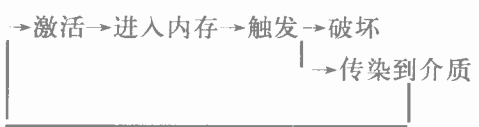
计算机病毒的免疫和监测方法

常州市统计局 高卫民

摘要：本文根据计算机病毒的工作机理，提出了采用保护磁盘的计算机病毒免疫法和监测内存的计算机病毒检测法，文中就设计思想，基本原理和处理办法进行了论述和探讨。

目前防治、检测计算机病毒的方法五花八门。但是从根本上实现计算机病毒免疫的方法还没有。从目前流行的计算机病毒防治方法来看，最可靠的是实现计算机使用的封闭式管理，由于降低了计算机的使用价值，因此，最不愿为广大计算机用户所采纳（对于银行系统、邮电系统和一些实时控制、监测系统是可行的）。一些计算机病毒的检测软件最为广大用户所欢迎，但检测的局限性使计算机仍然面临相当大的病毒感染的威胁。

如何从根本上防治计算机病毒呢？这首先要弄清病毒的工作机理。



病毒的工作过程告诉我们，介质（磁盘）上病毒的存在是病毒传播的必要环节，同时也可以看出，内存中病毒的存在是病毒发作（破坏和传染）的先决条件。因此，笔者认为，对于 DOS 系统，防治计算机病毒的最有效手段有两种：

1,对磁盘实现有效保护；

2,对内存使用实行实时监测。

对于第一种方案，计算机病毒是在磁盘中得以长久保存的，因此，切断病毒写入磁盘的途经是最有效和最可靠的防治手段。另外，由于计算机病毒在写入磁盘之前，必定先进入内存，因而检测到对磁盘的非法写入，就等于检测到了计算机内存中的病毒存在。在这种情况下，只要重新进行系统引异，就能消除病毒在计算机内存中的存在，并能及时确定病毒来源。

从病毒的工作过程看，计算机病毒必须具备可以激活的基本条件，就是说，保存到介质（磁盘）中的病毒必须具有可以执行的环境，否则只能是“死”病毒。因此，向磁盘写入的病毒一定是植入可执行的系统文件或用户文件中，而大都可执行文件正是禁止修改的文件。对于少数需要修改的可执行文件，可通过换名的办法来解决。

根据以上分析，可以从两方面来判断非法的磁盘写入：

1.在非磁盘初始化、格式化状态下对磁盘根区、系统文件区的写入；

2.对可执行文件（·EXE，·CON，·OVL，·SYS）的修改。

对第二种操作判断，我们可以通过修改 DOS 功能调用 INT21H 命令来实现，因为对文件的操作都是通过 FCB 文件控制块来进行的，因而，通过监测 FCB 状态，可以达到控制写磁盘文件的目的。这种判断过程可以简单用附图 1 表示。

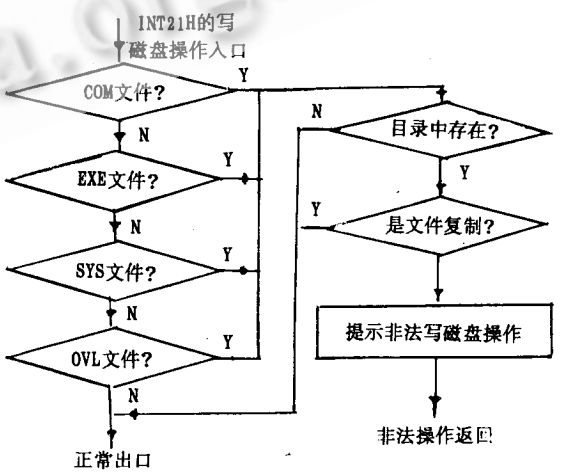


图 1

说明：INT21H 中有几个涉及到写磁盘操作的子程序，因此，该判别程序应插入到所有的子程序中。

对于第一种操作判断，可以通过修改 BIOS 中 INT13H 命令来实现，该命令因为在 ROM 中，因而修改比较困难，一个比较实用的方法是用扩充 ROM 卡，同时修改相应的中断向量，达到修正 INT13H 功能的目的。其基本判断过程可以用附图 2 表达。

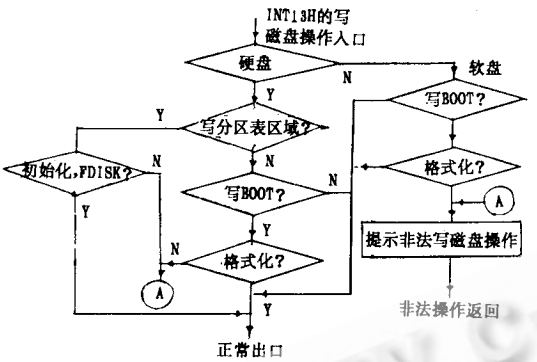


图 2

另外要说明的是，要从根本上切断病毒写入磁盘的通道，还应该考虑到 INT26H 对磁盘的写操作（该命令实际使用较少）。由于 INT26H 是对磁盘按逻辑扇区号顺序读写，而系统中能满足这种条件读写的只有三个系统文件（IBMBIO.COM，IBMDOS，COM，COMMAND、COM），因而只要在 INT26H 命令中插入对系统三个文件的保护即可。对于病毒写入非执行文件或病毒程序插入可执行文件之后用 INT26H 命令写入磁盘的情况，因为它仅仅构成了对磁盘文件的破坏，但却不具备激活和触发的基本条件，也就是说缺乏传染途径，因此它不是病毒，只能是一个破坏程序，当然不在计算机病毒防治范围。

对于第二种方案，可以及时发现病毒在内存中的存在，能及时发现病毒源，并防止病毒的传播。但由于病毒在触发前仅仅被包含在载体文件，虽然被激活进入内存，但还不可能被检测出来，就象许多计算机程序在待命状态下只是一个命令集，还无法判断其程序功能一样。它只能在触发之后，病毒在内存中被重新按装，使病毒处于随时可发作状态或直接对用户文件进行破坏并进行病毒传播，这时，可以从它的破坏和传播途经检测出来。可以把病毒触发之后对内存的影响分为下列两种情况：

1.病毒被按装到 DOS 系统的常驻内存区，使病毒处于随时可发作状态，这种情况病毒将在关机前一直存在。

2.病毒不在内存中重新安装，但作为传播的需要，它一定要把病毒插入到其它磁盘文件中去。这种情况下，病毒在内存中的生存期决定于载体文件在内存中的停留时间。

根据病毒特征（传播）我们对第一种情况分析可知，病毒侵入的 DOS 系统区域它定要具备可触发环境，而符合该条件的集中点只有二个，其一是系统中断向量表，其二是 DOS 内部命令表，因此，只要监测到系统向量表和 DOS 内部命令表的变化，就能判断病毒的侵入。当然，对于有些用户系统有意识的修改系统中断向量和 DOS 内部命令表，应该首先退出内存监测状态。特别是对于汉化操作系统，内存监测程序的加载应该是在其后，使系统进入完全稳定（即不再对系统向量和 DOS 内部命令表有修改要求）之后再加载。

对于第二种情况，由于病毒是随执行文件在内存中存在，但执行文件功能、特性各不相同，不可能有统一的检测方法。因此，只能通过其传播途径--向其它可执行文件扩散，来进行监测，该监视目标就是系统文件缓冲区中的文件修改标志。

因此，综上所述，我们设计内存实时监视的范围可以归纳为以下三类：

1.DOS 系统中断向量表

2.DOS 系统内部命令表

3.文件缓冲区中可执行文件的修改标志（可执行文件指 COM、EXE、SYS、OVL）

该监视程序的原理框图略，整个监视程序分为两个部分，其一是加载程序，可设计为外部命令形式，在计算机系统启动完成之后执行；其二是实时监视部分，可插入时钟中断（INT8 H）程序，实现定时监测。对系统中断向量和内部命令表监视的方法是，先建立一张系统中断向量（可全部也可部分）复制表和一张内部命令复制表，然后定时判断原表的改变情况。

比较上述两种方案，保护磁盘的方案比内存监测的方案更可靠，但实施比较困难。内存监测方案一般较易实施，因为不涉及到硬设置要求，但有可能监测到病毒的同时，磁盘也受到部分感染，因而要求内存监测程序应考虑到病毒传播途径的提示，以便及时恢复。

▲