第 7 章 计算机病毒

7.1 概 述

随着计算机应用的日趋广泛和计算机软件行业的迅猛发展，出现了一种严重阻碍人们正常使用计算机的新问题——计算机病毒。计算机病毒是隐藏在计算机系统的资源中，利用系统资源进行繁殖和生存，能够影响计算机系统正常运行并能通过系统中数据共享的途径进行传播的程序。

计算机病毒传播的范围以及不断发展改进的程度都是十分惊人的。前几年，当我们从新闻看到国外股票交易所内上百台机器由于遭到计算机病毒的攻击而陷于瘫痪的消息时，当我们从报纸上读到美国最大的计算机网络 INTERNET 网由于遭到计算机病毒的攻击而损失上千万美元的报道时，计算机病毒对于我们来说还是一个陌生的字眼。但是在今天，我们身边的每一台计算机随时随刻都可能被计算机病毒所侵袭，每一台从表面上看起来运行正常的机器也可能由于隐藏的计算机病毒突然发作而在短时间内毁掉数月辛勤工作的成果。每一个经常上机的计算机用户随口都能说出一大串计算机病毒的名称，如石头病毒(STONE)、磁盘杀手(DISK KILLER)、大麻病毒、火炬病毒、DIR-2 病毒，等等。针对计算机病毒这种“咄咄逼人”的架势，人们也开始采用各种各样的反击手段，出现各种各样的检查和消除计算机病毒的软件，还有不少硬件制成的防病毒卡等。但是，这并不是根本的解决办法。计算机病毒常常是“道高一尺，魔高一丈。”因为，计算机病毒的制造者可以根据目前的防病毒技术对计算机病毒加以改进，从而不断地产生出使原先的防病毒技术失效的新型计算机病毒。而这些计算

机病毒通常是在发作之后才能够被人注意到，再经过一段时间才能研制出新的解毒工具，而这时计算机病毒可能已经造成了相当大的损失。这就如同杀虫剂可以杀死害虫，但果树也已经被咬得千疮百孔了一样。因此，预防有时是比消除更有效的方法。本章旨在通过对计算机病毒产生和活动机理加以探讨，使计算机用户能够具备一些基本的预防、检查和消除计算机病毒的方法，并介绍一些计算机使用和维护的手段来减少计算机病毒发作时所能造成的损失。

计算机病毒存在的范围是相当广泛的。从小型机、工作站到最常见的微机，从 UNIX 到 DOS 系统，都有相应的计算机病毒。由于文章的篇幅有限，本文将以人们最广泛使用的微机及其上运行的 DOS 操作系统为基础，介绍计算机病毒的产生和运行机制以及检查、消除和预防的一些基本方法。

计算机病毒的编写往往是针对系统设计当中的一些缺陷所设计的，因此涉及到很多操作系统内部的知识，而且多数程序都是以汇编代码编成的，比较晦涩难懂。在本文中，我们尽量以通俗易懂的文字加以解说，目的是希望读者能够理解计算机病毒的原理，抓住病毒本身的弱点，扼住病毒的“咽喉”，具备较强的自我免疫功能和修复能力，而不仅仅是会使用病毒检查软件。

本文先举一简单的例子来讨论计算机“病毒”是怎么工作的。

7.2 计算机病毒产生的条件

在讨论计算机病毒之前，我们必须先澄清人们对它的认识。在前面讲到过，计算机病毒只是一段可被执行的程序，这种程序运行的结果对计算机系统造成的影响与生物病毒对人体造成的影响有类似之处，因此被形象地称为“病毒”，它当然不会对人造成任何伤害。计算机病毒既然是可执行的代码，那么就必须被载入内存并加以运行才能发挥作用。而一般的不可执行文件，如源代码、文本文件、数据库数据等都不会被感染上病毒。而对于染毒的可执行文件或带引导区病毒的软盘，只要不去执行该文件或用该盘冷(热)启动机器，病毒就没有被载入的条件，也就不会有任何不良影响。因此，如果机器尚未染毒，那么从软盘上拷取一些数据文件(非可执行文件)是不会将病毒引入计算机的，即便该软盘带有病毒。(注：为简洁起见，本文将计算机病毒简称为病毒，下同。)

7.2.1 计算机病毒所必需的两个条件

现在我们讨论计算机病毒产生的条件。由于计算机病毒是一段可被执行的代码，因此它要满足两个条件：一是要能够存储在外存介质上，否则一旦关机，病毒就被消除了。由于病毒代码不能像正常的文件一样存储，所以它必须以某种方式隐蔽在人们不易发现的地方。二是必须有被加载入内存并被执行的机会。因为病毒程序不能被人们主动地加以运行，因此必须寄生在某些会被正常执行的代码中，并抢先获取控制权。那么在微机上广泛应用的 DOS 环境中，它能怎样做呢?

DOS 操作系统是为基于 Intel 8086 系列芯片为核心的微机所设计的操作系统。它采用了一种全开放的设计思路，包括磁盘组织、文件系统以及系统运行机制等，这都给编程人员带来了极大的灵活性，但同时也为病毒制造者提供了条件。也许有人会问，为什么 DOS 不设计成一种像 UNIX 操作系统那种相对比较封闭、安全性较高的系统呢?笔者认为，除了 8086 芯片本身缺乏硬件设计上的安全性考虑外，性能也比较低。所以，作为一种面向个人计算机的操作系统，设计一种简单、高效、易用的系统比一个安全但复杂和低效的系统更合适。那么，病毒是如何利用它的这种开放性便利的呢?

1. 病毒是如何隐藏自身的

一种方法是将病毒本身与一些正常的可执行文件结合起来，这样做可以不涉及低层的文件管理系统；但这样做势必造成文件长度变长，对于一些有经验的操作员，观察到文件长度异常就会立刻想到病毒。

另一种方法是直接修改低层的文件管理系统，为自己分配一定的磁盘空间。

在 DOS 的磁盘管理中，将存放文件的磁盘空间映象到一块区域中来标记是否已被分配，这块区域就称为 FAT 表(File Allocation Table)。磁盘空间被划分为一个个簇(Cluster)来记录文件内容，因此一个簇在 FAT 表中可能会有三种状态。

(1)空闲状态　用 0000 表示。

(2)被占用态　其中若该簇记录了文件中间的一段内容，则该地址记录的是文件下一个簇在 FAT 表中的地址 × × × ×。若该簇记录了文件最后一个簇的内容，则该地址记录的是文件结束标记 FFFFH。由此也可以看出，在 DOS 系统中，文件在磁盘上的存放是以簇为单位的，整个文件则是以链表形式连接的。由于链表中构成链的信息全都被放在 FAT 表中，因此这个表也就成为了被病毒攻击的一个重要对象。一但毁掉这个表，则文件的内容就很难再找回来了。

(3)坏簇状态　由于磁盘质量和使用寿命等原因，在磁盘上可能会出现一些物理坏簇，使得无法正常地存取数据。DOS 操作系统允许这种情况存在。如果这个区域存在于文件区中，则将 FAT 表中相应地址处记为 FFF7H，表明是一个坏簇，以后所有的文件操作都不会理睬这个簇。正是由于这种情况的存在，病毒往往可以“栖身”于此。首先，它先选定一个磁盘区域，并将自身存储进去。然后，将该区域所在 FAT 中的标记记为坏簇，这样既隐蔽了自己，也防止了文件的存取操作将其覆盖掉，更主要的是摆脱了寄生在正常文件中而造成文件增长的弱点。还有一种方法，就是将自身存放在 DOS 看不到的磁盘空间中，例如：硬盘中的第 0 道第 0 号磁头所能读写到的扇区中。

以上这三种方法也正是三类计算机病毒。文件型病毒、引导区病毒和主引导区病毒所普遍使用的隐藏方法。

2. 病毒被加载入内存并获得控制权

计算机病毒要解决的另外一个问题就是如何被加载入内存并获得控制权。对于以上提到的三种类型的病毒也有相应的三种获取程序控制权的方法。

(1)对于文件型病毒　自然而然地想到利用宿主文件被加载的机会截取控制权。例如：对于一个 COM 型文件，文件被加载后将从第 1 个字节表示的机器码处运行，因此病毒程序通常在将自身代码附加在宿主文件之后，还要修改该文件的头三个字节为一条

含义为JMP×××××的机器代码；用以将程序运行过程先转向病毒程序，待病毒程序执行完后(完成修改中断向量、驻留等工作)，恢复宿主程序的头三个字节；然后再转回程序头去执行宿主程序，这样就完成了截获程序控制权并能正常执行原宿主程序的过程。对于另一类可执行程序EXE型文件，这个过程稍有不同。EXE型文件都含有一个文件头，该文件头包含有程序在内存中进行重定位的信息，并含有一个程序入口指针，指明程序入口的地址。因此，大多数病毒采用修改入口指针的方法，使其一进入就指向病毒程序的入口，待病毒程序运行完后，再返回宿主程序的入口继续执行。当然，为了保证病毒代码与宿主程序代码一致，还要修改文件头中的文件长度等项。

(2)对于引导区病毒　截取控制权的方法比较单一。由于系统将活动分区中逻辑上第1个扇区读入内存0:7C00H处执行，使得病毒通常只有一种方法进入内存，即用自身的代码替换原操作系统的第1扇区，而将原扇区内容移到它处存放，这样就很顺利地截取了控制权。

(3)对于主引导区病毒　截取控制权的方法与引导区病毒类似。由于主引导区位于磁盘的物理第0磁道0磁头1扇区中，在加载时也会被载入内存的0:7C00H处开始执行。因此，主引导区病毒同样采取“偷梁换柱”的手法，以自身代码代替原代码，并将原代码移至其它处存放，从而掌握控制权。

从以上病毒隐藏和截取控制权的方法中，我们可以看到DOS操作系统的开放性使得整个系统是多么的脆弱。磁盘组织和文件系统的开放为病毒“隐身”提供了方便，而文件结构的公开和系统启动过程的公开以及接口的标准化更由于缺乏安全机制，所有资源，包括系统资源，如文件系统、中断向量表等都能由用户程序访问，为病毒进入内存并运行提供了条件。

7.2.2　DOS系统的结构

既然病毒的产生和存在与DOS操作系统的结构有极其密切的关系；那么，就让我们来看看它到底有哪些地方容易被病毒利用或成为病毒攻击的对象。

1. 启动DOS的过程实际上可分为三个阶段

(1)第一阶段　由硬件重设CPU的各寄存器，并从F000:0000处开始执行程序；而F000段是BIOS部分(基本输入/输出系统)进行各项BIOS的初始工作后，从硬盘读入第0磁道0磁头1扇区的内容到内存0:7C00H后，转到第二阶段。

(2)第二阶段　程序指针转向0:7C00H，执行从硬盘中读出的程序。该段程序通常用来区分启动哪一个操作系统(DOS、UNIX或者Windows NT等)，并将物理硬盘划分为不同的逻辑盘。划分盘的数据以及此段程序通常是由DOS下的FDISK程序填写的。这段内容通常也被称作是主引导区。这段程序执行后将从硬盘的1磁道0磁头1扇区中将内容读到0:7C00H开始的内存中，然后转向第三阶段。

(3)第三阶段　程序指针仍转向0:7C00H，执行DOS的引导过程，因此这扇区的内容又被称为BOOT区；接下来连续载入IO.SYS和MSDOS.SYS两个系统文件，并启动COMMAND程序，于是DOS系统就加载在系统上了。

在 DOS 系统加载的三个过程中，都有一个控制权转交和载入下一段程序的过程。由于这个过程是公开的，因此就使病毒得到控制权成为可能。例如：第二阶段中执行的代码是从 0 磁道 0 磁头 1 扇区读到的，如果病毒替换了这个扇区，则可顺利被加载，此类病毒就被称为主引导区病毒。第三阶段中执行的代码是从 1 磁道 0 磁头 1 扇区读到，如果病毒替换这个扇区的内容，就成为另一种病毒——BOOT 区病毒。当然，还有的是没有出现在第一阶段就获得控制权的病毒，这是因为这个阶段执行的代码不是存放在硬盘上的，而是固化在 ROM 芯片中，自然无法替代。

在 DOS 环境下，文件系统的结构以及系统调用和中断处理过程都是完全公开的，很多程序都采用汇编代码写成。采用汇编代码写成的程序，代码量少，运行速度快。当然，对于病毒而言，这并不是主要原因。主要原因在于采用汇编编程就意味着可以方便地处理很多低层操作，如直接调用各种 BIOS 中断和 DOS 中断，可以容易地处理一些关键数据。例如：修改 FAT 表来提供病毒藏身之处，修改文件头内容用以加载病毒，同时也提供了病毒进行破坏的机会，即如果病毒能够存取主引导区、BOOT 区及 FAT 表的话，则可以很容易地将一台计算机置于瘫痪。

2. DOS 操作系统的中断过程

为了后面介绍病毒的方便，我们在此简单介绍 DOS 操作系统的中断过程。中断的概念是操作系统中的一个基本概念，相信大家都已经非常熟悉了。我们重点介绍中断在 DOS 操作系统中的实现。在 DOS 操作系统管理的内存最低端 1KB 空间中(0:0H ~ 0:3FFH)，存放了一张中断向量表，系统一共支持 0 ~ FFH256 个中断过程，中断向量表中记录的就是这 256 个中断过程的程序入口，每个向量占 4 个字节，包括两个字节的段址和两个字节的偏移量。每当程序发出一条指令 INT ××H 的时候，或系统硬件产生了某些中断信号的时候(例如，时钟中断)，系统就会首先计算出该中断向量在中断向量表中的位置(即 ××*4)；然后根据该点的段值或偏移量找到程序入口，继而完成保存现场和标志寄存器的工作，并转而执行中断过程。

中断向量表是一种系统资源，一般来讲用户程序是不应当任意修改它的；但操作系统并没有提供这种保护机制。中断向量表首先是由 ROM 中的 BIOS 程序初始化的，这时仅仅使用了其中的一小部分中断，都是涉及硬件的一些基本操作。例如：磁盘服务程序(INT 13H)、时钟服务程序(INT 8H)、显示器服务程序(INT 10H)等。紧接着在加载 DOS 时，DOS 系统会设置一些新的中断向量(最重要的当属 INT 21H 功能，即系统调用)，还要对某些向量重新定义(如磁盘服务功能)，以使其具有更多的功能。此外，还专门留下了一些中断号给用户使用。

中断调用是 DOS 操作系统的核心。一方面，采用中断调用的方式执行特定的操作，可以大大减短程序的长度。另一方面，通过改进 BIOS 过程和 DOS 系统，可以适应不断改进的外部设备和各种新技术的出现，而不必去修改原来的程序，使得原有程序的继承变得很容易。从另一个观点来看，是中断过程形成了软件和操作系统之间的一个标准接口，因此也就成为被病毒侵入的一个重要突破口。几乎所有的病毒都会主动地修改某些中断过程，以达到监测程序运行情况和判断是否进行传染或发作的目的，这在下面的病毒机制中将进行详细的介绍。

从这一节的介绍，我们可以知道，操作系统中那些公开的、缺乏保护的、标准的接口，往往是病毒存在和发作的基础。因此，对这些地方的过程和数据应当非常仔细地加以检查和保护。

7.3 病毒机制

从这一节开始，我们要对 DOS 环境下的病毒加以分类，并对其运行机制加以剖析。

7.3.1 病毒的分类

关于对计算机病毒的分类有很多方法。其中：按照病毒所攻击的机型来分，有 PC 病毒、Mac 机病毒等；按照病毒攻击的操作系统来分，有 DOS 病毒、UNTX 病毒等；按照病毒的寄生方式来分；按照病毒的破坏情况来分；等等。这些分类方法有的过大，例如前两种分类方法，实际上本文中只涉及到攻击 IBM PC 及其兼容机上 DOS 操作系统的病毒，而不涉及其它的机型及操作系统；有的分类法又过于模糊，例如最后一种，通过病毒造成的破坏来分为是良性病毒或恶性病毒是不太恰当的。因为，一方面我们不能通过这种分类方法来设计相应的病毒检测防范措施，另一方面这种分类实际上也不能将病毒明确地进行分类，而且绝大多数病毒的破坏能力都介于良性和恶性之间。况且，这种划分方法与人本身的因素也有很大关系，一个病毒造成的破坏对一般的计算机用户来说可能是灾难性的，但对于一些计算机专家却不是问题，他可以轻而易举地恢复计算机的状态，就像没有发生过破坏一样。

我们下面要介绍的是第三种分类方法，即按寄生方式分类。通过按照寄生方式的分类，我们可以设计出比较有效的防范措施，切断病毒存在的条件，并能够通过对病毒地区的监视达到检测病毒的目的。基于 IBM PC 及其兼容机上的病毒可以按照寄生的方式分为以下三类：

1. 寄生在主引导区

这类病毒将自身隐藏在硬盘系统的主引导区，利用 ROM BIOS 启动后向磁盘系统转交控制权时进行截获并驻留内存，然后再伺机传染和发作。这一类的病毒有 Disk Killer、Tourch、幻影病毒等。

2. 寄生在引导区

这类病毒将自身隐藏在 DOS 操作系统引导区的第 1 个扇区中，当启动 DOS 系统时首先截获控制权并驻留，然后再伺机进行传染和发作。这一类的病毒有 Stone、小球病毒、大麻病毒等。

3. 寄生在文件中

这类病毒将自身与正常的文件结合起来，通常加在程序的头部或尾部，在程序被加载时首先获得控制权。这一类病毒大部分也会驻留内存，并伺机传染和发作；但也有一

部分病毒并不驻留内存，而是每次仅执行一遍，并立刻进行传染其它文件的动作，然后迅速退出。这样做，主要的目的在于防止病毒检测工具通过对驻留动作的监视来发现病毒。此类病毒中驻留内存的有 1701 病毒、Yankee Doodle 病毒等。而不驻留内存的则有 VIENNA 病毒等。

以上这三种类型基本上可以涵盖微机中的绝大部分病毒，但也不是绝对的。例如：有一种叫做 2153 病毒(又称 Omicron 病毒)，该病毒既可以寄生在文件中，也可以寄生在引导区中。由于该病毒同时要有两种寄生方式和传染方式，因此会使程序编制起来比较复杂，增加程序的长度。这种病毒与其它病毒相比，具有更强的感染能力。由此可以看出，对病毒进行清晰精确的分类是非常困难的。而对于病毒制造者来说，编制一个具有多种属性的病毒却不是一件难事。

7.3.2 病毒的构成

大多数的计算机病毒一般都包含四个程序功能部分。

1. 程序引导部分

程序引导部分通常要将病毒自身置于内存中相应空间并驻留，修改相应的中断向量以连接检测激活部分。

2. 检测激活部分

检测激活部分通过当前计算机程序对中断的调用来感知目前计算机所处的状态和所做的操作。根据不同的情况决定不响应、传染或发作。

3. 传染部分

传染部分用来进行病毒自身的复制并附加到未染毒的引导区或代码中。

4. 表现部分

表现部分也就是病毒经过一定的潜伏阶段，在时机成熟时开始发作表现的代码段。病毒进行发作的现象无奇不有，有的仅仅是恶作剧，并不破坏整个系统；有的则会摧毁硬盘删除文件，使整个系统瘫痪。

虽然病毒通常都有以上这四个部分，但其中的巧妙却是各不相同，表现出来的现象也是各不相同。下面我们详细介绍各类病毒在不同阶段的具体实现方法。

7.3.3 若干病毒类型

(一)主引导区类病毒

主引导区类病毒，如大麻病毒和 6.4 病毒等，流行得非常广泛。首先，我们要介绍一下主引导区的基本功能和结构；然后，以典型的主引导区型病毒——大麻病毒为例分析此类病毒的构成。

1. 主引导区的基本功能与结构

在 IBM PC 及其兼容机上，一般同时安装一至两个硬盘(A、B 盘)，但为什么我们在上机时发现含有 C、D、E、F 等硬盘盘符呢?这是因为在每一个物理硬盘上都可以划

分出若干个分区来，这些分区在硬盘的管理和使用上更灵活、更方便，最重要的还在于可以在一个物理硬盘上安装多个操作系统，使不同的操作系统可以按自己的方式来组织硬盘而互不干扰。为了对物理硬盘进行划分，首先将硬盘的0磁道0磁头全部划归主引导区使用，将剩余的空间连续地划分给不同的分区。

主引导区由两部分构成：引导程序和分区表。其中，分区表描述了硬盘中各个分区的划分情况，包括起始磁间、磁道、扇区和终止磁头、磁道、扇区等以及是否为引导盘，如果被指明为引导盘，则接下来将会引导该分区上的操作系统。引导程序通常都比较短，最主要的作用就是读取磁盘划分的信息，并从被标记为引导盘的分区上读入第1个扇区的内容，并转去执行该段程序。这两部分内容都比较短，通常只需要一个扇区，其余的扇区就全部被空闲下来。

由于主引导区不属于任何分区，也不依赖于任何操作系统的载入；因此，并非基于DOS系统。所以，使用DOS系统中的功能调用(INT 21H)或绝对磁盘读写功能(INT 25H，INT 26H)都不能读写主引导区的内容，而只能用有关物理硬盘读写的BIOS调用(INT 13H)才能够读写该区内容。这也就是为什么有时人们采用格式化硬盘的方法仍然不能消灭病毒的原因。

2. 主引导区病毒的特点

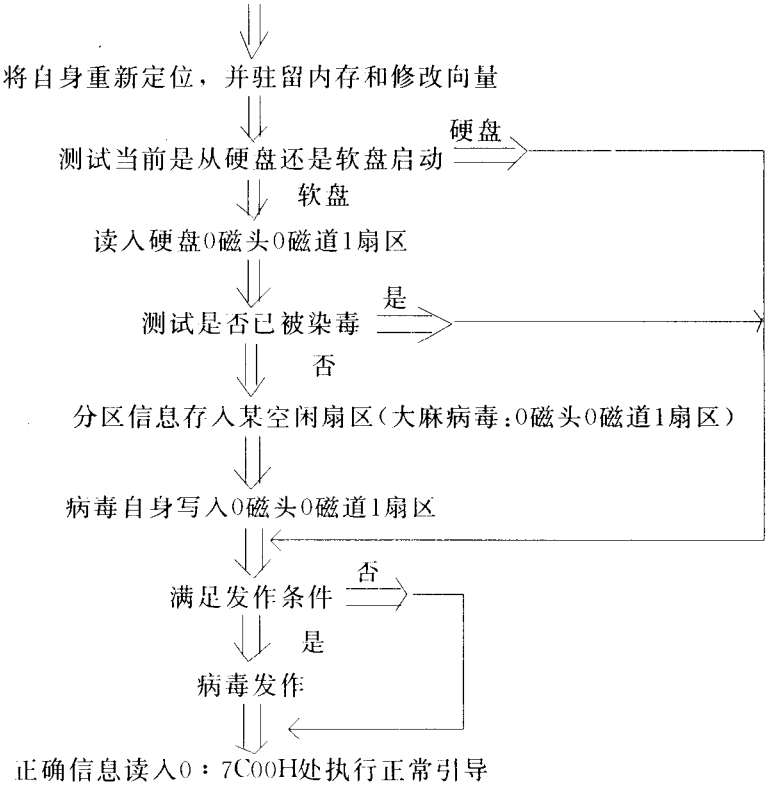

图7.1　病毒加载过程

(1)病毒加载过程　由于主引导区必然占据0磁头0磁道1扇区，同时又空出了0

磁间 0 磁道的其它扇区；因此，主引导区病毒必然要以自身替换原主引导区的内容，同时为了不造成死机，还要将原来内容移到空闲的其它几个扇区中。由于病毒占据了主引导区，系统启动后会首先进行病毒的加载，病毒进入内存后，再读出原主引导区的内容进行引导。病毒加载的过程见图 7.1。

(2)病毒驻留方式　主引导区类病毒在驻留时采用驻留高端的方法。大麻病毒就是首先确定出 RAM 的最后地址，然后将自身拷贝到 RAM 最高端的最后 2KB 中，并将 ROM BIOS 报告的 RAM 空间相应地减少 2KB。这样，在引导操作系统时，操作系统根据 ROM BIOS 的报告来确定可用的 RAM 空间，而不会理睬真正的 RAM 空间大小，因此就不会覆盖掉病毒存放的空间，从而使病毒能够完全地隐藏在内存中；但此时用 CHKDSK、MEM、PCTOOLS 等能查看内存大小的工具时，就会发现内存的减少，这是判断内存中是否有病毒的最简单方法之一。加之，主引导区病毒可修改的中断向量也很有限，因为与操作系统有关的中断向量尚未安装，所以只能修改 ROM BIOS 已经设置的一些向量，最重要的有 INT 13H(磁盘服务功能)、INT 8H(计时器中断)、INT 9H(键盘中断)和 INT 10H(显示器服务中断)。其中，为了能够传染的需要，INT 13H 是必定要被修改的，大麻病毒就是靠修改 INT 13H 中断向量来传染的。

(3)病毒监测部分特点　主引导区病毒的监测部分通常都是通过监测 INT 13H 的功能调用来确定是否进行传染或发作。对于硬盘的读写操作通常不予理睬而直接进入正常的中断部分，因为硬盘启动时就带有病毒或由软盘在启动时传染上，而不必重复传染。而对于软盘的各种操作，通常都要进行传染，因为这类病毒必须通过软盘来扩散。对于病毒发作的激活条件可以有很多，利用检测时间或检测启动或传染的次数等，这要具体到某一个病毒才能仔细地讨论。对于原始的非变种大麻病毒，其激活是靠一个内部计数器完成的，机器启动 8 次后，将显示：

Your PC is now stoned!

(4)病毒传染部分特点　关于病毒的传染部分有其独有的特点。因为分区是硬盘所特有的，而对于软盘来说，没有也不必有分区这一部分，其 0 磁头 0 磁道 1 扇区直接就是操作系统的引导部分。也不存在像硬盘上的独立于操作系统的空闲扇区。多数病毒为了使程序短小，通常都不再考虑这类问题，而是像感染硬盘一样将原 0 磁头 0 磁道 1 扇区的内容搬到 0 磁头 0 磁道的其它扇区中，而将自身隐藏于 0 磁头 0 磁道 1 扇区中。由于软盘没有分区，因此所有的扇区都已经被 DOS 管理起来，因此这种覆盖过程有时就会有负面的影响，例如：大麻病毒采用 1 磁面 0 磁道 3 扇区来存放 BOOT 区内容，这一物理上的扇区在不同的软盘上对应于不同的逻辑扇区，在 360KB 双面双密度软盘上对应于目录区的最后一扇区，若根目录中文件不太多也不致于有什么影响，而在 1.2MB 双面高密度软盘上对应于目录区的第 3 个扇区，由于每个扇区只有 16 个文件项，因此当根目录中的文件超过 32 个时，文件系统就会发生故障。这就是软盘和硬盘的使用方法不同，但病毒传染方法却相同所造成的不一致。

(5)病毒发作特征　病毒的发作部分很难找到其共有的特性。一般主引导区类病毒不依赖于操作系统，因此可用的中断比较少，功能也弱，所以表现也比较简单。如果病毒试图破坏时，通常会破坏系统的分区部分，造成系统不能启动；如果用软盘启动，也

看不到硬盘上的内容，因此对于无经验的用户或忘掉分区信息的用户都是灾难性的后果。有的恶性病毒如磁盘杀手病毒，发作后会对硬盘格式化导致严重后果。

(二)引导区型病毒

引导区型病毒在很多方面与分区表病毒有相似之处。这一类病毒的种类有很多，例如：小球病毒、磁盘杀手病毒等。引导区型病毒寄生在 DOS 系统分区的引导区中，通过分区中的引导程序向操作系统程序传交控制权时截取控制。下面我们以小球病毒为例，介绍引导区型病毒的结构特点。

前面讲过，通过分区表中的参数，硬盘被划分为一个个分区，其中有且仅有一个被标明是活动的(Active)，主引导程序将该分区起始磁头、起始磁道的第 1 个扇区读到内存 0:7C00H 处(就如同 ROM BIOS 连接硬盘分区程序一样)，然后转而将控制权转移到 0:7C00H 处执行引导程序。在目前绝大多数用户仅安装一个 DOS 操作系统的情况下，系统引导区的物理位置通常紧紧接在主引导区(包含空闲扇区)之后的 0 磁道 1 磁头 1 扇区上。

(1)系统引导区特点　系统引导区也由两个部分组成：一是基本参数区，另一是引导程序。基本参数区记录了该硬盘的一些物理属性，如每扇区字节数、每磁道扇区数、磁头数等，还有一些建立 DOS 文件系统所需的逻辑属性，如每簇扇区数、文件分配表(FAT)数目和根目录登记项数等参量，DOS 系统通过这些参量将物理硬盘映射到一个逻辑盘上，并建立起相应的文件系统，使高层的用户不必理会硬盘的物理属性就可以进行简单方便的文件操作。

引导区的另一部分是引导程序，引导程序的功能是根据基本参数表的参数确定系统软件 IO. SYS、MSDOS. SYS(MS DOS 系统)或 IBMBIO. COM 和 IBMDOS. COM(PC DOS 系统)的逻辑位置，并装入第一个软件加以运行，从而开始安装操作系统。

(2)病毒载入过程　引导区病毒的载入过程与主引导区型病毒非常相似。由于它仍旧是先于操作系统而进入内存的，因此内存驻留方式与分区表病毒一样，都是通过减少 ROM BIOS 报告的内存总量来将自身存放在系统不可见的内存高端。与分区表病毒差别较大的应该是该病毒的传染和发作部分。

(3)病毒传染部分特点　引导区病毒的传染部分与分区表有很多不同。首先，在操作系统管理的文件系统中没有像主引导区中那种既空闲又不会被用到的空间。因此在病毒将引导区搬家时是不能随便找扇区存放的，否则容易出现问题，也容易被发现。其次，如果将引导区移到分区表中空闲扇区的方法则势必如分区表病毒一样影响在软盘上的使用(软盘上没有分区)，为此，引导区病毒通常采取以下的方法来进行引导区的搬移：利用引导区的参数计算相应的参数，了解逻辑盘内磁记录的分布情况，利用 FAT 表查找空闲的扇区，并将引导区以及自身剩余的部分存入，再将 FAT 表中该扇区的记录由空闲变为坏簇。小球病毒就是通过这种方式传染的。

下面先介绍 FAT 表的基本结构。我们知道，磁盘主要是用来记录文件的，但又不能用物理连续的方式来记录文件，那样会造成大量的磁盘空间浪费和碎块。所以，操作系统采用以下的方案来进行分配。首先，将磁盘空间分为一个个基本分配单位，称之为

簇(CLUSTER)，FAT 表记录的就是这一个个簇的使用情况，如果未被分配，则标记 0000；如果被使用，则一定是某个文件的一部分。如果在该文件的中间，则该簇被标记为 0～FEFFH(即下一段文件占用的簇号)；如果是文件尾，则以文件结束标记 FFFFH 来记录。文件的第一个使用的簇记录在文件目录项中。这样就将文件的记录从物理结构上以链方式存储，其逻辑结构则是连续的。其次，还有一种情况就是坏簇标记，为 FFF7，这是为了防止有些磁盘由于质量问题出现少量的差错又不会影响到磁盘整体使用的方法。坏簇标记只有在磁盘被格式化时才会记录在 FAT 表中，除此之外，任何的 DOS 操作都会忽略这个区域。

有人可能会问，为什么只能用坏簇法来隐藏病毒，而不用记录文件的方式来存放病毒?这是因为记录文件的方式必须在文件目录项中有相应文件的一些信息，如文件名、日期、属性、长度以及最重要的首簇指针。而病毒在目录项中都不可能占据一个目录项。如果硬采用文件记录的方法，则当用户使用诸如 CHKDSK 一类的程序时，会检查 FAT 表的合法性，对于缺少文件头指针的文件链会报告错误并重新标记这些空间为空闲，从而回收到操作系统中。这通常是为了在计算机进行磁盘操作时出现故障而造成 FAT 表不一致的一种补救和恢复方法。所以，对于引导区类病毒，都是采用标记坏簇的方法来隐藏的。

虽然引导区病毒也是优先于操作系统被加载的，但也不是说只能用 ROM BIOS 的调用，如果像主引导区病毒一样只要用软盘启动就会传染硬盘的话，那么当然只能使用 INT 13H 进行传染，但那样对于在 DOS 的文件系统中查找空簇等过程就过于麻烦了。实际上，大多数的引导区病毒只是利用引导区中的过程加载并驻留到内存中，等到操作系统加载到内存中之后，再寻机进行传染，这时可以直接利用 INT 25H、INT 26H(逻辑盘中扇区的绝对读写功能)，用该功能来实现以上功能就要简便多了，也可以大大减少病毒代码的长度。这里的关键在于监测操作系统是否已被载入。方法可以多种多样，只要在得到控制权后检测一下 INT 25H、INT 26H 的中断向量与病毒被加载时是否一样就可以了。如果一样，表明向量未被修改，不能使用；否则，表明已被操作系统正常地设置了，则可以进行各种操作。

至于引导区病毒表现模块也可按发作时间的不同而分为两类：一类是在系统启动之前伺机发作，这样就如同分区表病毒一样，可选用的中断调用仅限于 ROM BIOS，因此表现方法通常很简单，以摧毁引导区和 FAT 表等为主。另一类是在系统运行期间伺机发作，这样可选用的中断调用就大大增加了，发现形式也就各式各样。

小球病毒就是采用截取时钟中断 INT 8H，在整点或半点对磁盘进行读操作时激发的，其表现为屏幕上出现一个来回反弹的小球，至机器重新启动。

主引导区类病毒和引导区型病毒的防范

从前面介绍中可以看出，引导区型病毒都是通过由软盘启动系统加载病毒而获得系统的控制权，进而驻留内存进行扩散或发作的。所以，有效地防止由带毒软盘启动系统是防范这类病毒的关键，而且非常有效。用户平常就应注意启动时不要在软驱中放入磁盘，并应将机器设置为由硬盘启动在先。采取以上措施，引导区型病毒的侵染是可以有

效预防的。

(三)文件型病毒

文件型病毒同前两类病毒比较而言，最大的优势在于可以充分地利用操作系统提供的丰富的中断调用，可以通过寄生在文件内部来隐藏，可以不管磁盘的物理结构，并且不会破坏磁盘的结构，就像正常的应用程序一样，具有很好的隐藏性能和较高的检测难度。常见的病毒有 1701、1575、黑色星期五等，种类很多。

(1)病毒驻留方式　文件型病毒只能寄生在可执行文件上，否则是不会被感染上病毒的，这就是为什么在检查文件时不检查数据文件的原因。病毒寄生在文件上不仅仅要从文件的逻辑结构上成为一体(嵌在原文件头部或者附加在尾部)，还必须使该程序的程序入口指向病毒，这样才能让病毒正确地进入内存并被执行。寄生在文件中不是件难事，但要想使程序入口指向病毒就必须去分析程序结构，并了解程序加载的过程。这一过程我们在讨论传染模块部分时再作介绍。

文件型病毒在文件被执行时首先获得程序控制权，其加载模块的目的仍旧是驻留内存，修改中断向量，使其连接到病毒的检测模块中。此类病毒的驻留方法已不能同前两类病毒一样进行驻留了。因为，此时的内存由操作系统统一控制，不再依赖于 ROM BIOS 报告的内存总量，此类病毒的驻留涉及到系统的内存分配控制链以及程序的进程创建等多项知识，为简便起见，在此就不做过多地介绍了，有兴趣的读者可以参考有关的资料。这类病毒虽然驻留过程比较复杂，但同时也带来了驻留方式多样化，与正常驻留过程难以区分的好处。由于文件型病毒种类很多，采用的传染方式和驻留手段也各式各样，没有特别典型的文件型病毒，在此就不举例了。

(2)病毒监测部分特点　对于文件型病毒的监测部分，由于已经加载了操作系统，因此可以截取一些含义更为明确的中断调用，例如 INT 21H 中的文件打开功能，从而获得该文件的路径及名称，如果恰好是可执行文件，则可以立刻启动传染模块将该文件染上病毒；如果仍旧截取 INT 13H 这类磁盘的操作，则不能确定该操作是否对文件进行，即便是对文件进行，也无法获得该文件存放的物理结构，并进行病毒附加的工作。总之，由于有了这些功能更强、分类更细的中断，监测部分可以更加容易地了解当前系统运行的状态，从而指示传染模块或表现模块执行更加有针对性的操作。

(3)病毒传染部分特点　在病毒的传染模块中，体现了不同文件型病毒千变万化的寄生方式。在这里，我们简要地介绍一下。

DOS 操作系统中含有可执行代码的文件有三类，分别以 COM、EXE 和 SYS 做为其后缀。其中，SYS 文件为设备驱动文件，不能在命令行中直接加以运行；因此，大多数病毒针对的是 COM 文件和 EXE 文件。

COM 文件是一种比较简单的可执行文件，整个文件被全部加载到内存中，并从该文件的头一条指令开始执行。对于这类程序，病毒通常采用附加在程序尾部的做法，同时保留原文件的前三个字节，并将原文件的前三个字节改为一条段内跳转指令 JMP × × × ×，使程序一进入内存就转到病毒内部执行，待病毒加载完毕后，恢复程序首部的头三个字节，然后转回程序首部继续执行宿主程序。

COM 文件结构简单，但限制编程人员只能编制单段程序，且长度小于 64KB 字

节。现在，大量的可执行文件采用 EXE 文件结构。这种文件在文件首部是称为文件头的部分，包含了程序在被加载时的一些重要参数，但是其本身并不被操作系统调入内存中。对于文件的其余部分，虽然也被加载到内存中，但是程序的入口却不一定是被加载部分的首部，该位置被文件头中的参数所设定。因此，病毒通常采取以下的方法：首先将自身附加在程序的尾部，然后记录下原程序入口的参数，并用新的病毒入口代替；这样，程序一被加载，即从病毒的入口处开始执行，待病毒加载完毕后，即根据原程序的入口参数将控制权交回原程序。

大多数病毒的寄生方式都是直接附加在程序尾部的，但也有一些是插在程序的首部(针对 COM 文件)，这样可以自然地获得程序控制权，但执行宿主程序时需要解决一些环境变化上的问题，例如程序段前缀 PSP 宿主程序不一致等，一般可以通过将宿主程序前移覆盖病毒自身来解决。

文件类病毒由于可以利用大量的由操作系统提供的中断向量；因此，无论在传染、发作、检测还是加载中的变化就非常之多，而且与正常的程序有较多的共性，难以有统一的检测方法。一般只能采用判断特征字串的方法检测。由于文件型病毒与可执行文件结合在一起，因而比引导区型病毒难于去除，更应该注意防范。

7.3.4 病毒的检测和消除

关于病毒的检测，主要可以分为静态检测和动态检测两类。静态检测指的是检查当前硬盘或软盘中的分区表、引导区和文件中是否含有病毒。动态检测指的是检查当前内存环境是否含有病毒以及加载的应用程序是否带有病毒等。

1. 静态检测

静态检测可以采用目前众多的病毒检查工具如 SCAN 和 KILL 等。在查病毒工作时需要注意以下几点。

(1)查毒工具使用　各种工具各有优点，如能交叉使用，效果会更好，一种查病毒工具发现不了的病毒往往可以被其它的工具发现。

(2)查毒运行环境　使用查病毒工具时应尽可能保证运行环境中无病毒。一般来讲，应用不带毒的软盘进入操作系统，再用带写保护的无病毒的查病毒工具来运行。

有些人认为病毒检测工具是没什么用的，因为每年都会有成千上百种新的病毒产生。实质上，这是一种错误的认识。首先，由于编程上的问题，很多的病毒并不能正确地工作和复制，以致于不能传播。对于其它正确的病毒，又有大部分由于没能在足够多的机器上进行传染而会在一定范围内逐渐消失。在剩下的病毒中，又有将近一半的病毒被立刻发现并被加入到反病毒软件中。由此可见，仅有很少的一部分新病毒可能会流传开。但即便如此，通常也会不久就被发现并报告出来。所以，采用病毒检查软件绝对是一个有效、简便的防病毒措施。其次，上面这个错误认识的另一缺陷在于认为新型的病毒是无法预见其特性的，这也是不对的。以文件型病毒为例，被感染的文件不可避免地其内容和长度会发生变化，因此采用校验和的方式就可以很好地检测文件是否被病毒感染，包括最新型的文件型病毒。

除了采用软件工具进行检测病毒之外，一些比较专业的计算机工作者也经常通过手动的方式来检测病毒(通常在软件工具无法查出病毒，但同时又怀疑机器中确有病毒存在的情况下)。采用手动的方式这里不详细讨论，仅提出下面的基本步骤以供参考。

(1)步骤一　用干净的软盘启动，保证机器运行中不带病毒。首先检测硬盘的主引导区和引导区。主引导区置于硬盘的 0 磁道 0 磁头 1 扇区中，该扇区不能由 PCTOOLS 等工具看到，可以使用 DEBUG 调试工具，直接调用 INT 13H 命令读取或写入。引导区大多在 0 磁道 1 磁头 1 扇区中，可以用 DEBUG 工具读写，也可以由 PCTOOLS 等软件读写。有经验的人员很容易判断其是否正常。由于主引导区和引导区存放硬盘使用的重要信息，因此对此不熟悉的人员最好不要随意修改，以防硬盘上的数据全部丢失。

(2)步骤二　若主引导区与引导区不含病毒，下一步就要寻找被病毒感染的文件了。最简易的方法是利用软件工具，如 CPAV 等在检查病毒时生成的文件校验和 CHKLIST. CPS 寻找被修改过的可执行文件。除此之外，也可以先检查诸如 COMMAND. COM 以及 EDIT. EXE 等被频繁使用的程序。一旦确定了病毒的所在，通常就可以利用软件调试工具对病毒加载，进而进行分析，这里就不再赘述了。

静态检测通常是作为一种例行的工作来进行的，例如每天开机之时。但这并不能防止人们在运行软件时未检测出的病毒侵入计算机，特别是不能有效地阻止病毒的发作。动态检测就是为这一目的所设置的。

2. 动态检测

动态检测就是在系统的内存中加载一段驻留程序或采用防病毒卡对用户运行的软件加以监测，一旦发现用户的程序有类似于病毒的操作，诸如修改中断向量表、驻留内存等可疑之处，立刻提示用户，由用户决定继续运行还是退出。即便用户不小心运行了带病毒的软件，并使病毒侵入了系统，也不必担心。动态监测还保护硬盘中的重要资料，如分区表、引导区以及可执行文件等。一般来讲，这些信息是不会被修改的，而病毒的传染及发作又势必要修改这些信息。因此，一旦监测程序发现有修改这些信息的操作，又会立刻示警，以提示用户注意。有了这样的双保险，病毒的感染当然被极大地限制了。

动态检测的工具也有很多，我们会在下一节加以介绍。通常没有直接的方法来判断系统是否已经感染了病毒。一般的方法比如查看系统内存、检查中断向量的设置情况等，只有比较有经验的人才会发现。一些查病毒软件在检查硬盘上的病毒之前会先检查一下内存中的病毒，通常采取特征串识别的方法扫描内存，却不是手动能办到的。况且，在大多数情况下，一旦发现内存可能含有病毒，都会重新启动机器并采用静态检测的方法去检查硬盘上的病毒。只要硬盘或软盘中没有病毒，机器启动后是不会带有病毒的。

与检测病毒紧密相联的则是病毒的消除问题。一般来讲，有两种方法消除病毒。一是根据病毒的特性，恢复被病毒替换的主引导区和引导区，删除寄生在文件中的病毒代码等。二是用新的主引导区、引导区或文件覆盖掉原先的内容。若采用软件工具来清除病毒，这些工具都采用第一种方法。而个人手动清除病毒，则采用第二种方法即简单又有效。这些方法的具体应用将在下一节中作详细的介绍。

7.4 实用的病毒防治技术

对于绝大多数的计算机用户而言，关心的主要问题并非全面地了解病毒运行机制，甚至手动地消除病毒或是编制病毒程序；而是如何在日常工作中有效地防止病毒侵入，又不至于过分限制计算机的使用。在病毒侵入或发作的时候如何处理，并将可能造成的损失减少到最少呢?本节介绍的主要内容就是利用目前的病毒防治工具保护自己的计算机系统，并提出一些日常工作的好的习惯来保护自己的工作成果。

本节介绍的软件是 Central Point 公司的 PCTOOLS 8.0 套装软件。相信大家对 PCTOOLS 工具都很熟悉，PCTOOLS 8.0 是该软件 5.0，6.0，7.0 后的又一升级版本，几乎覆盖了用户管理磁盘文件的所有需要，其中的病毒防护工具功能强大，若能熟练使用，即便没有防病毒卡等硬件措施，也能有效地阻止病毒侵入，同时具有的多个数据保存—恢复及磁盘修理工具可将病毒发作造成的损失全部恢复出来。同时，还将介绍另一个套装软件 Nort on Anti Virus，该软件也很有效，是很多人喜欢使用的一个工具。

7.4.1 备份重要的磁盘信息

当一台计算机刚刚将操作系统安装完后，首要的一件事就是保存这台机器的基本配置，如分区表、引导区、操作系统等信息，并将其妥善保存起来。这些数据一旦被破坏，整个系统就会完全瘫痪。因此，备份这些数据的目的就是留待以后恢复该系统所用。这样，所做的各项工作仍可从磁盘上找回，而不至于重新格式化造成数据全部丢失。

在 PCTOOLS 8.0 中有一应用程序，名为 EDISK.EXE，该程序就是专门为用户制作 Emergency Disk(应急盘)的，该程序可直接在 DOS 提示行下运行，也可从 PCSHELL 的菜单 TOOLS 一项中选取来运行。

该程序首先检测系统内存中是否有病毒，若没有，则进入主菜单。它提供三个功能：Create(建立)、Update(修改)和 Option(选项)。用户可以用建立命令建立一张系统数据的应急盘，也可选用修改功能将系统中某些变化了的数据存入先前建立的应急盘中，可以节约格式化以及存入其它不变信息的时间。选项功能可以让用户选择所需备份的信息，用户一般可以不理，程序会根据选用的应急盘容量大小自动选择最重要的信息装入。

应急盘中一般包含以下几项内容：

(1)操作系统　该系统与硬盘中的一致，在硬盘感染病毒之后，可以作为自启动软盘使用，并且不会与硬盘的操作系统版本冲突。

(2)磁盘修理工具 DISKFIX.EXE　这也是 PCTOOLS 8.0 中的一个应用程序，利用它可以很容易地恢复系统的 CMOS 设置、分区表、引导区等，还可以对磁盘文件系统进行修理等。具体操作不再详细介绍。

(3)MOS 以及分区信息　CMOS 中存储了机器硬件配置的一些基本参数，最主要的有软盘和硬盘的种类，日期、时间等。若病毒破坏了 CMOS 的内容，机器将可能识别不到软盘、硬盘等。其中硬盘参数在不识硬盘的情况下很难设置正确，用户可以先手动修改软驱类型，待系统从软盘启动后，利用 DISKFIX 程序可将其余参数复原。分区表以及各逻辑硬盘的引导区与以上的 CMOS 信息共同存放在文件 PARTNSAV. FIL 中。

(4)CONFIG. SYS 和 AUTOEXEC. BAT 文件　这两个文件用于在系统从软盘启动后自动进入 DISKFIX 软件。

除此之外，若软盘容量较大，还可装入其它一些工具，如 DOS 中的 FDISK、SYS、或 PCTOOLS 中的 PCFORMAT、CPAV 等，以方便用户在仅有软盘的情况下方便地管理硬盘。以上这些均由程序根据软盘容量自动选择，当然也可根据用户需要在“选项”功能中设置。

建立好的应急盘应当贴上写保护标签，并妥善保存，平时不再使用。一旦机器病毒发作，特别是出现硬盘不识别、不启动或确定在分区表、引导区中含病毒时，则将应急盘取出，从软盘启动后，恢复这些被破坏的信息。

运用应急盘可以方便地存储和恢复这些关键数据，但若没有此软件，用户也可以自行备份。首先用 FORMAT　A:　/S 命令制作一张可引导盘，然后拷入自己熟悉的一些应用软件，如 DOS 中的 FDISK、FORMAT 等，以及 Nort on 系列软件中的 NU、NDD、DISKEDIT 等工具。其它一些重要的系统信息必须由自己记录下来，如利用 NU 中的功能可以读写分区表、引导区等并以文件的形式存储在软盘中。不过这些都不如直接用 PCTOOLS 8.0 中的 EDISK 方便。

Nort on 的 Anti Virus 软件中也有类似的功能，在 NAV 软件中含有 Create Rescue Disk(建立急救盘)的功能，可将 CMOS、分区表、引导区的信息记录在软盘上，但用户必须先手动地格式化软盘，并手动地将相应的 NDD 等软件拷贝到软盘上。

7.4.2　定期检查病毒和备份数据

在日常使用计算机时，定期地进行病毒检查是必要的，这是预防病毒侵入计算机的第一步。PCTOOLS 8.0 中的 CPAV 就是专门检查和清除病毒的工具。一般来讲，可以在每日工作前运行 CPAV，检查一下硬盘上的文件是否含有病毒，然后再开始工作。

CPAV 在检查病毒时，会在每一个目录下生成一个 CHKLIST. CPS 文件，该文件记录了每个文件的文件日期长度、校验和等信息。以后再检查到这一文件时，若发现这些数据不同，则会提示用户。我们知道，对于文件型病毒，必然会修改被感染的文件，这必将在文件的校验和中反映出来。因此，这一点对于预防新型的未知病毒是十分有效的。但是，对于一些文件，如 CONFIG. SYS 和 AUTOEXEC. BAT 以及用户自己编制的软件，由于正常的改动也会导致 CPAV 报警，这时只要简单地选择 Update(更新)就可以了。如果是一些常用的文件发生了改变，如 COMMAD. COM 和 EDIT. COM 等，通常表明被新的病毒感染，而 CPAV 没有检查出来，这时应当换取其它的查病毒工具(如公安部发行的 KILL. EXE)再检查一遍。但这种情况是很少的。