本科毕业论文

（病毒入侵微机的途径与防治研究）

准考准号：____

考 生 单 位_____

邮　　编_____　电话_____

专 业 名 称　　计算机应用

论文提交日期　　2011 年 04 月 27 日

2011 年 04 月 26 日

病毒入侵微机的途径与防治研究

摘要：

目前计算机的应用深入到社会的各行各业，计算机与人们的生产生活密切相关已然成为人们生活的一部分或者说一种生活方式。每件事物都有它的好处和它的坏处，对于计算来说它丰富了我们的生活、方便了我们的工作、提高了生产率、创造了更高的财富价值这是它的好处，但同时伴随计算机的深入应用计算机病毒产生或发展也给我们带来了巨大的破坏和潜在的威胁，这是坏处。对于大多数一般的计算机用户来说，谈到“计算机病毒”似乎觉得它深不可测，无法琢磨。其实计算机病毒是可以预防的，随着计算机的普及与深入，对计算机病毒的防范也在越来越受到计算机用户的重视。作为计算机的使用者，应了解计算机病毒的入侵和防范方法以维护正常、安全的计算机使用和通信环境。因此为了确保计算机能够安全工作，计算机病毒的防范工作，已经迫在眉睫。本论文从计算机病毒概述及入侵途径、计算机病毒防范、计算机病毒治理清楚入手，浅谈计算机病毒的特点及其应对手法。

关键词:计算机病毒　计算机安全　入侵途径　病毒防治

目　　录

计算机病毒的概述

提起计算机病毒，绝大多数计算机的使用者都会深恶痛绝，因为没有“中过招”的人已经是凤毛麟角了。但在谈虎色变之余，很多人对计算机病毒又充满了好奇，对病毒的制造者既痛恨又敬畏。这种复杂的感情实际上很容易理解，就像古人面对大自然的感情一样，因为无法解释风雨雷电，也就只能制造神话，崇拜图腾了。

计算机病毒当然不值得崇拜，它给社会信息化的发展制造了太多的麻烦，每年因为计算机病毒造成的直接、间接经济损失都超过百亿美元。但同时，它也催化了一个新兴的产业——信息安全产业。反病毒软件、防火墙、入侵检测系统、网络隔离、数据恢复技术……这一根根救命稻草，使很多企业和个人用户免遭侵害，在很大程度上缓解了计算机病毒造成的巨大破坏，同时，越来越多的企业加入到信息安全领域，同层出不穷的黑客和病毒制造者做着顽强的斗争。

但稻草毕竟是稻草，救得一时不一定救得一世。目前市场上主流厂商的信息安全产品经过多年的积累和精心的研发，无论从产品线还是从技术角度来讲，都已经达到了相当完善的程度。但是，再好的产品，如果不懂得如何去使用，发挥不了产品真正的优势，又与稻草有什么区别呢？很多用户在被病毒感染以后才想起购买杀毒软件，查杀以后就再也不管，没有定期的升级和维护，更没有根据自己的使用环境的特点，制定相应的防范策略，可以说把产品的使用效率降到了最低，这样的状态，怎能应付日新月异的病毒攻击呢？

那么，如何将手中的稻草变成强大的武器，当危险临近时，能够主动出击，防患于未然呢？笔者认为，关键的问题在于对“对手”的了解。正如我们上面举过的例子，我们现在之所以对很多自然现象习以为常，是因为我们对其成因有了最基础的了解，这样才可能未雨绸缪，配合手中的工具，防患于未然。

一般来讲，凡是能够引起计算机故障，能够破坏计算机中的资源（包括硬件和软件）的代码，统称为计算机病毒。在 1994 年我国颁布实施的《中华人民共和国计算机系统安全保护条例》中，对计算机病毒有如下定义：“计算机病毒是编制或在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码”。

计算机病毒的产生与发展

自从 1987 年发现了全世界首例计算机病毒以来，病毒的数量早已超过 1 万种以上，并且还在以每年两千种新病毒的速度递增，不断困扰着涉及计算机领域的各个行业。计算机病毒的危害及造成的损失是众所周知的，发明计算机病毒的人同样也受到社会和公众舆论的谴责。也许有人会问：“计算机病毒是哪位先生发明的?”这个问题至今无法说清楚，但是有一点可以肯定，即计算机病毒的发源地是科学最发达的美国。

虽然全世界的计算机专家们站在不同立场或不同角度分析了病毒的起因，但也没有能够对此作出最后的定论，只能推测电脑病毒缘于以下几种原因：一、科幻小说的启发；二、恶作剧的产物；三、电脑游戏的产物；四、软件产权保护的结果.

IT 行业普遍认为，从最原始的单机磁盘病毒到现在逐步进入人们视野的手机病毒，计算机病毒主要经历了如下发展阶段。

DOS　引导阶段：

1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”和“石头”病毒。

当时的计算机硬件较少,功能简单,一般需要通过软盘启动后使用。引导型病毒利用软盘得启动原理工作,它们修改系统启动扇区,在计算机启动时首先取得控制权,减少系统内存,修改磁盘读写中断,影响系统工作效率,在系统存取磁盘时进行传播。1989 年,引导型病毒发展为可以感染硬盘,典型的代表有"石头 2"。

DOS　可执行阶段：

1989 年,可执行文件型病毒出现,它们利用 DOS　系统加载执行文件的机制工作,代表为"

耶路撒冷",星期天"病毒,病毒代码在系统执行文件时取得控制权,修改 DOS 中断,在系统调用时进行传染,并将自己附加在可执行文件中,使文件长度增加。1990 年,发展为复合型病毒,可感染 COM 和 EXE 文件。

批处理型阶段:

1992 年,伴随型病毒出现,它们利用 DOS 加载文件的优先顺序进行工作。它感染 EXE 文件时生成一个和 EXE 同名的扩展名为 COM 伴随体;它感染 COM 文件时,改为原来的 COM 文件为同名的 EXE 文件,在产生一个原名的伴随体,文件扩展名为 COM 。这样,在 DOS 加载文件时,病毒就取得控制权。

幽灵、多形阶段 :

1994 年,随着汇编语言的发展,实现同一功能可以用不同的方式进行完成,这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点,每感染一次就产生不同的代码。

生成器阶段 :

1995 年,在汇编语言中,一些数据的运算放在不同的通用寄存器中,可运算出同样的结果,随机的插入一些空操作和无关指令,也不影响运算的结果,这样,一段解码算法就可以由生成器生成。当生成的是病毒时,这种复杂的称之为病毒生成器和变体机就产生了。具有典型代表的是"病毒制造机"VCL

网络、蠕虫阶段:

1995 年,随着网络的普及,病毒开始利用网络进行传播,它们只是以上几代病毒的改进。在非 DOS 操作系统中,"蠕虫"是典型的代表,它不占用除内存以外的任何资源,不修改磁盘文件,利用网络功能搜索网络地址,将自身向下一地址进行传播,有时也在网络服务器和启动文件中存在。

Windows 病毒阶段 :

1996 年,随着 Windows 和 Windows95 的日益普及,利用 Windows 进行工作的病毒开始发展,它们修改(NE,PE) 文件,这类病毒的机制更为复杂,它们利用保护模式和 API 调用接口工作,清除方法也比较复杂。

宏病毒阶段 ：

1996 年,随着 Windows Word 功能的增强,使用 Word 宏语言也可以编制病毒,这种病毒使用类 Basic 语言,编写容易,感染 Word 文档文件。在 Excel 和 AmiPro 出现的相同工作机制的病毒也归为此类。

互连网阶段 ：

1997 年,随着因特网的发展,各种病毒也开始利用因特网进行传播,一些携带病毒的数据包和邮件越来越多,如果不小心打开了这些邮件,机器就有可能中毒。

计算机病毒的特性

寄生性。计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

传染性。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪.

潜伏性。有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。

隐蔽性。计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序，如不经过程序代码 分析或计算机病毒代码扫描，病毒程序与正常程序是不容易区别开来的。

破坏性。计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏 。通常表现为：增、删、改、移。

可触发性。病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

除了上述五点外，计算机病毒还具有不可预见性、衍生性、针对性、欺骗性、持久性等特点。正是由于计算机病毒具有这些特点，给计算机病毒的预防、检测与清除工作带来了很大的难度。

随着计算机应用的不断发展病毒又出现一些新的特性如：

利用微软漏洞主动传播、局域网内快速传播、以多种方式传播、大量消耗系统与网络资源、双程序结构、用即时工具传播病毒、病毒与黑客技术的融合、远程启动。

按照科学的、系统的、严密的方法，计算机病毒可分类如下：按照计算机病毒属性的方法进行分类，计算机病毒可以根据下面的属性进行分类：

（1） 按病毒存在的媒体

根据病毒存在的媒体，病毒可以划分为网络病毒，文件病毒，引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件（如：COM，EXE，DOC 等），引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR），还有这三种情况的混合型，例如：多型病毒（文件和引

导型）感染文件和引导扇区两种目标，这样的病毒常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

（2）按病毒传染的方法

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒，驻留型病毒感染计算机后，把自身的内存驻留部分放在内存（RAM）中，这一部分程序挂接系统调用并合并到操作系统中去,他处于激活状态,,一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

（3）按病毒破坏的能力

无害型：除了传染时减少磁盘的可用空间外，对系统没有其它影响。

无危险型：这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

危险型：这类病毒在计算机系统操作中造成严重的错误。

非常危险型： 这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其它的程序产生的错误也会破坏文件和扇区，这些病毒也按照他们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其它操作系统造成破坏。例如：在早期的病毒中，有一个“Denzuk”病毒在 360K 磁盘上很好的工作，不会造成任何破坏，但是在后来的高密度软盘上能引发大量的数据丢失。

（4）按病毒的算法

伴随型病毒,这一类病毒并不改变文件本身,它们根据算法产生 EXE 文件的伴随体,具有同样的名字和不同的扩展名（COM），例如：。病毒把自身写入 COM 文件并不改变 EXE 文件，当 DOS 加载文件时，伴随体优先被执行到，再由伴随体加载执行原来的 EXE 文件。

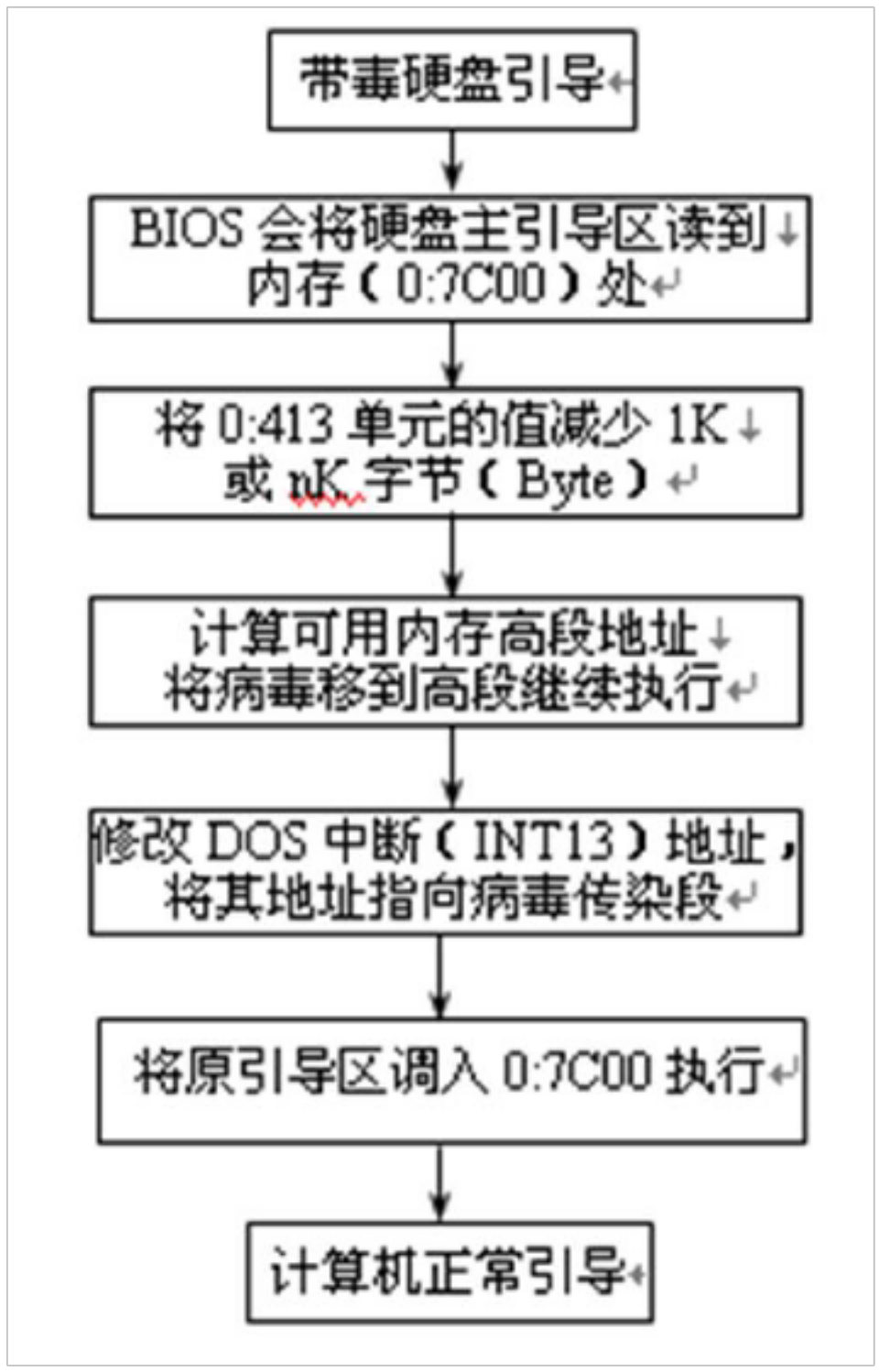
“蠕虫”型病毒，通过计算机网络传播，不改变文件和资料信息，利用网络从一台机器的内存传播到其它机器的内存，计算网络地址，将自身的病毒通过网络发送。有时它们在系统存在，一般除了内存不占用其它资源。

寄生型病毒 除了伴随和“蠕虫”型，其它病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播，按其算法不同可分为：练习型病毒，病毒本身包含错误，不能进行很好的传播，例如一些病毒在调试阶段。

诡秘型病毒 它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

变型病毒（又称幽灵病毒） 这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的作法是一段混有无关指令的解码算法和被变化过的病毒体组成。

（5）按计算机病毒的工作方式



2. 文件型病毒的工作方式

在目前已知的病毒中，大多数属于文件型病毒。文件型病毒一般只传染磁盘上的可执行文件（COM、EXE）。在用户调用染毒的可执行文件时，病毒首先被运行，然后病毒驻留内存伺机传染其他文件或直接传染其他文件。其常见的传染方式是附着于正常程序文件，成为程序文件的一个外壳或部件。

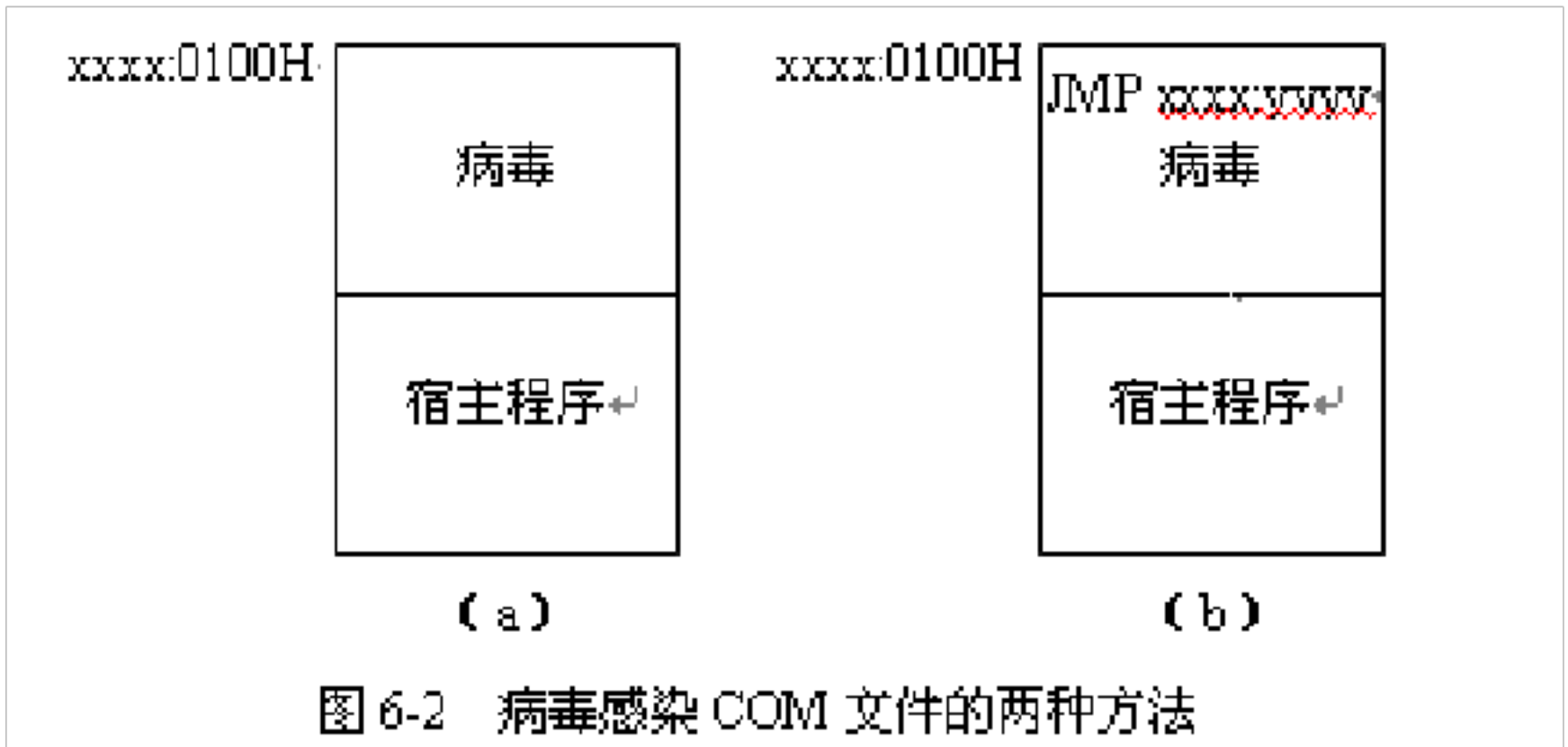
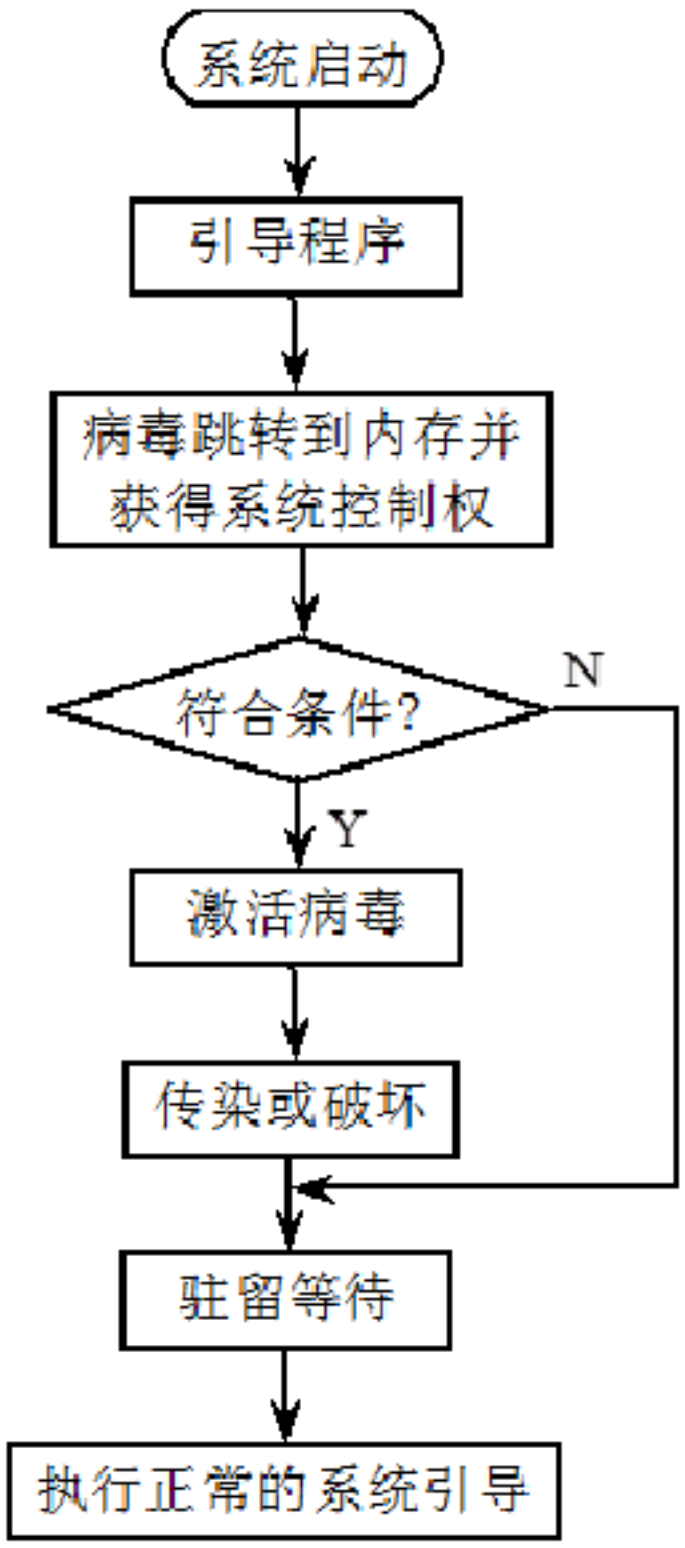
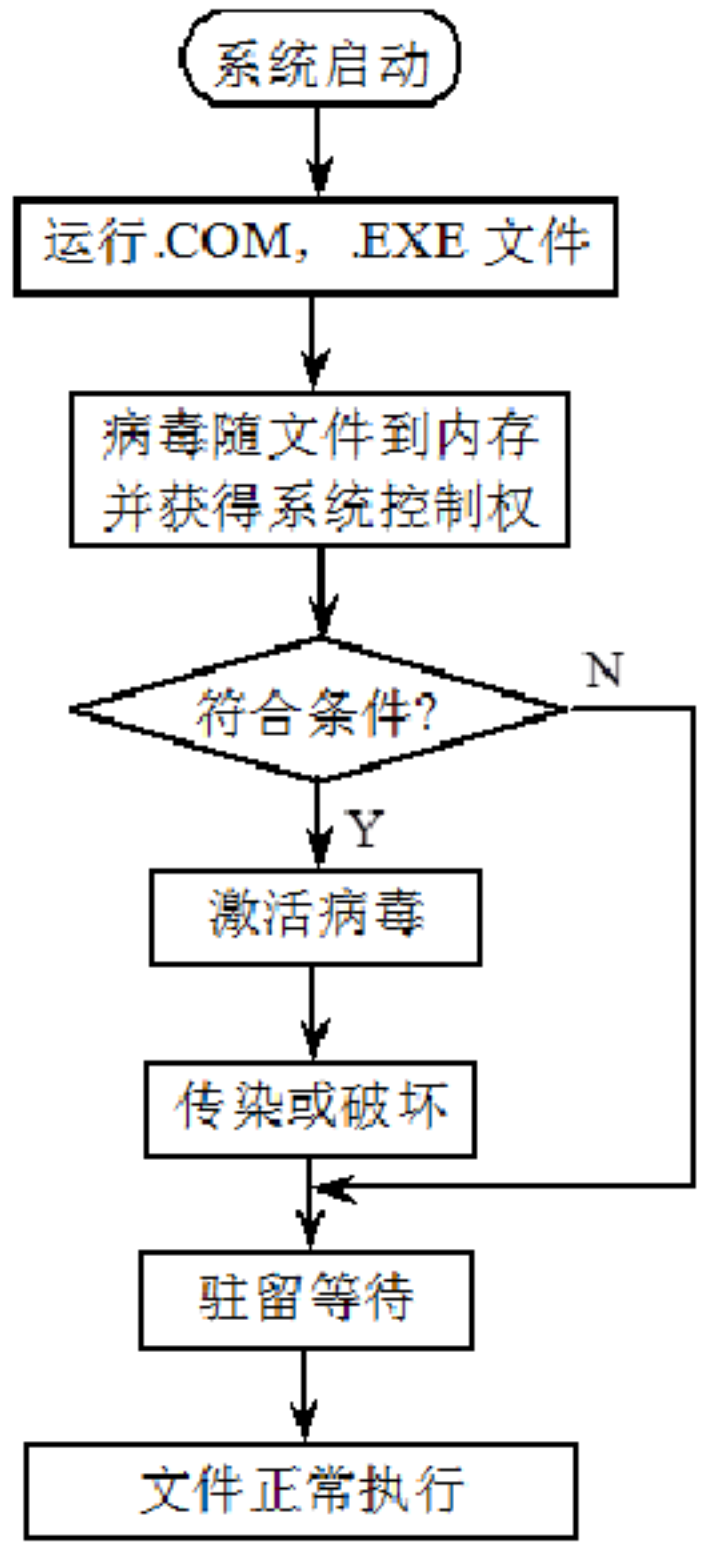


图 6-2　病毒感染 COM 文件的两种方法





（a）引导型病毒　　（b）文件型病毒

3.　混和型病毒工作方式

混和型病毒在传染方式上兼具引导型病毒和文件型病毒的特点。这种病毒的原始状态是依附在可执行文件上，以该文件为载体进行传播。当被感染文件执行时，会感染硬盘的主引导记录。以后用硬盘启动系统时，就会实现从文件型病毒转变为引导型病毒。，，主要感染 COM 、EXE 和 MBR 。它将自己附着在可执行文件的尾部，将破坏性的代码放入 MBR 中，然后清除硬盘中的文件

4.　宏病毒的工作方式

宏病毒是利用宏语句编写的。它们通常利用宏的自动化功能进行感染，当一个感染的宏被运行时，它会将自己安装在应用的模板中，并感染应用创建和打开的所有文档。Office中的 Word 、Excel 和 PowerPoint都有宏。

5. Java病毒工作方式

Java是由 Sun 公司创建的一种用于互联网环境中的编程语言。Java应用程序不会直接运行在操作系统中，而是运行在 Java虚拟机（JVM ）上。因此用 Java编写的应用程序的移植性非常强，包括现在的手机中的一些程序也是用 Java编写的。

Java Apple是一种内嵌在 HTML 网页中的可携式 Java小程序。具有 Java功能的浏览器可以运行这个小程序。Java Apple可供 Web 开发人员建立含有功能更丰富的交互式动态 Web 网页。它们会在使用者访问网页时被执行。黑客、病毒作者或其他恶意人士可能会用 Java恶意程序代码当作武器攻击使用者的系统

6.　网络病毒工作方式

随着互联网的高速发展，计算机病毒从原来的磁盘进行传播发展到现在的通过网络的漏洞进行传播。到如今，网络病毒已经成为计算机网络安全的最大威胁之一。网络病毒中又以蠕虫病毒出现最早，传播最为广泛，例如“冲击波”、“红色代码”病毒等。

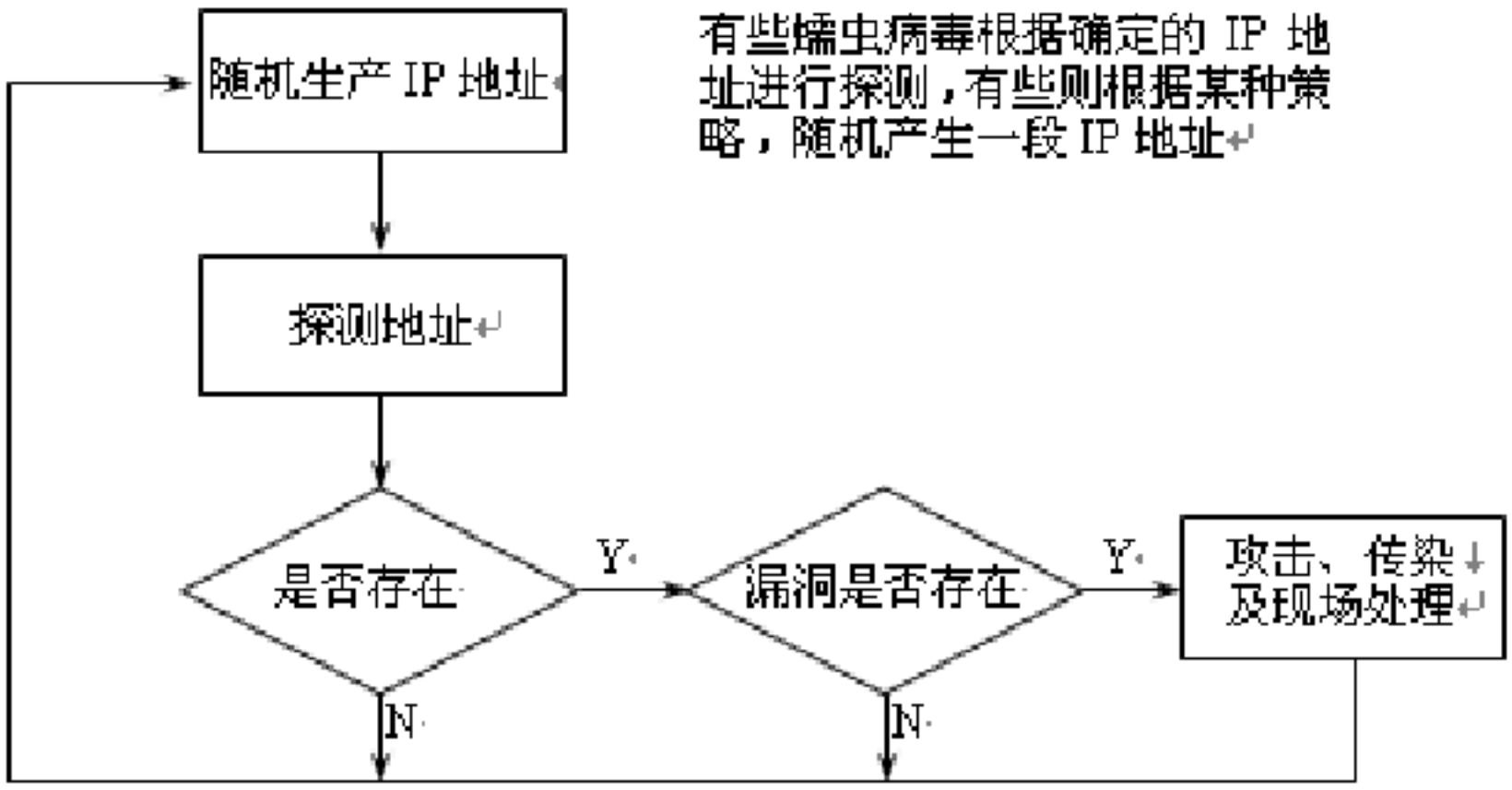


图 6-3　蠕虫病毒的工作流程

7.　脚本病毒工作方式

脚本病毒也是一种特殊的网络病毒。脚本是指从一个数据文档中执行一个任务的一组指令，它也是嵌入到一个文件中，常见的是嵌入到网页文件中。脚本病毒依赖于一些特殊的脚本语言（例如 VBScript、JavaScript、Jscript、PerlScript、PHP、Flash 等）。有些脚本语言，例如 VBScript（Visual Basic Script）以及 JavaScript 病毒，必须通过 Microsoft 的 Windows Scripting Host（WSH ）才能够激活执行以及感染其他文件

8. PE 病毒工作方式

PE 病毒，是指感染 Windows PE 格式文件的病毒。PE 病毒是目前影响力极大的一类病毒。PE 病毒同时也是所有病毒中数量极多、破坏性极大、技巧性最强的一类病毒。如 FunLove、“中国黑客”等病毒都属于这个范畴。

计算机病毒传播途径关键环节

计算机病毒要实现传播，有三个关键环节:

(1)带毒文件的迁移。即感染病毒的文件从一台计算机复制、迁移到另一台计算机。

(2)计算机操作者的触发。计算机病毒是寄生在受感染文件上的，只有计算机操作者执行或者打开受感染的文件，计算机病毒才有执行的机会，才能取得主机的控制权。

(3)感染。病毒在取得主机的控制权后，就随时可以寻找合适的目标文件进行感染，把病毒副本嵌入到目标文件中。

计算机病毒入侵的途径

随着社会的不断进步科学的不断发展计算机病毒的种类也越来越多，但终究万变不离其宗！那他们是靠什么途径传播的了？

目前比较常见的病毒入侵的途径有几种：

1　木马入侵

木马有可能是黑客在已经获取我们操作系统可写权限的前提下，由黑客上传的;也可能是我们不小心，运行了包含有木马的程序，最多的情况还是我们防范意识不强，随便运行了别人发来的“好玩”的程序。所以，我们自己要多加注意，不要随意打开来历不明的电子邮件及文件，不要随便运行别人发来的软件，之前要查毒。安装木马查杀软件并及时更新。

2　共享入侵

是为了方便远程管理而开放的共享，这个功能对个人用户来说用处不大，反而给黑客入侵提供了便利。个人用户应禁止自动打开默认共享，给自己的帐户设置复杂密码，最好是数字、字母以及特殊符号相结合，安装防火墙。

3　漏洞入侵

（Internet Information Server）服务为 Web 服务器提供了强大的 Internet 和 Intranet 服务功能。主要通过端口 80 来完成操作，因为作为 Web 服务器，80 端口总要打开，具有很大的威胁性。长期以来攻击 IIS 服务是黑客惯用的手段，远程攻击者只要使用 webdavx3 这个漏洞攻击程序和 telnet 命令就可以完成一次对 iis 的远程攻击，这种情况多是由于企业管理者或网管对安全问题关注不够造成的。我们要时刻关注微软官方站点，及时安装 iis 的漏洞补丁。

4　网页恶意代码入侵

在我们浏览网页的时候不可避免的会遇到一些不正规的网站，当打开一个网页后，就发现注册表和 IE 设置被修改了，这就是网页恶意代码造成的破坏，但是这种网页恶意代码有着更大的危害，很有可能在我们不知道的情况下下载木马，蠕虫等病毒，同时把我们的私人信息，如银行帐号，QQ 帐号，游戏帐号泄露出去。要避免被网页恶意代码感染，首先关键是不要轻易去访问一些并不信任的站点，尤其是一些带有美女图片等的网址。否则往往不经易间就会误入网页代码的圈套。。但是这个并不能真正防止网页恶意代码的攻击,因为这些恶意代码有可能在任何地方出现。我们应尽量避免从 Internet 下载不知名的软件、游戏程序，即使从知名的网站下载的软件也要及时用最新的木马查杀程序对软件和系统进行扫描,这样才能减少误中病毒的机会。安装具有注册表实时监控功能的防护软件，做好注册表的备份工作，禁用 Remote Registry Service 服务。

5 通过光盘

由于光盘的容量大，对于只读式光盘，不能进行写操作，因此光盘上的病毒不能清除。为了使软件及相关的数字资源的传播而得到广泛应用。一些不法分子将病毒刻录到光盘中让用户在不知不觉中被隐藏与其上的病毒感染从而入侵你的电脑系统。

6 通过 U 盘

U 盘作为当前人们最方便、最常用的存储介质和文件拷贝、携带工具，同时病毒的传播中发挥了重要的作用。

7 通过网络

计算机网络特别是 Internet 的普及，给病毒的传播提供了便捷的途径。计算机病毒可以附着在正常文件中，当你从网上下载一个被感染的程序或文件，并在你的计算机上未加任何防护措施的情况下运行它，病毒就传染过来了。

通过 Internet 传播病毒的方式很多，包括 FTP 文件下载、访问恶意 WWW 网站、P2P 文件下载、即时通讯等等。人们使用 Internet 的频率是如此之高，使得 Internet 已是计算机病毒的第一传播途径。

知道了计算机病毒的传播途径，那他们都是通过什么样的方式传播的呢？

计算机病毒的入侵方式

如按其入侵的方式来分为以下几种：

a、源代码嵌入攻击型

从它的名字我们就知道这类病毒入侵的主要是高级语言的源程序，病毒是在源程序编译之前插入病毒代码，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。当然这类文件是极少数，因为这些病毒开发者不可能轻易得到那些软件开发公司编译前的源程序，况且这种入侵的方式难度较大，需要非常专业的编程水平。

b、代码取代攻击型

这类病毒主要是用它自身的病毒代码取代某个入侵程序的整个或部分模块，这类病毒也少见，它主要是攻击特定的程序，针对性较强，但是不易被发现，清除起来也较困难。

c、系统修改型

这类病毒主要是用自身程序覆盖或修改系统中的某些文件来达到调用或替代操作系统中的部分功能，由于是直接感染系统，危害较大，也是最为多见的一种病毒类型，多为文件型病毒。

d、外壳附加型

这类病毒通常是将其病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。目前大多数文件型的病毒属于这一类。

知道了计算机病毒的特性、分类和传播途径，找到了病根，只要对症下药就 OK 了！

计算机病毒防范和清除的基本原则和技术

计算机病毒的存在和传播对用户造成了很大的危害，为了减少信息资料的丢失和破坏，这就需要在日常使用计算机时，养成良好的习惯，预防计算机病毒。并且需要用户掌握一些查杀病毒的知识，在发现病毒时，及时保护好资料，并清除病毒。

计算机病毒防范，是指通过建立合理的计算机病毒防范体系和制度，及时发现计算机病毒入侵，并采取有效的手段阻止计算机病毒的传播和破坏，恢复受影响的计算机系统和数据。

原则以防御计算机病毒为主动，主要表现在检测行为的动态性和防范方法的广泛性。

计算机病毒预防是在计算机病毒尚未入侵或刚刚入侵，就拦截、阻击计算机病毒的入侵或立即警报。目前在预防计算机病毒工具中采用的主要技术如下：

1、特征代码技术

特征代码法被早期应用于 SCAN,CPAV 等著名病毒检测工具中，目前被认为是用来检测已知病毒的最简单、开销最小的方法。防毒软件在最初的扫毒方式是将所有病毒的病毒码加以剖析，并且将这些病毒独有的特征搜集在一个病毒码资料库中，每当需要扫描该程序是否有毒的时候，启动杀毒软件程序，以扫描的方式与该病毒码资料库内的现有资料一一比对，如果两方资料皆有吻合之处的话，既判定该程序已遭病毒感染。特征代码法的实现步骤如下:

1)采集已知

病毒样本。如果病毒既感染 com 文件，又感染 EXE 文件，那么要对这种病毒要同时采集 COM 型病毒样本和 EXE 型病毒样本。

2)在病毒样本中，抽取病毒特征代码。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)检测文件。打开被检测文件，在文件中搜索，检查文件中是否含有病毒数，根据数据库中的病毒特征代码。如果发现病毒特征代码，由特征代码与病毒一一对应，便可以断定，被查文件所感染的是何种病毒。

2、校验和法技术

通常，大多数的病毒都不是单独存在的，它们大都依附或寄生于其它的文档程序，所以被感染的程序会有档案大小增加的情况产生或者是档案日期被修改的情形。这样防

毒软件在安装的时候会自动将硬盘中的所有档案资料做一次汇总并加以记录，将正常文件的内容计算其校验和，将该校验和写入文件中或写入别的文件中保存。在每次使用文件前，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，它既可发现已知病毒又可发现未知病毒。运用校验和法检查病毒采用三种方式：

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。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。

3、行为监测法技术

利用病毒的特有行为特征性来监测病毒的方法，称为行为监测法。通过对病毒多年的观察、研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

4、软件模拟技术

多态性病毒每次感染都会变化其病毒密码，对付这种病毒，特征代码法失效。因为多态性病毒代码实施密码化，而且每次所用密钥不同，把染毒的病毒代码相互比较，也各不相同，无法找出可能的作为特征的稳定代码。虽然行为检测法可以检测多态性病毒，但是在检测出病毒后，因为不知病毒的种类，难于做杀毒处理，由此出现了一种新的软件模拟法。

有了病毒的一些基本知识后现在我们就可以来检查你的电脑中是否含有病毒，要知道这些我可以按以下几个方法来判断。

判断病毒的方法

1、反病毒软件的扫描法

这恐怕是我们绝大数朋友首选，也恐怕是唯一的选择，现在病毒种类是越来越多，隐蔽的手段也越来越高明，所以给查杀病毒带来了新的难度，也给反病毒软件开发商带来挑战。但随着计算机程序开发语言的技术性提高、计算机网络越来越普及，病毒的开发和传播是越来越容

易了，因而反病毒软件开发公司也是越来越多了。但目前比较有名的还是那么几个系统的反病毒软件，如金山毒霸、KV300、KILL、PC-cillinVRV、瑞星、诺顿等。至于这些反病毒软件的使用在此就不必说叙了，我相信大家都有这个水平！

2、观察法

这一方法只有在了解了一些病毒发作的症状及常栖身的地方才能准确地观察到。如硬盘引导时经常出现死机、系统引导时间较长、运行速度很慢、不能访问硬盘、出现特殊的声音或提示等上述在第一大点中出现的故障时，我们首先要考虑的是病毒在作怪，但也不能一条胡洞走到底，上面我不是讲了软、硬件出现故障同样也可能出现那些症状嘛！对于如属病毒引起的我们可以从以下几个方面来观察：

a、内存观察

这一方法一般用在 DOS 下发现的病毒，我们可用 DOS 下的“mem/c/p ”命令来查看各程序占用内存的情况，从中发现病毒占用内存的情况（一般不单独占用，而是依附在其它程序之中），有的病毒占用内存也比较隐蔽，用“mem/c/p ”发现不了它，但可以看到总的基本内存 640K 之中少了那么区区 1k 或几 K。

b、注册表观察法

这类方法一般适用于近来出现的所谓黑客程序，如木马程序，这些病毒一般是通过修改注册表中的启动、加载配置来达到自动启动或加载的，一般是在如下几个地方实现：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windwos\CurrentVersion\Run]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windwos\CurrentVersionRunOnce]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windwos\CurrentVersionRunSevices]

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion

\RunOnce]

等等，在其中对注册表中可能出现的地方会有一个比较详尽的分析。

c、系统配置文件观察法

这类方法一般也是适用于黑客类程序，、（Win9x/WinME ）和启动组中，″shell″=项，“load= ”、“run= ”项，这些病毒一般就是在这些项目中加载它们自身的程序的，注意有时是修改原有的某个程序。我们可以运行 Win9x/。具体也可参考我的《通通透透看木马》一文。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/306052055103010210