计算机系统而言的，称为并行传染；第二种现象称为计算机病毒的交叉传染。

4. 计算机病毒的破坏性

计算机病毒的破坏及表现部分能反映计算机病毒制造者的目的，因此，计算机病毒的破坏

性取决于计算机病毒的设计者。如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对于计算机系统进行攻击所造成的后果是难以设想的，它可以毁掉系统内的部分数据，也可以破坏全部数据并使之无法恢复，同时也可以对系统的某些数据篡改，使系统的输出结果面目全非。但也并非所有的病毒对系统都产生极恶劣的破坏作用。事实上，也存在着对系统在一定程度上是有益的病毒。

5. 计算机病毒的潜伏性

计算机病毒的潜伏性是指计算机病毒的一种依附于其宿主程序而寄生并不被用户发觉的能力，是指计算机病毒传染系统之后，在其宿主程序执行时病毒不进行表现或破坏(如屏幕没有异常显示、没有文件的异常丢失等等)的一段时间。计算机病毒的潜伏期是指计算机病毒传染其宿主之后，到计算机病毒表现部分及破坏部分被激活而不被用户发现的一段时间。一个编制巧妙的计算机病毒程序，可以在几周或者几个月甚至几年内隐蔽在合法文件之中，对其它系统进行传染，而不被人们发现。计算机病毒潜伏性的好坏是与病毒本身的编制方法和采用的技术有关的，但病毒在特定系统内的潜伏期的长度则与多种因素有关。人们必须注意的是在病毒潜伏期内，有时系统的备份设备很可能将病毒随其宿主程序一起备份起来，或制成程序或数据的副本，甚至这些备份还可能被保存起来，致使这种病毒被消灭许多年后，又卷土重来，使系统再次遭受到这种人们已认为消失的病毒的传染。计算机病毒的潜伏性与其触发条件紧密相关，与传染性相辅相承，潜伏性越好，病毒在系统中存在的时间就会越长，被人们"保存"起来的可能性就会越大，病毒"卷土重来"的机会也就越大，病毒的传染范围也就会越广，造成的损失也就越惨重。

6. 计算机病毒的可触发性

计算机病毒一般都有自身设定的触发条件，这种触发条件包括传染触发条件和破坏及表现触发条件。当病毒的触发条件得到满足之后，计算机病毒就开始活动，如进行传染、出现表现症状、破坏系统等等。病毒的触发条件得到满足并使病毒开始活动称之为计算机病毒的激活。计算机病毒的传染触发条件用于触发病毒传染，如在一定的条件下激活一个病毒的传染机制(即调用病毒的传染部分)使之进行传染；计算机病毒的表现及破坏部分的触发条件用于触发病毒的表现或破坏，即在一定条件下激活计算机病毒的表现部分或破坏部分，使系统出现该病毒的表现症状或按病毒的约定破坏系统或合法程序。计算机病毒的触发条件可以是外界的(如用户的特定操作)也可以是系统内部(如系统内部的时钟)的，但对病毒本身而言，触发条件都是外部因素。因为一种病毒只是设置一定的触发条件，这个条件的判断是病毒自身的功能，而条件的满足则不是病毒自身提供的。如 Unprinting 病毒在其内部设置有一计数器，当这一计数器的值为 224 时，病毒将系统的串行口和并行口地址归零，但设置计数器记录的是系统的启动次数，系统的启动对于病毒而言是外部因素。触发机制是一种条件控制，一个病毒程序可以按照设计者的要求，在某种情况下激活并对系统发起攻击。病毒攻击操作是否进行可以与多种情况联系起来，包括病毒指定的某个时间或日期、特定的用户识别符的出现、特定文件的出现或使用、用户的安全保密等级和一个文件使用的次数以及系统的启动次数等等。计算机病毒的可触发性也就是计算机病毒的条件性和目的性。

7. 计算机病毒攻击的主动性

一般而言，计算机病毒设计者的目的在于对计算机进行攻击，所以所有病毒对系统的攻击都是主动的。从一定程度上讲，计算机无论采取多么严密的技术性保护措施都不可能彻底排除病毒对系统的攻击，而保护措施只能是一种预防的手段而已。计算机病毒技术和反病毒技术是

一种矛与盾的关系，锋利的矛可以有坚固的盾来抵抗，坚固的盾又引来更锋利的矛，而后又产生更加坚固的盾……依次循环，必然会形成计算机病毒和反病毒技术螺旋式上升的发展结果。

8. 计算机病毒的针对性

计算机病毒的针对性包括传染的针对性和破坏的针对性两部分。传染的针对性是指不同的病毒可能传染不同种类的计算机，如 MacMag 是传染 Macintosh 计算机的，而 Flip 是传染 IBM PC、286、386 等 IBM 及其兼容机的。而破坏的针对性是指计算机病毒的破坏性可以是针对特定系统的，如含有某种信息或程序的系统，传染 Macintosh 计算机的评分病毒就是一个典型的例子。

9. 计算机病毒可作为一种攻击载体

这里所说的计算机病毒可以作为一种攻击载体，是对计算机病毒的传染部分及破坏部分而言的。病毒的传染及病毒的触发反映了计算机病毒设计者的攻击目的。一种计算机病毒的破坏部分的破坏程序反映了病毒设计者的初衷和目的。由于病毒的破坏部分也是由计算机语言来编制的一些编码语言，所以这一部分可以按照编写者的本意做编写者所要做的一些事情，而这一部分进入计算机系统则是需要传染部分辅助的，即通过传染部分的运行将计算机病毒的全部代码传染到病毒宿主程序之上，采用同样传染部分的病毒只要病毒的破坏部分不同，病毒对系统的攻击也就不同。所以针对这种情况，可以说计算机病毒是一种携带破坏性程序（指病毒的破坏部分）的载体。计算机病毒的传染部分可以携带其破坏部分，躲避开系统检测程序。因此病毒可被用来制造隐蔽通道，修改操作控制，或者进行其它的破坏活动。

10. 计算机病毒是一段可执行程序

计算机病毒和其它合法程序一样，是一种计算机高级语言的语句组成的可存储、可执行的非法程序，是由系统可以运行的合法指令、编码，如一种计算病毒可以是用汇编语言编写的，也可以是用 C 语言、FORTRAN 语言、BASIC 语言、PASCAL 语言，甚至是计算机的机器指令等编写的。它可以间接地运行，即通过运行病毒的宿主程序使病毒程序得到运行。计算机病毒传染其宿主后，隐蔽在合法的可执行程序或数据文件中而不易被人们察觉和发现。病毒程序在运行时，与合法程序争夺系统的控制权（病毒一般总是在运行其宿主程序之前首先运行自己，通过这种方法抢夺系统的控制权）。病毒在随着宿主程序运行时，由于病毒代码（即使是代码长度再短的病毒）的运行，其也要占用系统时间，所以病毒总是和合法的程序抢夺系统的运行时间，使得系统运行合法程序的时间延长。计算机病毒在其传染文件后（合法文件的长度一般来说都要增长），由于病毒的存在，使得系统存储空间减少。

11. 计算机病毒的变种和衍生性

在计算机病毒的演化过程中，以一种计算机病毒代码为基础，经过一定的修改后而产生的和原版病毒的传染方式、方法或表现、破坏方式、方法相同的病毒的一种新版本称之为计算机病毒的变种。在计算机病毒变种的基础上继续修改而最终导致的一种和原病毒的设计思想（包括传染方式、表现破坏方式）都不同的病毒称之为原始病毒的衍生体。计算机病毒的这种衍生性是计算机病毒种类、数量不断增加的一个主要原因。

12. 计算机病毒传染的相容性和互斥性

几种不同的病毒可以同时寄生于同一宿主上，即是病毒的相容性。当一种病毒寄生于一个宿主后，另一个病毒则不能寄生，即是互斥性。相容性和互斥性与病毒寄生于宿主的先后顺序有关。

1.8 计算机病毒的破坏现象及表现症状

计算机病毒的破坏现象和表现症状是因具体病毒而各异的，但就总体而言，病毒可能造成的系统破坏及异常现象有：

(1) 破坏文件分配表，使用户在磁盘上的信息丢失。如大麻病毒将正常的硬盘(20MB)主引导程序移至物理第 7 扇区，而第 7 扇区正是硬盘的 FAT1。

(2) 改变磁盘分配，造成数据写入错误，特别是将文件读入 RAM 时，会引起系统崩溃。

(3) 删除磁盘(包括硬盘和软盘)上特定的可执行文件或数据文件。对于这种情况而言，若计算机病毒删除的文件是系统文件的话，则会导致这片磁盘不能引导系统。

(4) 修改或破坏文件中的数据。这种计算机病毒对金融系统的破坏是致命的。

(5) 影响内存常驻程序的正常执行。

(6) 使磁盘坏扇区增多，可用空间减少，有些程序或数据文件被破坏。

(7) 更改或重新写入磁盘的卷标。

(8) 计算机病毒程序自身在计算机系统中的多次繁殖，可以导致系统的存储空间减少，使得正常的数据或文件不能存储。

(9) 对整个磁盘或磁盘的特定磁道、扇区进行格式化。

(10) 改变磁盘上目标信息的存储状态。

(11) 系统空挂，可以造成显示屏幕或键盘的封锁状态。

(12) 盗取有关用户的重要数据。

(13) 在系统中产生新文件，这些文件对于用户而言，可能是可见的，也可能是隐含的。

(14) 改变系统的正常运行进程。

(15) 对于系统中用户存储的特定文件进行加密或解密。

(16) 删除或改写磁盘的特定扇区。

(17) 影响屏幕的正常显示，如造成屏幕异常滚动，显示异常图形等。

(18) 打印和通信端口异常。

(19) 软盘驱动器的磁头来回移动。

(20) 中断向量异常变化或出现系统非法(未提供)的中断服务程序。

(21) 机器的蜂鸣器发出异常声音。

(22) 磁盘的目录区被破坏。

(23) 影响系统正常启动，键盘锁定。

(24) 改变文件属性、建立日期，增长文件，系统运行速度变慢等。

计算机病毒的具体症状如下：

上面概括地介绍了计算机病毒传染系统后系统的一般症状。实际上病毒所引起的症状是多种多样的，并且是不能预先断定的。就目前出现的计算机病毒而言，病毒在系统中表现的具体症状大体有如下 26 种：

(1) 计算机屏幕的异常滚动，如小球病毒在 CCDOS 下，当病毒发作时系统的屏幕就会异常滚动；

(2) 计算机屏幕上出现异常信息揭示，如大麻病毒在系统启动时提示："Your PC is now stoned!"，disk killer 病毒在破坏条件成立时提示：

Disk Killer——Version 1.00 by COMPUTER OGRE 04/01/1989
PROCESSING
Warning!!
Don't turn off the power or remove the diskette while Disk Killer is Processing!
PROCESSING
Now you can turn off the power
I wish you luck

实际上许多病毒都是提示信息。

(3) 计算机屏幕上出现异常的图形。如 1575 病毒发作时屏幕上出现小毛虫；

(4) 计算机屏幕上的字符(英文字符)出现滑落。如 1701/1704 病毒发作时，屏幕上的字符落到屏幕底部；

(5) 计算机屏幕上显示的汉字不全。如小球病毒在 CCDOS 环境下发作时，跳动的小圆点在遇到汉字时将消去整个汉字的一半；

(6) 计算机系统的蜂鸣器出现异常声响。如 1701/1704 病毒、音乐病毒以及 Yankee Doodle 病毒都会导致系统蜂鸣器的异常声响；

(7) 计算机系统的运行速度减慢。这种现象在任何染毒的系统上都会出现，这对于有经验的用户而言是一种较为明显的症状；

(8) 计算机系统出现异常死机。有些病毒如 Brain、Lehigh 等有时都会造成系统异常死机，有一些病毒在传染失败时也将导致系统异常死机；

(9) 系统文件的长度发生变化。文件型的计算机病毒一般都将修改文件的字节长度，如黑色星期五传染.COM 文件，使文件增加 1,813 字节，Yankee Doodle 使文件增加 2,885 字节等；

(10) 计算机存储系统的存储容量异常减少，在应该能存入文件的存储介质上存储文件时出现不能存入的现象，如一些病毒由于病毒自身的“漏洞“，在传染文件时反复传染，造成存储系统的存储容量明显减少。多种病毒同时传染一个宿主程序后也能造成磁盘容量的迅速减少，如小球病毒、Brain 病毒同时传染系统，随系统的启动反复在系统盘上制造坏簇，从而迅速减少磁盘的可用空间。黑色星期五和 Yankee Doodle 病毒同时传染 .COM 文件时，也造成两病毒反复传染 .COM 文件的现象，从而以 4.7K 的速度迅速吞噬磁盘空间；

(11) 打印机的打印速度降低或打印机失控。如 Unprinting 病毒造成打印机不能打印，出现 “No Paper”提示；

(12) 丢失文件。一些病毒在发作时删除或改名被传染的文件甚至其它文件，如黑色星期五病毒在破坏部分被触发时将删除执行的文件；

(13) 丢失数据、数据泄密；

(14) 用 DIR 命令显示时，磁盘的卷标发生变化。如巴基斯坦智囊病毒将卷标修改成 (C) Brain；

(15) 系统引导过程变慢。如传染引导区的病毒，一般均能使系统的引导速度变慢；

(16) 系统不承认硬盘或硬盘不能引导系统等。传染主引导区的病毒如大麻、6.4 等将正常的主引导区移到磁盘特定的扇区，而当这些存储有正常主引导区程序的扇区被其它数据占用时，就会出现系统不承认硬盘的现象；

(17) 异常要求用户输入口令。如小球病毒的国内变种苹果病毒等；

(18) 出现对存储系统的异常访问。如当某些病毒运行时出现非法访问磁盘现象；

(19) 键盘上敲入的字符和屏幕上显示的字符不一致；

(20) 文件的建立日期、时间等发生变化。如 1575 病毒传染文件后，被传染文件的建立日期变为染毒时的系统日期；

(21) 通信接口异常。如 Unprinting 传染系统后，当病毒的计数器值为 224 时，系统不能通信；

(22) DIR 显示磁盘目录时出现重复显示现象。如在 A 驱动器中插入一磁盘用 DIR 列 A 盘目录，取出 A 盘换另一张盘插入 A 驱动器列磁盘目录时，屏幕显示的目录内容仍是第一次插入的盘的目录内容；

(23) 错误地执行命令，如要执行 COPY 命令但系统实际执行的是 FORMAT 命令；

(24) 键盘锁定或偷换键盘的功能键；

(25) 中断向量发生变化，文件链接异常；

(26) 执行正常文件导致系统的重新启动。

总而言之，计算机病毒的表现症状相当复杂，而且不同病毒之间的症状又有交叉。虽说计算机用户不能完全根据病毒的症状来判断病毒的种类，但总可以根据某些症状尽早地发现某种病毒有所帮助。

1.9 计算机病毒的标识和特征字

计算机病毒的标识是指计算机病毒本身在特定的寄生环境中确认自身是否存在的标记符号，是指病毒在传染宿主程序时，首先判断该病毒欲传染的宿主是否已染有自身时，从特定的偏移量处提出的用以判断的字符。如 1575 病毒在被传染文件的尾部均标记有 0A0CH，0A0CH 即是 1575 病毒的标识；Liberty 病毒传染 .COM 文件时标识为 Liberty，传染 .EXE 文件时标识为 FFFFH 等。一般计算机病毒都有自己的标识，这种标识的作用是使病毒自身能认识自己，从而能够简单地起到一次传染宿主的作用。病毒的标识一般为：26 个英文字母(包括大、小写)0、1、2、3、4、5、6、7、8、9 以及键盘上所拥有的符号等计算机所能处理的各种符号。多数情况下，病毒用以标识的是 26 个(大写或小写，或大、小写混合的)英文字母及数字。

计算机病毒的特征字有别于病毒标识，特征字是指一种病毒有别于另一种病毒的字符串。一般而言，一种病毒的标识可以作为一种病毒的特征字，而一种病毒的特征字并不一定是病毒的标识。如 1575 病毒的特征字可以是 0A0CH，也可以是从病毒代码中抽出的一组 16 进制的代码：06 1E 8C C0 0E 1F 0E 07 A3 等，前者是 1575 病毒的传染标识，而后者则不是。

关于计算机病毒特征字的提取方法有多种，具体提取方法介绍如下：

(1) 在计算机病毒表现形式出现或破坏部分触发时，病毒在计算机屏幕上出现的信息用来作为病毒的特征字串。例如大麻病毒的提示为："Your PC is now stoned!"等。

(2) 用病毒标识作为病毒的特征字串。

(3) 从病毒代码的任何地方开始取出连续的、不大于 64 且不含空格(ASCII 32)的字节串都可以作为计算机病毒的特征字串。例如洋基病毒的特征串为 FAH 7AH 2CH 00H。从理论上讲，简单地从病毒头部取出连续的 64 字节，则判断的病毒数可达 $256+256^2+\cdots+256^{64}>256^{64}$。但在实际上由于病毒种类繁多，且病毒制造者有可能针对一定的病毒特征修改病毒，因此不一定连续的 64 字节就能完全区分两种不同的病毒。

计算机病毒的特征字串是用户或反病毒工作者鉴别特定计算机病毒的一种标志。目前出现的许多消毒软件都采用了计算机病毒特征字串的鉴别方法。

第二部分　计算机病毒的检测、消除实例

2.1　文件型病毒交叉感染的分析和解毒方法

本文分析了交叉感染后可执行文件的结构，提出了一种实用解毒方法。

1. 单个病毒感染分析与解毒

文件型病毒感染可执行文件必须满足两个基本要求：①加载被感染的可执行文件时，病毒代码先于原代码执行，以进一步传染其它文件；②基于隐蔽病毒自身的考虑，原代码要真实地执行。以上两点决定了可执行文件感染后的结构特点，前者使病毒代码包在原代码周围，形成“外壳”；后者使原代码被妥善保存，从而为解毒、恢复提供了可能。

.EXE 文件被加载时，系统根据 .EXE 文件头中的 CS：IP 参数确定第一条执行语句，所有文件型病毒感染 .EXE 文件时，均将病毒代码附在原代码之后。通过修改文件头中的 CS：IP 参数，使得加载感染后的 .EXE 文件时，病毒代码首先被执行。为保证执行的正确，还修改了文件头中的 SS：IP 参数及总页数：尾页长参数(本文简称 NP：NT)。三对原始的参数保存在病毒代码区，被感染的 .EXE 文件结构如图 2.1(a)所示。

.COM 文件的第一条语句即为首条执行语句，病毒感染 .COM 文件有两种情况：①病毒代码插在原代码之前，首条执行语句即为病毒代码，故加载时病毒先执行，称这类病毒为 A 型；②病毒代码附于原代码之后，.COM 文件头第一条语句被改为 JMP ×××× 或其它跳转语句，加载 .COM 文件后，立即转去执行尾部的病毒代码，之后才执行原代码。原 .COM 文件头被改写的若干条语句完整保存在病毒代码区，称此类病毒为 B 型。感染后 .COM 文件的两种结构见图 2.1 (b)和 2.1(c)。

对于仅感染了单个病毒的可执行文件，其解毒方法如下：对 .EXE 文件，从尾部病毒代码区取出上述三对参数还原旧文件头，再截去尾部的病毒代码；对 A 型病毒感染的 .COM 文件，直接切掉前部分病毒码；对 B 型病毒感染的 .COM 文件，从尾部病毒代码区取出原 .COM 文件头的几条语句还原 .COM 头，然后截去尾部病毒码。不同的病毒保存原文件头时作了不同的处理，因此提取旧文件头还原的方法也是不同的。从这点来看，不存在完全通用的解毒方法，每种病毒均要单独处理。

在仅感染单个病毒的情况下，.COM 文件解毒比 .EXE 文件容易(尤其在手工方式下)，然而一旦文件被交叉感染，情况则变得相反。

2. 交叉感染后可执行文件的结构

由前面的分析可知，病毒每感染一次 .EXE 文件，都附在尾部，同时修改文件头指向尾部。交叉感染后 .EXE 文件尾部形成明显的层次，最终文件头指向最后一次感染的病毒。假设有 V1、V2、V3 三种病毒，其中 V1 为 A 型，V2 和 V3 为 B 型，则三次感染后 .EXE 文件结构如图 2.2(a)；对 .COM 文件，三次感染后 V1 在头部，V2 和 V3 在尾部，结构如图 2.2(b) 。

对图 2.2(a)，感染的次序是 V1→V2→V3；而对图 2.2(b)，却可能有 3 种不同的感染次序：①V1→V2→V3，如图 2.3(a)；②V2→V1→V3，如图 2.3(b)；③V2→V3→V1，如图 2.3