# 第5章 计算机病毒概述

- 在生物学中，病毒是那些能够侵入动物体并给动物体带来疾病的一种微生物。
- 计算机病毒则是在计算机之间传输，并自己进行复制而给计算机系统带来一定后果的一类程序。
- 计算机病毒是随着计算机软件技术的发展而逐渐产生的，是计算机科学技术高度发展与计算机文明得不到完善这样一种不平衡发展的结果。

# 5.1 计算机病毒的发生和发展

- 5.1.1计算机病毒的起源
- 在1977年夏季Tkomas.J.Ryan推出了轰动一时的科幻小说，名叫《The Adolescence of P-1》。
- 在这本书中，作者构造了一种神秘的、能自我复制、利用信息通道传播的计算机程序，称为计算机病毒。
- 这些病毒飘泊于电脑之内，游荡于硅片之间，控制了7000多台计算机的操作系统，引起混乱和不安。
- 从科幻到大规模泛滥仅用了十多年时间，故有人认为计算机病毒起源于科幻小说。

- 作为计算机病毒起源的另一种说法是恶作剧说。
- 即一些人为了显示自己的计算机知识方面的天资，或出于报复心理，编写了恶作剧程序，并通过软盘交换特别是游戏盘的交换，引起计算机病毒的广泛传染
- 软件制造商制造病毒程序
- 计算机病毒的产生是一个历史问题，它是计算机科学技术高度发展与计算机文明得不到完善这样一种不平衡发展的结果。

# 5.1.2计算机病毒的发展历史

- 1977年，在科幻小说中提出了计算机病毒，
- 1983年，美国计算机安全专家Fred Cohen通过实验证明了产生计算机病毒的现实性，制造了世界上第一例计算机病毒。并在1984年9月的加拿大多伦多国际信息处理联合会计算机安全技术委员会举行的年会上，发表了题为“计算机病毒：原理和实验”的论文。其后，又发表了“计算机和安全”等论文。

- 1987年年初，美国东部一所医疗中心存储在计算机系统中的一些病历突然消失，经查是计算机病毒在作怪。
- 这年的12月下旬圣诞节前夕，计算机病毒侵袭了IBM公司的国际电子信息网，向每个曾使用过该信息网的用户发出了相同的贺信，大量连锁信件使得该网络因不堪重负而瘫痪，这就是IBM圣诞树病毒。
- 1988年11月2日的蠕虫病毒攻击Internet则把早期计算机病毒推向了高潮。一夜之间造成与该网络系统连接的6000多台计算机停机，其中包括美国国家航空和航天局、军事基地和主要大学，直接经济损失达9200多万美元。

- 早期的计算机病毒有感染引导区和文件两类。
- 直接修改部分中断向量表，而且不隐藏不加密自身代码，因此很容易被查出和解除。
- 其代表是：感染引导区的Stone病毒、小球病毒和磁盘杀手等，感染文件的耶路撒冷病毒、维也纳病毒和扬基病毒等。其中扬基病毒略有对抗反病毒手段
- 此后一些能对自身进行简单加密的病毒相继出现，其代表是1366、1824、1741等。
- DIR-2病毒的出现则改变了修改中断向量表方法，并且也改变了传染文件的病毒通常把病毒程序体直接链接在文件处的方法
- 新世纪病毒类型的计算机病毒的出现，则标志着传染引导区和文件的双料病毒的产生。

- 以CIH病毒为代表的纯32位Win 95、Win 98计算机病毒的出现，标志着以DOS系统攻击对象的计算机病毒将逐渐让位于针对Windows的病毒。
- 数千种Word宏病毒的出现，则形成了计算机病毒的另一派系，由于宏病毒编写容易，互联网上又较多采用Word格式进行交流，从而通过互联网传播更加快了这类病毒的流传。
- 变换自身代码的变形病毒也连续出现，使得一些病毒扫描软件时常漏查漏杀，象“台湾2号变形王”其病毒代码可变无限次，并且变形复杂，几乎达到了不可解除的状态。
- Mutation Engine（变形金刚或称变形病毒生产机）遇到普通病毒后能将其改造成为变形病毒，给清除计算机病毒带来极大困难。

- 红色代码病毒的出现，标志着病毒与黑客程序的结合。
- 冲击波病毒的肆逆提醒我们时刻警惕病毒的危害，同时对软件系统漏洞存在的担忧
- 美国《连线》杂志2011年10月7日在其网站首次曝光克里奇空军基地大约两周前发现遭电脑病毒入侵的消息，当后方控制人员在计算机系统平台操控无人机在阿富汗、伊拉克等地执行远程飞行任务时，这种植入式病毒可记录下控制人员的每一次按键操作，类似木马行为。

- 现阶段尚未发现信息丢失或泄露事件。
- 病毒本身无碍控制人员操控无人机执行海外任务。
  迄今无法确认这一病毒是否属恶意病毒。
- 病毒如何入侵基地计算机系统也仍未知。
- 控制系统没有接入互联网, 但独立系统并不意味着平台的绝对安全。
- 2009年,伊拉克武装人员借助一款廉价软件成功入侵无人机图像系统,获取无人机拍摄的动态画面。

- 控制系统的后台独立,但前端却有许多开放式端口,使病从“口”入成为可能。
- 控制系统可能遭“流氓程序”攻击。因为克里奇空军基地借助移动存储设备在电脑间传输信息, 这种信息传输方式在美军基地的计算机系统中已不多见。
- 移动存储设备是病毒感染和传播的载体。
- 计算机病毒在抗病毒技术发展的同时，自己也在不断发展，编制者手段越来越高明，病毒结构也越来越特别，
- 抗击病毒有待于我们的研究和开发。

# 5.2计算机病毒的定义

- 计算机病毒实质上是指一段程序，它们通过把自己的一个副本附加到另一个程序上面进行复制。它们不仅出现在可执行程序中，也可通过嵌套在数据文件中进行扩散。
- 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程序代码。

# 5.2.2计算机病毒的特点

- 计算机病毒一般具有如下重要特点：
- 一段可存储可执行的非法程序。
  直接或间接地运行，
  与合法程序争夺系统的控制权。
  隐藏在可执行程序和数据文件中不易被人们察觉和发现
- 有广泛的传染性。
  传染性是计算机病毒的特征。不具传染性的破坏程序不是计算机病毒。
  一个计算机病毒能够主动将自身的复制品或变体传染到其他对象上去，
  程序，系统中的某些部位
  启动带毒系统或运行带毒程序，
  掌握系统控制权，传染到整个系统或硬盘上。
  传染局部网络、大型计算机中心或多用户系统。

# 计算机病毒的特点

- 具有潜伏性。

  依附于其他媒体而寄生。

  可以在几周或者几个月甚至几年内隐藏在合法文件中。

- 具有隐蔽性

  非授权加载到被感染对象

  在进入系统并破坏数据的过程中通常不被用户感觉到，而等到有明显变化时，往往计算机病毒已造成危害。

- 对系统危害大，有时难以清除。

  破坏系统，删除、修改数据，还占用系统资源、干扰机器运行。

  所破坏的数据、程序和操作系统往往难以恢复。

  病毒有时不易清除。

# 计算机病毒的特点

- 具有欺骗性，
- 某些病毒常以某种特殊的表现方式，引诱欺骗用户触发、激活病毒。从而实施其感染、破坏功能。
- 有的病毒伪装成文件夹图标，或者图片图标
- 由于是可执行文件，当然不会轻易双击，但如果病毒具有把扩展名隐蔽起来功能，则会使用户上当。

# 计算机病毒的特点

- 甚至还有冒充清除病毒，善意提醒的。如情书病毒的变种VBS.LoveLettrr.F,传播该病毒的电子邮件附件名为”VirusWarming.jpg.vbs”,主题为“dangerous virus warning”，
- 其内容是“There is a dangerous virus circulating. Please click attached picture to view it and learn to avoid it
- 引诱用户点击实际上是VBS脚本而非JPG图片的程序。

# 5.3计算机病毒的分类

- 计算机病毒的分类取决于所采用的分类标准。
- 按给计算机系统带来后果的不同来划分，
- 恶性病毒和“良性”病毒。
- 恶性病毒是指那些一旦发作或在传染过程中会破坏系统数据，删除文件，摧毁计算机系统的危害性极大的计算机病毒。

  黑色星期五病毒，每逢星期五又是13日，就会删除磁盘上和系统中所有正在执行的文件

  磁盘杀手病毒在发作时，会把硬盘上的数据一块块破坏，直至全部破坏为止。

- “良性”病毒是指那些只是为了表现自己，并不破坏系统和数据的计算机病毒
- 会大量占用CPU资源，增加系统开销，降低系统工作效率。
- 如1575病毒，它常驻内存，感染COM文件和EXE文件。该病毒发作时，就会在屏幕上显示“绿毛虫”的信息，并不破坏系统和文件。
- “良性”病毒并非没有危害，它们会大量占用CPU资源，增加系统开销，降低系统工作效率
- 1575病毒在发作时，就会影响程序的正常执行，只是危害性相对于恶性病毒来讲要小。但在用户缺乏对病毒和系统的了解情况下，也会产生较大的破坏性。

- “良性”病毒必然会降低系统运行速度，
- “良性”只是一个相对的概念，它也是对计算机系统的非授权入侵，是对系统正常工作的一种干扰和破坏。
- 决不能对所谓的“良性”病毒掉以轻心，更不能出于恶作剧的想法去制造病毒。

- 另一种划分方法：按病毒的寄生和传染方式来划分，文件型病毒和系统引导型病毒以及混合型病毒。
- 文件型病毒：专门感染可执行文件（以EXE和COM为主）的计算机病毒。

病毒与可执行文件链接。

运行被感染的文件，病毒获得系统控制权，驻留内存监视系统的运行，寻找满足传染条件的宿主程序进行传染。

黑色星期五病毒，DIR-2病毒，瀑布病毒和维也纳病毒就是常见的文件型病毒。

文件型病毒的症状是染毒的可执行文件字节明显增大，系统可用空间减少，显示非法信息以及覆盖重要文件，造成系统死机等。

一些文件型病毒如DIR-2病毒并不会使感染病毒的程序字节增加。

感染带有宏能力的数据文件的计算机宏病毒则是一代新的文件型病毒。

- 系统引导型病毒是常驻计算机引导区，通过改变计算机引导区的正常分区来达到破坏目的的。

磁盘格式化后，会在引导扇区建立操作系统的引导记录。

硬盘，则有两个引导区，一个是主引导区，另一个是DOS引导区又称逻辑引导区；

软盘，只有一个引导区。

引导区内所存储的内容应该是正常的引导记录。

系统引导型病毒用病毒程序的全部或部分来取代正常的引导记录，把正常的引导记录隐藏在磁盘的其它存储空间中。

磁盘的引导区是磁盘正常工作的先决条件，系统引导型病毒在系统启动时，就获得了控制权，从而使得这类病毒具有很大的传染性和危害性。

- 在防治计算机病毒技术提高的同时，病毒程序制造者的手段也越来越高，
- 有些计算机病毒既感染引导区又感染可执行文件，即出现了所谓混合性病毒，
- 新世纪病毒能传染硬盘的主引导扇区和所有在系统中执行的文件。

# 5.4计算机病毒命名规则

- 按照病毒发作时间命名，如黑色星期五病毒，米氏病毒，米开朗基罗的生日3月6日发作；
- 按照病毒发作症状命名，如小球病毒，发作时在屏幕上出现小球而不断运动，杨基病毒发作时奏“Yankee Dodle”的美国民歌；
- 按照病毒字节长度命名：如幽灵病毒因为病毒代码长度为3544，故又成为3544病毒。

- 国际上，科学的命名方式是三元组命名规则：
- <病毒前缀>.<病毒名>.<病毒后缀> 。
- 病毒前缀是指病毒的种类，区别病毒的种族进行分类；
- 木马病毒的前缀 Trojan ，蠕虫病毒的前缀是 Worm 等等。
- 病毒名是指病毒的家族特征，区别和标识病毒家族的，如CIH病毒的家族名都是统一的“ CIH ”，振荡波蠕虫病毒的家族名是“ Sasser ”。
- 病毒后缀是指病毒的变种特征，区别具体某个家族病毒的某个变种的。一般采用英文中的26个字母来表示，如Worm.Sasser.b就是指 振荡波蠕虫病毒的变种B；
- 如果该病毒变种非常多，可以采用数字与字母混合表示变种标识。

- 一个病毒的前缀对于快速判断该病毒属于哪种类型的病毒有非常大的帮助。
- 通过判断病毒类型，对病毒有大概的评估
- 通过病毒名可查找资料等方式进一步了解该病毒的详细特征。
- 病毒后缀能知道现在的病毒是哪个变种。

- 1、系统病毒
- 系统病毒的前缀为：Win32、PE、Win95、W32、W2K等。公有特性是可以感染windows操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如CIH病毒。
- 2、蠕虫病毒
- 蠕虫病毒的前缀是：Worm。公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波(阻塞网络)，小邮差(发带毒邮件)等。

- 3、木马病毒
- 木马病毒前缀是：Trojan，黑客病毒前缀名一般为 Hack 。
- 一般的木马如QQ消息尾巴木马 Trojan.QQ3344 ， 还有针对网络游戏的木马病毒如 Trojan.LMir.PSW.60 。
- 病毒名中有PSW或者PWD之类的一般表示这个病毒有盗取密码的功能
- 黑客病毒网络枭雄（Hack.Nether.Client）

- 4、脚本病毒
- 脚本病毒的前缀是：Script。公有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码(Script.Redlof)。脚本病毒还会有如下前缀：VBS、JS(表明是何种脚本编写的)，如欢乐时光(VBS.Happytime)、十四日(Js.Fortnight.c.s)等。
- 5、宏病毒
- 宏病毒也是脚本病毒的一种，由于特殊性，通常单独算成一类。宏病毒的前缀是：Macro，第二前缀是：Word、Word97、、Excel、Excel97。
- 凡是只感染WORD97及以前版本WORD文档的病毒采用Word97做为第二前缀，格式是：Macro.Word97；凡是只感染WORD97以后版本WORD文档的病毒采用Word做为第二前缀，格式是：Macro.Word；
- 凡是只感染EXCEL97及以前版本EXCEL文档的病毒采用Excel97做为第二前缀，格式是：Macro.Excel97；凡是只感染EXCEL97以后版本EXCEL文档的病毒采用Excel做为第二前缀，格式是：Macro.Excel，依此类推。

- 6、后门病毒
- 后门病毒的前缀是：Backdoor。公有特性是通过网络传播，给系统开后门，带来安全隐患。如IRC后门Backdoor.IRCBot 。
- 7、病毒种植程序病毒
- 公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者（Dropper.BingHe2.2C）、MSN射手(Dropper.Worm.Smibag)等。
- 8．破坏性程序病毒
- 破坏性程序病毒的前缀是：Harm。公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化C盘（Harm.formatC.f）、杀手命令（Harm.Command.Killer）等。

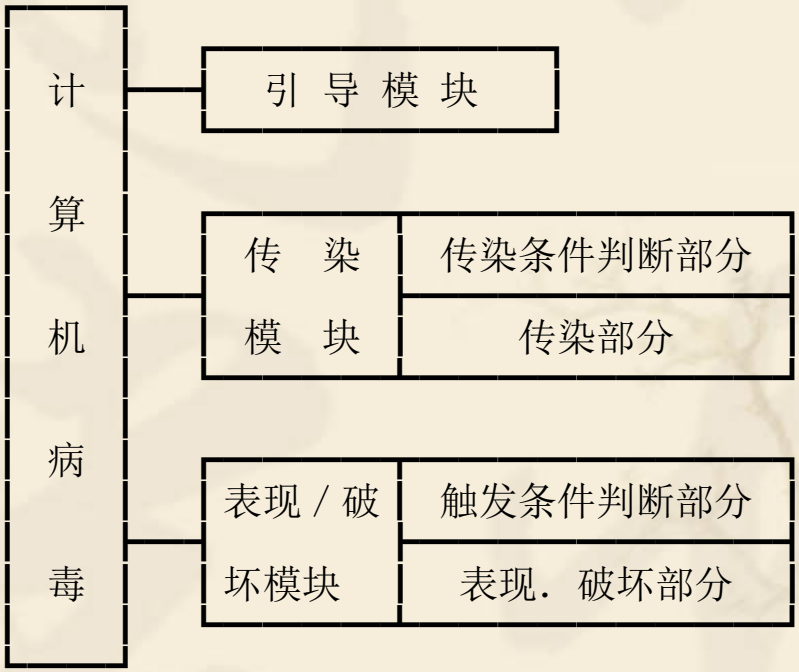
- 9．玩笑病毒
- 玩笑病毒的前缀是：Joke。恶作剧病毒。
- 公有特性是本身具有好看的图标来诱惑用户点击，点击后病毒会做出各种破坏操作来吓唬用户，但实际上没有进行任何破坏。如：女鬼（Joke.Girlghost）病毒。
- 10．捆绑机病毒
- 捆绑机病毒的前缀是：Binder。公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如QQ、IE捆绑起来，表面上看是一个正常文件，当运行捆绑病毒时，会隐藏运行捆绑在一起的病毒，从而造成危害。如：捆绑QQ（Binder.QQPass.QQBin）、系统杀手（Binder.killsys）等。

# 5.5计算机病毒的构成

- 5.5.1计算机病毒的基本模块
- 小球病毒包括下面几部分：
- 标识：记录于被传染的系统BOOT区尾部用于病毒鉴定自身是否存在的代码：1357（十六进制）。
- 引导模块：用于初始化自身入口及需要参数并将自身驻留于内存以便执行，然后读DOS引导程序进行正常启动的部分。

- 传染模块：分为条件判断部分和传染部分。
  前者通过判断系统引导区的偏移量1FCH及1FDH两处的内容是否为57H和13H来确定是否被传染；
  后者则是负责将病毒的全部代码通过被修改的INT13H中断按病毒的约定写入系统。
- 表现模块：分为表现部分的判定和表现部分。
  前者通过INT8H中断判定是否在被传染的系统屏幕上显示跳动的小圆点，即触发病毒的表现部分，
  后者则是在其表现部分的判定条件得到满足的情况下，在被传染的系统上显示一个跳动的小圆点。

- 计算机病毒程序包括三大模块，即引导模块，传染模块和表现/破坏模块，其构成见下图。其中后两个模块各包含了一段触发条件检查代码，分别检查是否满足传染和表现/破坏的触发条件，只有在满足相应条件时，计算机病毒才会进行传染或表现/破坏。



- 计算机病毒有两种状态，即静态病毒和动态病毒。
- 静态病毒是指存储介质上（如软盘、硬盘、磁带等）上的计算机病毒，由于没有处于加载状态，故不能执行病毒的传染或破坏作用。
- 动态病毒是指已进入内存，处于运行状态，或通过某些中断能立即获得运行权的计算机病毒。
- 引导模块的工作方式就是通过非授权加载，使静态病毒激活为动态病毒。

- 在操作系统把含有病毒程序的载体加载到内存时，首先读入的是病毒程序的引导模块，
- 开辟所要用的内存空间或覆盖系统占用的部分内存空间，以便驻留内存，发挥破坏作用。
- 在驻留内存后，为掌握系统控制权，还会改变系统中断向量，使之指向病毒程序的传染和表现/破坏模块。
- 引导模块会对内存的病毒代码采取保护措施，以避免病毒程序被覆盖。
- 在完成病毒程序的安装后，执行正常的系统功能，以隐蔽和保护自己。

- 计算机病毒传染模块的作用就是将病毒传染到其它对象上去。
- 包括两部分内容，传染条件判断部分和传染部分。
- 多数的病毒都带有传染标志，如果某个目标有该病毒的特殊标识，就不再向该目标传染。

原因:如果一个目标多次感染病毒，就会导致该目标明显的变化（文件长度成倍增加，系统不能运行等），而让人们察觉到，这样就无法传染更多的目标和表现/破坏模块的执行。

设置病毒标识为了实现病毒的隐蔽性和潜伏性所采取的措施。

- 监视系统运行
- 发现攻击目标后，判断是否有病毒的传染标识以及其它的特定条件，
- 把病毒全部链接到被传染的攻击目标。
- 计算机病毒的表现/破坏模块的作用就是实施病毒的表现及破坏作用。
- 分为触发条件判断部分和表现/破坏部分
- 在病毒大规模传染之前，不让察觉到。
- 是实现病毒的隐蔽性和潜伏性所采用的方法。

- 驻留内存，掌握系统控制权。
- 通过病毒触发条件判断部分来确定是否要对计算机系统进行破坏或向人们显示自己的存在。
- 触发条件有这样几类：
  一是与系统时钟有关的以时间、日期和星期等作为触发条件；
  另一类是以计数作为触发条件，当满足某个设定值时，即触发病毒；
  此外还有上述两类触发条件的逻辑运算以及其它工作触发条件。

- 计算机病毒三个模块各自运行,在时间上不一定连续
- 执行完病毒的引导模块后，可能就直接退出病毒代码，以后两个模块要到触发了某个机制才执行。
- 不是任何病毒都包括这三个模块。

维也纳病毒就没有引导模块。
不驻留内存，其生命期只有病毒代码运行的瞬间，但在首次运行时，就执行其传染模块或破坏模块
巴基斯坦病毒没有表现/破坏模块。

# 5.5.2计算机病毒的引导机制

- 计算机病毒是一种可执行文件，
- 但不以独立文件的形式存在，而是隐藏在合法文件中，通过非授权加载，使病毒的引导模块被执行，病毒由静态转为动态。
- 计算机病毒是以现有的软硬件资源为环境而存在的。

- 1.计算机病毒的生存载体——磁盘
- 磁盘
- 病毒在磁盘中的存储位置有两种：
- (1) 存储于引导区。

病毒在硬盘中既可存于主引导区，也可存于引导分区中。

在软盘中只存于引导分区中。

储存在引导区的计算机病毒通常采用替代法，病毒程序把自己部分或全部代码替代原正常文件的全部或部分。

- (2) 存储于格式化磁盘的用户空间中。
  存储于用户空间的病毒一般采用链接法，把病毒程序和原正常文件链接在一起。
  病毒也可通过替代法将自己加入到原正常文件中，当然这需要更为复杂的程序技术和对攻击对象的了解。
- 计算机病毒寄生的链接法可分为文件头链接、文件尾链接和文件中链接三种。
- 链接于被攻击文件的头部，称为文件头链接。此时病毒程序寄生于合法程序的开始处，只要执行该程序，首先运行的是病毒，且病毒立即获得对系统的控制权。

- 链接于被攻击文件的头部，称为文件头链接。此时病毒程序寄生于合法程序的最后，但在合法程序的开始处增加了“goto 病毒程序”语句。这样执行该程序，病毒同样先获得对系统的控制权。
- 链接于被攻击文件的中间，称为文件中链接。此时病毒程序寄生于合法程序的中间，但在合法程序的开始处增加了“goto 病毒程序”只要执行该程序，计算机病毒也先获得对系统的控制权。

但这种情况的病毒程序设计较为困难。

- 2.计算机病毒的引导机制
- 计算机病毒的引导模块的作用就是将病毒由外存引入内存，将分散的病毒程序在非法占用的存储空间进行重新装配，构成一个整体病毒程序，使静态病毒激活成为动态病毒。
- 计算机病毒程序由外存引入内存后，其程序就保留在内存中，通过某种触发手段不断检查是否满足传染或表现/破坏条件，以便执行相应功能。

- 病毒程序将自身一段程序代码保留在内存中有两种手段：一种是通过程序驻留；
- 另一种是将病毒代码移到内存的最高段，然后把内存大小指示单元减少几K，以欺骗系统，使之不会再使用最高端的病毒代码所占用的空间。
- 计算机病毒的引导模块在把病毒程序代码引入内存后，还有两个功能：
- 一是对内存的病毒代码采用保护措施，使之不会被覆盖；
- 二是要对内存中的病毒代码设定某种激活方式，使之在适当时候取得执行权。

# 5.5.3计算机病毒的传染机制

- 1.计算机病毒的传染过程
- 计算机病毒的载体有哪些？
- 计算机病毒载体有三个层次：单个计算机系统，单个存储介质，单个文件。
- 从带毒载体进入内存是由计算机病毒的引导机制利用操作系统的加载机制或引导机制
- 从内存侵入无毒介质或文件是利用操作系统的读写磁盘中断或加载机制，
  内存中的病毒在时刻监视着操作系统的每一个操作，满足传染条件则病毒程序将自身代码拷贝到受攻击目标上去，完成病毒的一次攻击过程。

- 系统引导型病毒在感染磁盘前，通常要确定磁盘是否已经被感染。
- 把引导记录装入内存并与自己的内容进行比较，以确定是否传染。
- 在传染时，把原来引导记录的内容存储到磁盘的某个扇区，而把病毒程序存放在原来引导记录位置处。

- 文件型病毒在感染前检查被传染对象是否有病毒标识。
- 传染的手法通常有添加和嵌入。添加就是把病毒程序添加到文件的头部和尾部。
- 用这种方法编制的病毒为了在宿主程序运行时获得对控制权，根据被传染文件类型采用不同的方法。
- .com和.exe文件使用不同的算法通知计算机程序入口点。
- 要使病毒能够有效感染这两种类型的文件，就要把这些程序的差别考虑进去。
- 嵌入法则是将病毒程序代码直接存放在可执行程序的未用代码和数据权段内。
- 采用这种方法编制病毒程序比较困难，其原因是必须保证病毒代码长度小。这是因为通常可执行文件不可能有较长的未用程序空间。
- 长度上的严格限制减少了病毒程序增加的功能,也减少了病毒码的适应能力。

- 2.计算机病毒的传染途径和传染范围
- 计算机病毒传染的途径有两种：
- 一是利用磁性存储介质如磁盘或磁带等传染载体。

  病毒最先是隐藏在磁介质中，当一台计算机使用该介质时，病毒进入系统。
- 另一种是利用网络作传染载体。

  计算机网络是在一定的通信协议及网络操作系统支持下而实现的一种数据共享环境，

  通信与共享为计算机病毒的传染提供了机会。

- 计算机病毒载体扩散区域称为计算机病毒的传染范围。
- 计算机病毒的传染范围可以分为理论上的传染范围和实际上的传染范围。
- 理论上的传染范围是指病毒所能攻击的计算机系统分布区域，

  病毒在其出现后的一定时间内所传染过的计算机系统分布区域称为实际上的传染范围。

  病毒的传染范围是一种地理分布区域，这一分布区域在地理位置上并不一定连续
- 理论传染范围要比实际传染范围大。

- 计算机病毒可能对系统构成攻击的计算机系统地理分布区域称为计算机病毒的潜在传染范围。
- 计算机病毒理论传染范围等于计算机病毒实际传染范围与潜在传染范围之和。
- 如果区域中计算机病毒的载体已经存在，但系统尚未受到攻击，这样的地理分布区域称为实际潜在范围。
- 把实际传染范围与实际潜在传染范围之和称为传染范围。

- 计算机病毒从其出现到广泛实施攻击并传播开来需要一段时间，这段时间称为计算机病毒实施攻击时间。
- 实际传染范围是在一定时间点上来评判感染病毒的计算机系统的分布情况。
- 在实施攻击时间内，病毒从一个系统传染给另一个系统，并使后者也成为一个病毒源，进而再传染给其他未受感染的系统，并使之成为又一个病毒源。

- 3.计算机病毒的交叉感染
- 计算机病毒的交叉感染是指多种计算机病毒存在于同一个系统或文件中，使得一个计算机系统或文件成为两种或两种以上的计算机病毒携带者。
- 交叉感染导致病毒之间的相互影响，争夺寄生位置和传染控制权，
- 病毒作用的复杂化，检测和清除病毒带来困难
- 一个带有两种病毒的传染源，通过某种加载都进入内存后，遇到第一个传染目标时，哪种病毒会先攻击呢？

## 软盘先染上小球病毒，然后再染上大麻病毒

| 软盘 / 病毒入侵 | 0面0道1扇区 | 1面0道3扇区 | 1个空簇 | INT13H |
|---|---|---|---|---|
| 无病毒 | 引导程序 | 数据文件或根目录 | 空 | 正常的中断服务程序 |
| 小球病毒入侵 | 小球病毒内容 | 数据文件或根目录 | 引导程序 | 小球病毒执行入口 |

染上小球病毒后，软盘引导扇区放的是小球病毒的部分代码，正常引导程序则被放到某一空簇上。

再染上大麻病毒后，引导扇区中的小球病毒又被大麻病毒看作为引导记录内容而被移走，占据引导扇区的是大麻病毒。

用该软盘启动系统时，引导扇区中的大麻病毒先进入内存然后有大麻病毒把小球病毒作为引导程序加载运行，使得小球病毒进入内存

最后由小球病毒加载运行真正的引导程序。

- 后染上的病毒先进入内存。
- 在大麻病毒进入内存后，即修改INT 13H中断向量指向自己的传染模块，
- 然后小球病毒再进入，它再次修改INT 13H中断向量，使之指向小球病毒传染模块。
- 当遇到第一个传染目标时，总是判断是否满足小球病毒的传染条件，然后判断是否满足大麻病毒的传染条件。
- 如果两个传染条件都满足，则先传染小球病毒，再传染大麻病毒。
- 如果只满足其中一个病毒的传染条件，只传染该病毒。
- 对于一个已具备病毒传染条件的目标来说，感染病毒的先后次序取决于哪种病毒先进入传染源。
- 这个结论对于一般的文件型病毒交叉感染同样成立。

- 计算机病毒的交叉感染有时还会导致染有病毒的磁盘无法使用。
- 一张系统软盘同时带有“大麻病毒”和“六·四病毒”后，就不能再使用。
- 这两种病毒都是把引导扇区中的引导程序放到1面0道3扇区，
- 这样在感染这两种病毒中的某一个后，引导程序就被病毒程序移到1面0道3扇区中，而引导扇区中放的则是该病毒程序；
- 再感染这两种病毒中的另一个时，病毒程序就把已经占据引导扇区的前一个病毒程序作为引导程序放到1面0道3扇区中，从而把真正的引导程序覆盖掉，
- 该软盘无法使用。

- 4.计算机病毒的被动传染
- 被动传染是指把一个带毒文件拷贝到另一盘上去或对带毒盘作整盘拷贝，都会使另一个盘染上病毒。
- 这时病毒的传染机制并没起作用，故称为被动传染。

# 5.5.4计算机病毒的表现和破坏机制

- 1.计算机病毒的破坏性
- 对于每个计算机病毒的破坏性，可以从下面三个方面来分析：
- 从病毒程序的剖析，了解病毒设计者的目的和企图
- 从病毒传染和实际运行中的作用，了解对计算机系统所造成的危害。
- 计算机病毒交叉感染与环境因素影响所造成的破坏性。
- 计算机病毒对计算机系统的实际破坏能力，特别是计算机病毒交叉感染引起的系统并发破坏机制和后遗症，以及对系统所产生的综合效应，还有待进一步的研究和探讨。
- 计算机病毒的破坏性不一定是由表现/破坏模块造成的，在计算机病毒传染过程中也可能造成破坏。

- 2.计算机病毒的表现破坏模块
- 表现及破坏模块包括触发条件部分和执行表现破坏功能部分
- 计算机病毒的触发是计算机病毒活动的首要条件。
- 触发是指在一定条件下对于表现破坏功能的调用过程。
- 计算机病毒的触发条件通常可分为时钟触发、功能触发和时钟与功能联合触发三类。

- 时钟触发也称时间触发，它是以特定的时间为条件，当特定时间条件满足后就激活病毒表现破坏功能。
  时钟触发可分为纯时间触发和以时间为基数条件的触发两种。
  纯时间触发是指计算机病毒以时间(如年、月、日、时、分、秒等)为直接的触发条件
  以时间为基数条件的触发是以特定的时间T为触发条件的基数，该基数和一定的因数(或条件)F进行算术(+,-,*, /)或逻辑()运算，若满足特定条件就触发。
- 功能触发包括系统的软硬件的特定功能以及计算机的一些指令命令，如复制命令和汇编指令等。
  功能触发的条件组合情况与时间触发类似。
- 第三种触发情况是以时钟触发和功能触发的逻辑运算的结果作为触发判断条件的。

- 计算机病毒的破坏表现部分是根据计算机系统所提供的指令和功能对计算机系统进行破坏的一段指令代码，它可分为可恢复性破坏和不可恢复性破坏两类。
- 如果计算机病毒破坏的数据能够通过已有的数据恢复软件得到恢复，则称为可恢复性破坏。
- 病毒的不可恢复性破坏则是用现有数据恢复软件不能恢复被破坏的磁盘扇区和文件。

# 5.6计算机病毒的检测与防范

- 计算机反病毒技术包括三个部分：
- 计算机病毒的检测技术
- 计算机病毒的清除技术
- 计算机病毒的预防技术

# 5.6.1计算机病毒的检测

- 病毒检测是消除病毒的先行工作，它包括人工检测和自动检测两种。人工检测是指计算机用户利用计算机提供的实用程序的有关功能进行病毒检测，而自动检测则是指利用诊断软件来判断一个系统或磁盘是否含有病毒的一种方法。

- 任何一种病毒都是利用操作系统环境及体系结构特点来实现的，
- 一个程序是否为病毒其依据就是该程序是否具有传染性，
- 一个直观想法是编制一个能检验其他程序传染性的程序。
- 但是，由于病毒程序的传染部分有很多种编制方法，很难找出某种规律去判别。
- 而且这是一个不可精确判定问题。

- 计算机病毒一般是通过替代法和链接法存储于载体程序的，这样就会引起载体程序代码的某些特征变化，如文件长度、程序代码和、程序代码积等发生变化，而对于系统和应用程序来讲，其代码是不变的，

- 1.比较法
- 引导型病毒通常是用替代法传染的，即病毒程序用自己的部分或全部代码来取代正常引导记录，并将正常引导记录移至可用空间中的一个特定簇中。
- 病毒替代正常引导记录内容，使引导区中的内容发生了变化，
- 通过对引导区的检测来评定是否有病毒存在
- 用原始备份与被检测的引导扇区或被检测的文件进行比较。
- 用常规DOS的DISKCOMP和PCTOOLS等工具软件就可以进行，

- 对硬盘主引导扇区或DOS引导扇区做检查，通过比较法发现其中的程序代码是否有变化
- 硬盘的主引导扇区、分区表以及文件分配表、文件目录区是病毒攻击的主要目标。
- 硬盘存放主引导记录的主引导扇区一般位于0面0道1扇区。
- 病毒侵犯引导扇区的重点是前面的十几个字节。

- 检查FAT表：病毒一般要对存放的位置作出“坏簇”信息标志并反映在FAT表，看是否有坏簇，进而确定是否感染了病毒。
- 多数文件型病毒通常会使染毒文件的长度发生变化，而且通常采用链接的方法把病毒程序与正常程序链接，因此都有跳转指令，检查比较文件长度变化和文件头与尾检查跳转指令。

- 对于引导型和文件型病毒，为了延长活动时间，以得到更多的传染机会，通常把自己驻留在内存里，以得到更多的传染机会。
- 驻留的目的是传染，方法是修改中断向量，使系统中断转向病毒的控制部分，而由控制部分在适当时候转到原中断处理程序处执行。
- 检查中断向量是检测病毒的重要手段。
- 病毒最常攻击的中断有磁盘输入、输出中断(13H)、绝对读/写中断(25H,26H)、时钟中断(08H)等。

- 病毒在传染或执行时，必然占有一定的内存空间，并驻留在内存空间中，而其所占据的内存空间,用户一般是不能覆盖的。
- 由于重要数据总是放在固定区域内(0:4000H-0:4FF0H)，通过检查内存大小和内存中的数据，来判断是否有病毒。
- 比较法简单、方便，不需专用软件。
- 缺陷是无法确认计算机病毒的种类名称

- 2. 加总对比法
- 根据程序的名称、大小、时间、日期和内容，加总为一个检查码，把它附在程序后面，或将所有检查码放在同一个数据库中，通过检查此信息来确定程序是否被更改，由此判断是否感染病毒.
- 能够发现已知病毒和未知病毒。
- 但较难确定是何种病毒
- 病毒一旦具有更改这些检查码功能，就无效。
- 这种方法不能检测新的文件，如从网络(E-mail/FTP/BBS/Web)传来的文件、拷入的文件压缩文档中的文件等，误判率高，

- 3.搜索法
- 用病毒特征值对检测对象进行扫描。
- 病毒特征值是指计算机病毒本身特定的寄生环境中确认自身是否存在特殊的标记符号。
- 病毒的标识可以作为病毒的特征值，但病毒的特征值并不一定就是病毒的标识。
- 例如，1575病毒的特征值可以是传染标识0A0CH，也可以是从病毒代码中抽出的一组16进制的代码：06 12 8C C0 02 1F 0E 07 A3等
- 对检测对象进行扫描，确定是否有特定字符串(特征值)，。
- 人工检测可以这样
- 目前计算机病毒检测软件也采用此方法。关键是病毒代码库的建立。

- 传统的特征值搜索技术实现步骤是：
- 1)采集病毒样本，必须注意的是，同一种病毒，当它感染一种宿主时，就要采集一种样本，若感染.com文件，和.EXE文件，则要采集2个样本，若还感染引导区，则要采集3个样本。
- Why?传染和寄生方式有区别。

- 2)在病毒样本中，抽取特征值，
- 必须注意：不能随意从病毒程序中选取一段作为病毒特征，
- 病毒数据区也不要包含在病毒特征中。
- 获取病毒特征值的方法是
- (1)抽取表现形式
- (2)抽取感染标识
- (3)从病毒代码的任何地方开始取出连续的不大于64且不含空格的字节串作为病毒的特征值。
- 根据病毒特征值的搜索法缺点是扫描时间长，速度慢，随着病毒种类的增多，检索时间变长。如果检索5000种病毒，必须对这些病毒特征代码逐一检索。

- 广谱特征过滤技术
- 为了提高检测效率，把病毒分成一些大类，通过检测，确定是否有病毒，属于哪个大类，然后再确定是哪种病毒。
- 统计一系列病毒的特征，明确完全相同的代码，如果一定位置上的代码是不同的，则用“??”来替代，每个双问号代表一个字节。
- 如果在各样本的病毒特征串中，从第一组(一个字节及以上)相同的特征串之间的代码，不仅常变换，而且在每个样本中，间距也不相同，若是在32个字节内变化，用“%%”来过滤这些变化的代码。
- 如下面的2个例子即为广谱特征串：
- 1)B8 ?? 42 ?? ?? ?? ?? %% B4 40 %% %% %% %% B8 ?? 57
- 2)13 04 %% B1 06 %% D3

- 13 04 %% B1 06 %% D3
- 代表了小球病毒，巴基斯坦病毒，Stone(A-H,即8种), 5种bloody病毒，4种香港病毒，米氏病毒，磁盘杀手病毒，Pretty Girl病毒，CMOS Destroyer, Ctrl+Break 病毒,新世纪病毒，扬基病毒，Trill病毒，Invader病毒，Plastique病毒，Libery病毒，广大1号，Flip-PT，Mask-1，Mask-2，31 #，2709/ROSE, BUPT, 3072, ALFA/3072-2, Ghost/One-half, 3584－2，Denzuko，DBF/BOOTEXE，Hard Disk kill，共44种病毒

- 新病毒出现后，老版本无法检测。
- 不能对付隐蔽性病毒。因为这类病毒在进入内存后会先于检测工具将被查文件中的病毒代码剥去。

- 4.行为监测技术
- 检测病毒的另一种方式是从病毒行为角度考虑
- 截留盗用INT13H,
- 修改INT13H,21H,24H,25H,26H
- 修改内存总量
- 修改最后一个内存控制块的段址
- 对可执行文件进行写操作
- 写磁盘引导区
- 修改代码入口点。
- 正常程序也可能会具有上述情况，但只有病毒才可能同时具有数种情况。
- 能够发现已知病毒和未知病毒。
- 但较难确定是何种病毒
- 会误报。

- 5. 分析法
- 开发检测和杀灭计算机病毒的软件都是建立在对各种病毒的细致分析基础上。基本步骤是：
- 利用相关工具判断引导扇区和程序中是否有病毒；
- 确认病毒类型和种类，判定是否为新病毒；
- 对新病毒要搞清其大致结构，从提取特征串添加到病毒代码库中；
- 详细分析病毒代码，设计出防杀病毒的方法。

- 分析有静态和动态两种。
- 静态就是用反汇编工具将病毒代码打印成反汇编指令的程序清单进行分析，了解病毒的分成几个模块，怎样进行系统调用，所采用的主要技巧，研究哪些代码串体现了该病毒的特征。
- 动态分析则 是利用DEBUG等调试工具在内存带毒情况下，进行动态跟踪，观察病毒具体过程，在静态分析基础上进一步了解病毒工作原理。

- 设计自动检测软件的基本思想：
- (1)建立正常程序和BOOT区内容的档案

  对一个特定版本的操作系统而言，BOOT区的内容及正常的可执行文件长度是固定的，故可在检测程序中建立正常的特征库，并通过文件的读取比较文件是否发生变化，通过对BOOT区的读取查看BOOT区的变化，以确定系统是否异常
- (2)建立病毒特征值库

  通过分析现有病毒的特征建立病毒特征值库，检测时通过比较来判断病毒的种类。
- (3)建立内存中断向量库，

  在运行中通过对系统中断向量的检测，发现是否有对中断向量作修改的程序存在。
- (4)建立内存容量库，

  通过对不同容量内容的测试，以确定内存容量中内容是否与正常内容相同。

- 目前计算机病毒检测软件就是依据这一思想，采用判定技术，依据病毒的特征码检测病毒。
- 采用静态和动态相结合的综合判定技术搜索特定字符串。
- 特别注意特定病毒特征码提取的合理性，因为这是检测病毒的关键，将直接影响检测的漏报和误报，尤其是对变型病毒的检测要避免漏报。

- 6.新一代病毒检测技术
- (1)启发式代码扫描技术
- 病毒和正常程序的区别可以体现在许多方面，如：应用程序通常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，而病毒程序通常最初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系列。
- 根据显著的不同，去判断确定

- 一个运用启发式代码扫描技术的检测软件，实际上就是以特定的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真正目的。
- 具体实现时，该技术还是比较复杂的。
- 识别并检测一系列可疑的程序代码指令序列，包括格式化磁盘类操作、搜索和定位可执行程序的操作、驻留内存的操作、非常的或未公开的系统功能调用操作等，但这些操作有时也是合法和必需的
- 根据安全和可疑等级排序，特别根据常规给予不同的加权值。

- 例：格式化磁盘的功能操作几乎从不出现在正常的应用程序中，而病毒程序中出现的几率极高，则可对这类操作的指令系列给予较高的加权值。
- 而驻留内存的操作许多应用程序也要使用，因此应给这类操作较低的加权值。
- 每个程序的各状况的操作的加权值之和即为一个判断依据。通常会规定一个阀值，若超过此阀值，则检测程序就可以报警。

- (2)主动内核技术
- 现代各种实时反病毒软件，能够在用户不知道病毒入侵的情况下发出报警并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，作为上层应用软件借助于操作系统或网络系统所提供的功能被动防治病毒。
- 主动内核技术就是将已经开发的各种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，成为操作系统本身的补丁。但实现难度较大。

- (3)智能检测方法
- 从某些病毒的共性出发，加以判断，在一定程度上查出未知病毒。
- 除智能检测外，病毒的检测和清除程序都是针对已知病毒的，通过对已知具体计算机病毒程序的分析，设计出检测病毒程序的。其优点是针对性强，缺点是时间上滞后，要待人们发现病毒后作进一步的分析，才能“对症下药”，检测出病毒。
- 由于新病毒不断出现，因而检测病毒系统需要不断更新。

# 5.6.2计算机病毒的清除

- 计算机病毒的清除同样有两种方法：
- 人工处理和自动处理。
- 人工处理就是利用现有的调试程序和实用工具软件对染有病毒的系统进行处理
- 对系统引导型病毒用实用工具将正常引导记录写回，若有坏扇区则把它恢复。
- 对文件型病毒则是恢复正常文件，消除链接的病毒。
- 对于宏病毒，则可以通过清除或修改宏来解决

- 计算机病毒清除程序是对特定种类病毒进行处理的可执行程序，它是在分析研究了具体病毒之后编制出来的，因此具有一定的局限性，不可能清除所有的病毒。
- 计算机病毒的清除技术一般采用还原技术，根据病毒的传染方式设计出消病毒程序。
- 对破坏性传染的病毒（即采用部分覆盖方式传染的病毒），只能用未被破坏的正常程序去覆盖以达到清除病毒的目的

- 对于宏病毒的清除，是清除指向宏的链接及宏内容本身。又由于宏结构的性质，可以清除所有宏。
- 病毒的清除程序一般是针对已知病毒的，通过对已知具体计算机病毒程序的分析，设计出消除病毒的程序。
- 其优点是针对性强，缺点是时间上滞后，要待人们发现病毒后作进一步的分析，才能“对症下药”，检测并消除病毒。
- 新病毒不断出现，查杀病毒系统需要不断更新。

- 杀毒软件必须先清除内存病毒，然后进行病毒的检测
- 系统引导性和文件型病毒的隐藏技术
- 系统引导性病毒改变基本输入输出系统(BIOS)13H中断的入口地址使其指向病毒代码，当发现有调用INT 13H读被感染扇区的请求时，用正常13H中断代码进行操作返回给调用程序，因此较难察觉病毒的存在。
- 即使采用直接对磁盘控制器进行操作的方法读写磁盘扇区也可能无效。
- Why?
- 某些病毒具有在加载程序时制造假象的能力：
- 当启动任何程序时，修改DOS执行程序的中断功能，首先把被病毒感染的扇区恢复原状，这样即使杀毒软件采用直接磁盘访问也只能看到正常的磁盘扇区。当程序执行完成后再重新感染。

- 文件型病毒的隐藏技术类似于系统引导性病毒。
- 改变DOS或基本输入输出系统(BIOS)的文件系统相关调用，在打开文件时将文件的内容恢复成未被感染的状态，在关闭文件时重新感染文件。
- 对付这类隐藏功能病毒的有效方法是在进行病毒检测前先清除内存中的病毒。

# 5.6.3计算机病毒的预防

- 预防的方式有管理手段预防和技术手段预防两种。
- 管理手段预防就是加强对计算机系统使用的管理，制定一些管理措施来防止计算机病毒的侵入，而通过免疫软件和预警软件等技术措施来预防计算机病毒对系统的入侵则是技术手段预防。

- 计算机病毒的传染是通过一定途径来实现的。
- 制定一些针对传染途径的管理制度，来抑制病毒的传染。
- 通常可制定如下措施：
- (1)谨慎使用公用软件和共享软件
- (2)对新来的计算机系统先检查才使用，尽量避免计算机系统的互相借用。
- (3)不执行不知来源的程序
- (4)限制计算机网络上的可执行代码的代换
- (5)对重要文件和数据进行写保护，系统中的数据或重要程序要定期拷贝。

- 管理措施对病毒的预防是通过牺牲系统数据共享的灵活性而换得系统的安全性
- 在管理措施的制定上必须考虑到计算机系统使用的方便性和实用性，采取折衷的办法，与技术预防手段相结合，以有效预防病毒入侵。

- 计算机病毒预防的技术手段一般采用病毒免疫技术、校验码技术和行为规则判定技术等方法。
- 病毒免疫技术是对执行程序附加一段程序，这段程序负责程序的完整性检验，发现问题时自动恢复原程序。
- 校验码技术是对程序进行完整性检验。对系统内的有关程序代码依照一定的算法计算出其特征参数并加以保存。在装入执行程序代码时进行校验，依照同一算法扫描程序代码，算出特征参数，与原特征参数加以比较，如果一致则准予执行，否则拒绝执行并予以报警。

- 计算机病毒的预防主要是采用病毒行为规则判定技术。
- 采用人工智能的方法，归纳出病毒的行为特征，在计算机系统中设立警戒网，预防已知、未知病毒的入侵和传染。
- 该技术的关键是对病毒行为特征的归纳是否有效、可行，否则容易产生误报和漏报。
- 随着计算机病毒的发展，计算机病毒的行为规则需要不断完善。

- 计算机反病毒系统的一个趋势是向集成化方向发展，即同时具有计算机病毒的检测、清除和预防三大功能。
- 计算机病毒防火墙借用了信息网络环境中“防火墙”概念，它采用一种实时双向过滤技术，对系统的所有操作实时监控，能够将来自外部环境的病毒代码实时过滤掉,并且能阻止病毒在本地系统扩散或向外部环境传播。从而在本地系统和外部环境之间筑起一道壁垒。

- 关键在于“实时双向过滤”。所谓病毒防火墙的“实时双向过滤”含义是：
- (1)病毒防火墙能够对计算机病毒起到“双向过滤”作用。
- 体现在两个环节上：
  - 第一环节，保护计算机系统不受来自于任何方面病毒的危害，
    本地资源，远程资源。
  - 第二环节，病毒防火墙对系统提供的保护应该是着眼于整个系统而且是双向的
    应该能够对本地系统内的病毒进行过滤，防止向网络或软盘等外部存储介质扩散。

- (2)病毒防火墙对病毒过滤的实时性。
- (3) 病毒防火墙本身应该是一个安全的系统。
- 安全有两方面的含义：
- 其一，病毒防火墙本身是安全的，它能够抵抗病毒对其进行的任何形式的攻击；
- 其二，病毒防火墙对计算机系统来说也是安全的，在过滤病毒的过程中，不应该对无害的数据进行任何形式的损伤。

# 5.7计算机病毒编制的关键技术

- 5.7.1 DOS病毒
- 1.DOS下PC机的启动流程
- 任何PC机，在运行程序执行命令之前，都要进行简单的硬件自测
- 打开电源，电源设备进行检测后向CPU发出启动信号，CPU进行初始化然后执行存储在只读存储器上的基本输入输出系统的硬件自测程序
- 只读存储器在主板的集成电路芯片上。

- 检测显存，寻找其他的ROM芯片进行初始化，检查系统内存中的临时存储单元，确定是冷启动还是热启动。如果是冷启动，则对RAM内存进行检测，运行RAM自测程序。
- 寻找ROM中设置的第1个驱动器
- 读取第1个物理硬盘的0面0道1扇区进入内存。该扇区包含了主引导记录MBR和分区表。由此确定哪个分区哪个扇区包含操作系统的启动代码，最后把操作系统的引导扇区读入内存并且开始执行。

- 接下去要找的文件是IO.SYS,再由IO.SYS寻找MSDOS.SYS并装入内存，然后MSDOS.SYS被执行，Config.sys执行，Command.com执行，Autoexec.bat执行。
- Autoexec.bat，对于要在每次启动时运行的程序都可以写进Autoexec.bat
- 一个程序中的一条命令或是一个动作可以直接使用BIOS调用访问硬件，也可以通过操作系统调用或使用驱动程序来访问硬件。
- 病毒可以使用这3种选择的任意组合来达到目的。

- 病毒通常通过修改中断代码或者通过将中断向量表指向内存中的其他位置来获得对系统的控制。
- 各中断程序的关系
- 病毒程序要做的事情可以归结为：
- 寻找宿主文件，打开该文件并把自己写到此文件中，然后关闭该文件。

- 2.DOS环境下病毒程序编写的关键
- 系统引导型病毒在开机后即获得控制权，为保护自己在内存中，进行传播，引导机制模块必须编写下列程序：
- (1)修改内存的程序，以便减少可用最大内存容量。
- (2)修改中断向量的程序。
- (3)将病毒移到内存高端的程序
- (4)根据标记从相应扇区读入病毒其他部分的程序；
- (5)读入原引导扇区内容并完成系统引导的程序。

- 5.6.2.Windows病毒
- 1.Windows启动
- 所有Windows平台都要经历极为复杂的启动过程。
- 先经历一个文本过程或非图形化过程。测试底层硬件，基本的系统文件载入内存，为内核加载做准备。
- 然后主要文件载入内存，设备启动程序载入内存，检查注册表获得启动的进一步信息
- 运行设定好的应用程序、过程 和服务
- 注册表的设置是为了方便管理，但为病毒提供了方便

- 2.Windows环境下病毒程序编写的关键技术
- Windows环境下系统功能调用不是通过中断来实现的，而是由DLL中导出，直接得到API入口比较困难。
- 利用同一windows版本下同一个核心函数入口固定这一特点，编写获得函数入口的程序；
- 或者编写截留I/O操作的程序。
- 其他则是与DOS类似。

- 3. 病毒程序编写实例
- DOS批处理病毒源程序
- ECHO OFF
- IF EXIST c:\autoexec.bat  GOTO Virus
- GOTO No_Virus
- :Virus
- C:
- Ren  autoexec.bat auto.bat
- COPY a:\autoexec.bat c:\
- ECHO Hello World!
- :No_Virus
- a:
- ECHO ON
- /AUTO
- PAUSE

# 第6章 典型计算机病毒分析

- 目前计算机病毒的种类日趋增加，为了有效地防范计算机病毒，分析典型计算机病毒是必要的。
- 从现象中认识事物的本质，掌握其规律
- 从而找出防范计算机病毒的方法和措施
- 进而发展计算机系统安全的技术和理论

# 6.1大麻病毒

- 大麻病毒又名石头病毒，是一种系统引导型病毒，它攻击软盘的引导区或硬盘的主引导区，是恶性的计算机病毒。
- 6.1.1大麻病毒的表现症状
- “Your PC is Now Stoned”。
- 蜂鸣器会发出一响声。
- 当提示字符闪过之后，机器并无其他异常现象，但对某些硬盘和软盘可能无法再使用。

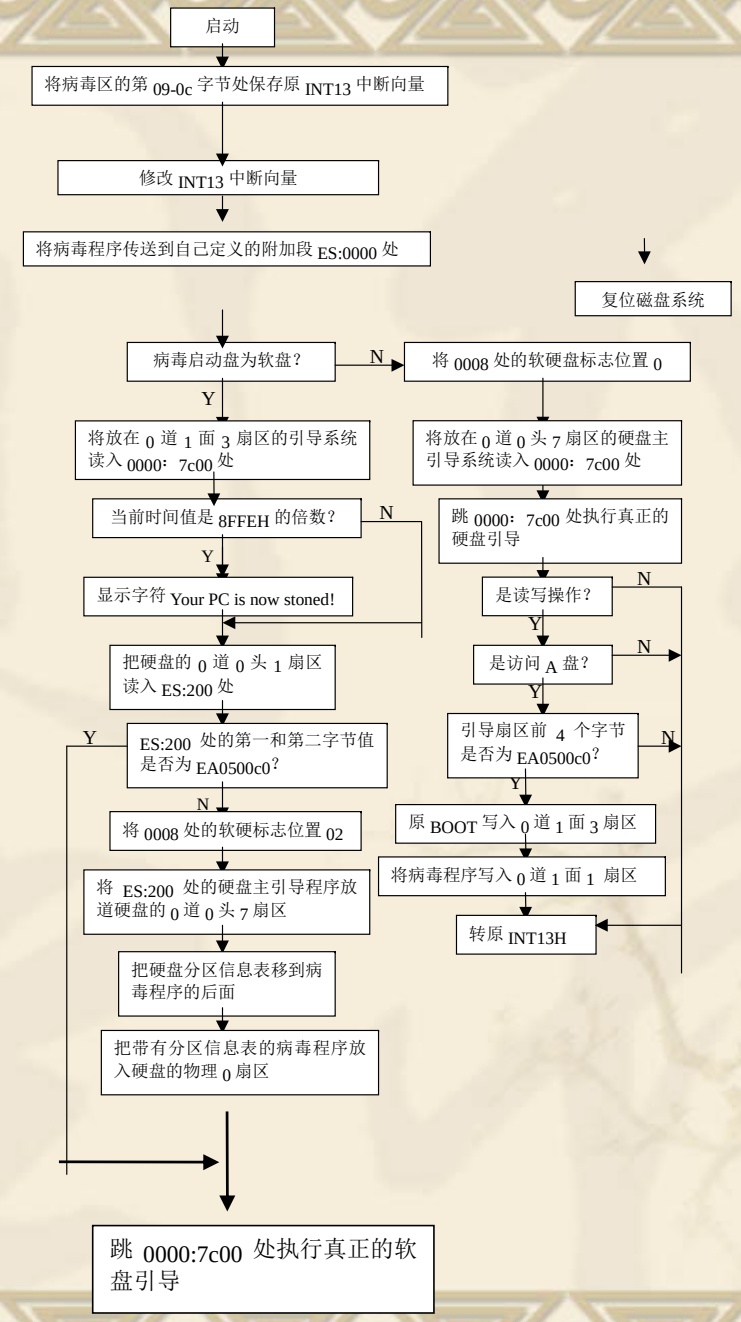
- 大麻病毒的传染途径主要是：
- 或是在有病毒的机器上对软盘作了读写操作，
- 或是用带毒软盘启动系统，
- 或是把带毒系统盘整盘拷贝。

## 6.1.2大麻病毒的工作原理

- 大麻病毒包括引导模块、传染模块和表现模块
- 用带毒盘引导系统时，引导模块首先运行，
  如果是软盘启动，则有八分之一的可能调用表现模块，表现模块只在这一时刻才可能执行。
- 传染模块分两部分，
  第一部分用来传染硬盘，在引导模块执行时被调用，
  第二部分用来传染A驱动器中的软盘，
  它是通过调用磁盘操作中断INT13H获得执行权的

- 大麻病毒程序的有效长度不到一个扇区，全部藏身于硬盘的主引导扇区和软盘的引导扇区中。
- 当系统启动时，大麻病毒首先进入内存并将原属于磁盘操作系统的控制权交给大麻病毒的主程序，
- 该程序获得控制权后，即作下列工作：

- (1)将病毒程序存放到内存的某一位置保护起来，随时准备攻击用户的磁盘。
- (2)保存原来的INT13H中断向量，并修改正常的INT13H中断服务程序的向量，使之指向病毒的INT13H中断服务程序。
- (3)判断是否从带毒A盘启动。若是的，则立即调用传染模块的第一部分，然后调用表现模块。
- (4)无论是从硬盘还是软盘启动，最终都要跳到0000:7c00处，执行正常的引导程序。


启动
将病毒区的第 09-0c 字节处保存原 INT13 中断向量
修改 INT13 中断向量
将病毒程序传送到自己定义的附加段 ES:0000 处
复位磁盘系统
病毒启动盘为软盘？
N
将 0008 处的软硬盘标志位置 0
Y
将放在 0 道 1 面 3 扇区的引导系统读入 0000：7c00 处
将放在 0 道 0 头 7 扇区的硬盘主引导系统读入 0000：7c00 处
当前时间值是 8FFEH 的倍数？
N
跳 0000：7c00 处执行真正的硬盘引导
Y
显示字符 Your PC is now stoned!
是读写操作？
N
Y
把硬盘的 0 道 0 头 1 扇区读入 ES:200 处
是访问 A 盘？
N
Y
Y
ES:200 处的第一和第二字节值是否为 EA0500c0？
引导扇区前 4 个字节是否为 EA0500c0？
N
Y
N
将 0008 处的软硬标志位置 02
原 BOOT 写入 0 道 1 面 3 扇区
将 ES:200 处的硬盘主引导程序放道硬盘的 0 道 0 头 7 扇区
将病毒程序写入 0 道 1 面 1 扇区
转原 INT13H
把硬盘分区信息表移到病毒程序的后面
把带有分区信息表的病毒程序放入硬盘的物理 0 扇区
跳 0000:7c00 处执行真正的软盘引导

- 大麻病毒对硬盘主引导扇区及软盘引导扇区内容移动的位置是固定的。
- 感染硬盘时，主引导记录被移到0道0面7扇区。
- 此时，若DOS分区的隐含扇区数为11H或17H，则0面0道7扇区空出不使用，病毒不会给系统造成破坏；
- 如果隐含扇区数为1，则0面0道7扇区为FAT表，这样当DOS把这里的主引导记录当做FAT表进行修改分配，则主引导记录失效，导致硬盘无法引导系统。

- 对软盘感染时，大麻病毒不区分软盘种类，把原BOOT区内容写入0道1面3扇区，这样对某些软盘可能造成破坏。

| 扇区分配 / 软盘 | BOOT | FAT1 | FAT2 | 根目录区 | 数据区 | 每道扇区数 |
|---|---|---|---|---|---|---|
| 360KB | 0 | 1-2 | 3-4 | 5-11 | 12- | 9 |
| 1.2MB | 0 | 1-7 | 8-14 | 15-28 | 29- | 15 |

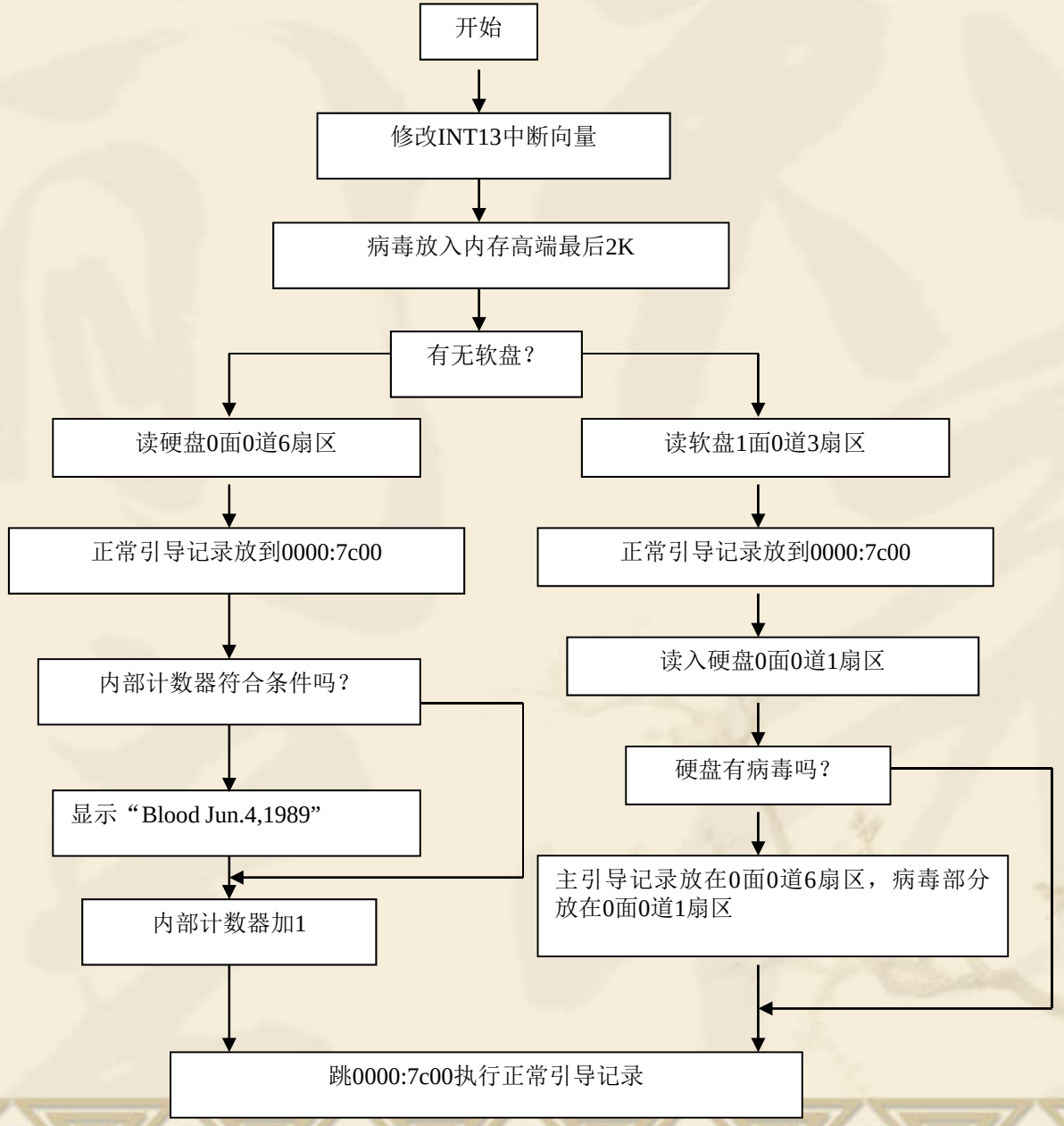
- 6.1.3大麻病毒的防治
- 1.对软盘的检测和消除
- 读出软盘的引导扇区内容与正常引导记录和病毒程序进行比较，就可确定该软盘是否感染了大麻病毒。
- 如果确定软盘已感染了大麻病毒，则只需把1面0道3扇区的原DOS引导记录写回到引导扇区即可。

## 2.对硬盘的检测和消除

- 硬盘的0面0道1扇区为主引导扇区，借助于汇编程序，把主引导扇区内容读到内存指定位置，确定是否感染大麻病毒。
- 在确定硬盘上存在大麻病毒之后，编写汇编程序，把放在0面0道7扇区的硬盘主引导记录写回到主引导区。
- 如果硬盘已不能引导，则说明主引导记录已被破坏。
- 恢复主引导记录。通常可先从同样机型、同样DOS版本做的分区且分区大小一样、不带毒的机器，用汇编程序读出主引导记录，再把它写入一个文件。然后用软盘启动出现故障的机器，并把前面得到的文件装入内存，最后把内存中存放的正常主引导记录写回到主引导扇区，重新启动系统。

# 6.2 六·四病毒

- 当满足一定条件时，在硬盘启动过程中会显示“Bloody!Jun.4,1989”。
- 与大麻病毒相同的是在软盘和硬盘的存储方式也是不一样的。
- 在软盘上也是存放在1面0道3扇区，
- 但在硬盘上是占据0道0面6扇区，此外该病毒还可传染B驱动器中的软盘。


开始
修改INT13中断向量
病毒放入内存高端最后2K
有无软盘？
读硬盘0面0道6扇区
读软盘1面0道3扇区
正常引导记录放到0000:7c00
正常引导记录放到0000:7c00
内部计数器符合条件吗？
读入硬盘0面0道1扇区
显示“Blood Jun.4,1989”
硬盘有病毒吗？
内部计数器加1
主引导记录放在0面0道6扇区，病毒部分放在0面0道1扇区
跳0000:7c00执行正常引导记录

# 6.3 米开郎基罗病毒

- 米开郎基罗病毒又称“米氏”病毒，这个名称来源于它的发作日期：每年的3月6日，而这一天恰是意大利画家米开郎基罗的生日。
- 3.3.1“米氏”病毒的特点
- 病毒程序占据一个扇区，共512字节。对于硬盘占据主引导扇区，而对于软盘则占据引导扇区。

- 当用带有病毒的磁盘启动系统时，病毒程序首先进入内存，减少内存总量2KB，并修改系统的INT 13H中断向量，使其指向病毒的传染模块，从而获得对系统的控制权。
- “米氏”病毒对硬盘和360KB软盘的传染与大麻病毒类似。与大麻病毒不同的有以下3点
- 1.对1.2MB软盘传染时，是将正常引导扇区内容放到根目录最后一个扇区，即1面0道0EH扇区。
- 2.用破坏程序段代替大麻病毒的表现程序段。
- 3.病毒程序标识不同。

- 6.3.2病毒的作用机制
- “米氏”病毒的引导过程与大麻病毒完全相同
- 由于它占据了软盘的引导扇区或硬盘的主引导扇区，故系统启动时，病毒程序首先被装入内存，并获得对系统的控制权，
- 病毒程序在驻留内存后，修改系统的INT13H中断向量，使之指向病毒的传染部分。
- 然后系统判断系统日期，若发现为3月6日，则执行破坏程序，破坏系统的硬盘和工作软盘。

- “米氏”病毒对硬盘的传染和对软盘的传染是不同的
- 首先判断是否有该病毒的标识，以决定是否传染。
- 当用带毒软盘引导系统时，若硬盘无病毒标识，就先将硬盘主引导扇区中的数据移到硬盘的另一扇区，再向硬盘主引导扇区写入病毒程序。
- 对软盘传染时，只传染A驱动器中所操作的软盘，因此除了判断病毒标识外，还要判断驱动器号。
- 如果对A驱动器中的盘进行任何读写操作时，病毒程序的传染部分首先获得控制权，在确定该软盘没有该病毒标识后，就将病毒程序传染到该磁盘上。
- 为麻痹用户，病毒程序会将包含DOS两个隐含模块名称的引导扇区中后21H字节内容移到病毒程序尾部
- 由于用户查看引导扇区时，常要查看这一内容，对用户有一定的欺骗性。

- 病毒程序的破坏模块的作用是判断是否为3月6日，若满足，则不管启动盘是否为系统盘，只要启动盘中染有“米氏”病毒，病毒程序就会将内存中的一块随机数据写入启动盘中从第一物理区开始的整个磁盘，从而导致磁盘中数据全部丢失。

- 其基本原理是：

1.对软盘的INT13H中断调用写入功能，预置每次写入9个扇区
2.根据[0008]单元内容判断是360KB还是1.2MB。若是360KB则转向5；否则每次写14个扇区，转向4。
3.对硬盘设置写入操作，置[0007]单元为4，每次写入17个扇区
4.从内存中5000段地址起开始写。
5.执行INT13H中断，成功时转向6，若不成功则使磁头复位。
6.使写操作磁头号加1。
7.若磁头号低于[0007]单元指示值，则转向1。

- 以上操作实际上是对硬盘执行了4次写操作，每次17个扇区，共68个扇区。

对360KB软盘是执行了2次写操作，每次9个扇区，共18个扇区
对1.2MB软盘执行了2次写操作，但每次14个扇区，共28个扇区

- 这些写操作的结果是完全破坏了操作盘中的BOOT区FAT表和目录区，使操作盘中数据全部丢失。

- 6.3.3诊治
- 对该病毒的检测和清除也类似大麻病毒，当然使用消毒软件则是最方便的方法，一种比较被动的方法就是为了避免损失，通过修改系统日期来避免病毒破坏部分的触发统计。

# 6.4 香港病毒

- 病毒发作时，封锁打印机。
- 该病毒对软盘传染时，将引导扇区内容放到磁盘1面27道08扇区，又称2708病毒
- 3.4.1病毒程序特点
- 传播方式与大麻病毒类似，传染力更强
- 病毒程序短，320多字节，驻留在硬盘主引导扇区，软盘的引导扇区
- 在系统引导时进入系统，它将系统内存总量减少1KB，并驻留在内存高端，其传染过程极为迅速、隐蔽，一般较难觉察。

- 病毒程序在向软、硬盘上传染时，将原来正常引导扇区首部第3个字节起8个字节和尾部90H字节内容先传递到病毒程序段的对应位置，然后再和病毒程序一起写回到操作盘的(主)引导扇区中。
- 对于软盘，前8字节内容为DOS版本号，后90H字节内容为系统启动时的错误提示信息；
- 对于硬盘，后90H字节则为硬盘的分区信息。其目的是迷惑用户，使得在查看引导扇区内容时误认为染毒的引导扇区是原正常的引导程序。

- 该病毒在向硬盘传染时，覆盖了原主引导扇区内容，
- 注意，与前面的几个病毒是不同的。
- 为了使硬盘仍能正常引导系统，在病毒程序中，专门有一段子程序：判定是硬盘引导系统后，直接调硬盘上活动分区的引导扇区内容，完成系统的引导。
- 这使病毒程序既短小，又能蒙骗人们。当用户分析病毒程序时，在查找搬移的原主引导扇区内容上花费更多时间。

## 6.4.2病毒程序的作用机制

### 1.引导过程

- 用带毒软盘引导系统，此时引导扇区中的病毒程序首先进入内存中，获得系统的控制权。
- 病毒程序提取系统INT13H中断向量，保存在其6CH-6FH单元中，并使系统内存总量减少1K以保护驻留内存高端的病毒程序
- 随后计算出内存高端段地址，将整个病毒程序移至内存高端，
- 修改INT13H中断向量指针，使之指向病毒程序的传染部分，完成病毒程序的激活。
- 将控制转移到内存高端的病毒引导程序处，读正常引导记录内容到0000:7c00处，再将硬盘主引导扇区内容读入内存高端,检查该引导扇区是否已被感染。
- 如果硬盘已经感染香港病毒，则执行正常的DOS引导；
- 否则将硬盘首部第3个字节起8个字节和尾部90H字节内容移至病毒程序相应位置，然后将病毒程序写到硬盘主引导扇区，完成对硬盘的感染，
- 最后再执行正常的DOS引导。

- 用带毒硬盘引导系统，此时主引导扇区中的病毒程序首先进入内存中，获得系统的控制权。
- 病毒程序修改INT13H中断向量、内存总量以及转移病毒程序到内存高端的过程与带毒软盘引导相同。
- 在完成病毒程序的激活后，病毒程序查找硬盘活动分区地址，然后直接调用该分区的引导扇区，并将控制转向该引导扇区，完成系统的正常引导。

## 2.感染软盘过程

- 病毒程序进入系统后，所有INT13H中断调用请求，均转到病毒程序传染部分执行。
- 如果判定不是读写请求或是对硬盘的读写请求，则执行正常的INT13H中断服务。
- 如果发现是对软盘的读写请求，则首先将该操作盘的引导扇区调入内存中，检查其特定位置上是否有病毒标记，若有就退出传染模块，转向正常的INT13H中断服务；
- 否则就将引导扇区内容写到1面27道08扇区，并把首部第3个字节起8个字节和尾部90H字节内容移至病毒程序相应位置，
- 然后将病毒程序写到该盘的引导扇区，完成对软盘的感染，
- 最后再执行正常的INT13H中断服务。

- 3.病毒的破坏模块
- 香港病毒在感染硬盘后，每从硬盘启动一次，病毒内部计数器加1，当系统从硬盘启动次数累计达224次后，病毒程序就会将打印口PRN1和通信口COM1的基地址置为00，使系统误认为未配置通信口和打印机，无法联机通信和打印。
- 在用软盘重新启动后，又恢复正常。

- 6.4.3诊治
- 对病毒程序的检测和清除带毒软盘的方法请自行设计
- 对于硬盘中的病毒，因为病毒程序已覆盖了主引导扇区中的内容，因此必须用原来提取的正常硬盘主引导记录，否则提取与该机硬盘相似的硬盘正常主引导记录，
- 分区信息则用带毒主引导扇区的后90H字节内容代替，把上述内容写回硬盘的主引导扇区，然后重新启动系统即可。

- 作业：p21 4， p53 2
- 1.大麻病毒、六·四病毒、米氏病毒和香港病毒它们对硬盘的感染方式有何异同点？
- 论文：写1篇2011年9月到12月期间发生的3个计算机典型病毒分析，2012年1月3日交(2000字）