硬盘加锁及病毒防治

徐炳亭 （国家教委高等工程教育培训中心）

对微机硬盘来说需防止别人未经许可的拷贝和调用，还要注意防止带病毒软盘对硬盘感染，这是用户最关心的两大安全问题。子目录与文件名及其内容加密、设置口令字等措施和防治病毒程序时见报刊介绍，这些方法都能提高计算机系统的安全性。本人受这些文章启发，编写了既能给硬盘加锁，又可防治硬盘引导型病毒的程序，适用于IBM系列及其兼容微机。下面从原理开始作一介绍。

1.硬盘结构及主引导扇区

硬盘容量大，而DOS一般只能管理32M以下的空间，同时也为了在同一硬盘上配置其他操作系统（如XENIX等），需要将一个硬盘划分为多个（≤4个）分区，但只能指定其中一个分区为活动分区，这项工作用FDISK命令进行。DOS操作系统可以占有两个这样的分区：一个主DOS分区（活动分区），一个扩展DOS分区。而扩展DOS分区可再划分为多个逻辑驱动器。因此，大容量硬盘除建立主DOS分区的C盘外，还须将扩展DOS分区分为D、E等逻辑驱动器。硬盘0柱面0磁头所辖的17个扇区独立于分区之外称为隐含扇区，其0柱面0磁头1扇区称为主引导扇区，存储启动计算机的主引导程序及硬盘四个分区的分配情况，其余16个扇区闲置。隐含扇区不能用PCTOOL和DOS命令读写，因此常常是引导型病毒最隐蔽的“根据地”。各分区开始的首扇区同软盘的0面0道1扇区一样，存储的是相应操作系统的引导程序，称为分区引导扇区。

主引导扇区空间布局如图所示。主引导程序和有关提示信息占用了近100H字节，其后直到01BDH间其字节内容全为0，这也是引导型病毒的“窝藏地”。01BEH后的40H字节为分区信息表，自举有效标志（AA55H）占该扇区的最后2字节。分区信息表中每个分区信息从xxxEH字节开始到xxxDH字节止，按以下格式存放：

00H:可引导指示符:

80＝活动分区(可引导)

00＝不可引导

01H～03H:分区起始地址

05H～07H:分区终止地址

08H～0BH:本分区前的扇数

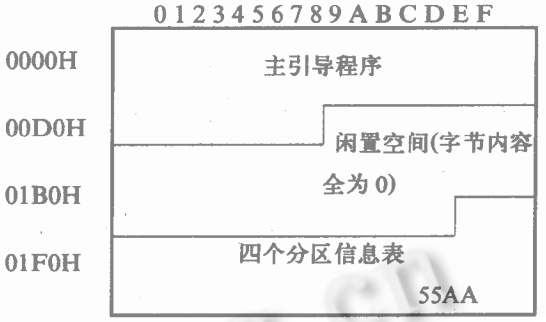
0CH～0FH:本分区所含扇数

04H:操作系统代码:

00＝未知,

01＝DOS系统(12位FAT表),

02＝XENIX系统，04＝DOS系统(16位FAT表),05＝逻辑盘，等。



分区信息表中信息的完整及自举有效标志是计算机启动成功的关键，否则即使用软盘启动计算机，硬盘也会“丢失”，这常常是硬盘故障所在，也是病毒攻击的对象。

由硬盘启动时，自举程序先将主引导扇区入内存0000:7C00H处，再由此主引导程序将其自身复制到内存0000:0600H处，接着用JMP 0000:061D语句在新区接续执行主引导程序。其后程序主要是在分区信息表中找引导指示符为80H的活动分区，根据活动分区表提供的信息将该分区引导扇区读入0000:7C00H处，再用JMP 0000:7C00H，把程序控制交给分区引导程序完成计算机的启动。

2.引导型病毒的预防

计算机病毒分为引导型病毒和文件型病毒，引导型病毒占硬盘隐含扇区和分区引导扇区；文件型病毒则改

换或破坏各分区的 FAT 表、文件目录和文件内容。有些病毒对所感染过硬盘和文件加感染标志，病毒依此标志为依据不再继续迭加此类病毒。最近出现的“新世纪”(New Century)病毒是一种既感染硬盘隐含扇区，又感染文件的混合型病毒，这种病毒是在主引导扇区 00EBH 偏移处写入 0519H 病毒感染标志字。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；文件型病毒一般在调用带毒文件时才进入内存，所以引导型病毒有更多传播机会。如前所述，隐含扇区主要是主引导扇区的内容，而其中部分区间和其余扇区又都是 0 字节，使检查和消除主引导型病毒变得很容易，这就是事先将干净无毒的主引导扇区进行备份(存入软盘或打印)，当发现隐含扇区上的内容有变或可疑时，对照备份修改或拷贝覆盖即可消毒。但隐含扇区独立于 DOS 分区，只能用 DEBUG 调试软件调用 BIOS 的 13H 中断功能进行读写。具体操作过程如下(划线部分为键盘输入内容，其他为屏幕的自动显示，右部为本文对汇编命令的注释)：

```
C>A:GEBUG                    从A盘调入DEBUG.COM
-A100                        编写(A)汇编程序
XXXX:0100 MOV DX,0080        将硬盘(80)从0柱面
XXXX:0103 MOV CX,0001        0磁头1扇区开始的
XXXX:0106 MOV AX,0211        17(11H)个扇区读(02)
XXXX:0109 MOV BX,0200        到内存XXXX:0200H处
XXXX:010C INT 13             BIOS磁盘I/O中断(13H)
XXXX:010E INT 3              BIOS断点中断(3H)
XXXX:0110                    按回车结束编程
-G                           执行(G)100H-10EH间的程序
    (屏幕显示略)
-D 200 L 2200 浏览(D)读入同存的隐含扇区的数据
    (屏幕显示略。此时可以按 Ctrl+P 键，同时打印下来)
```

观察数据内容，当没有病毒时，可用以下命令将程序和主引导扇区备份下来：

```
-N B:BOOT                    建立(N):B:BOOT文件
-R CX                        修改(R)CX寄存器的值(文件长度)
300                          为300H
-W                           写入(W)B:BOOT文件(从内存XXXX:0100始)
Writing 0300 bytes           (屏幕显示写入文件中的字节数)
-Q                           退出(Q)DEBUG
```

隐含扇区中除主引导扇区的其他扇区因所有字节均为 0，可不用备份。当内容非如前所述时，0 字节非 0，主引导程序和分区信息表与无毒的备份内容不一致时，硬盘已被病毒感染。最简单的办法是用无毒引导软盘启动计算机，再调用 DEBUG 将备份的无毒 BOOT 文件调入内存，将数据重新写回硬盘隐含扇区，操作如下：

```
C>A:DEBUG B:BOOT      调DEBUG并读入:B:BOOT文件
-F 300 L 2000 0       清(F)内存xxxx:0300H后的2000H为0
-A106
-XXXX:106 MOV AX,0311 将原程序的读(02)改为写(03)
-XXXX:109
-G                    运行(G)程序重新写入硬盘隐含扇区
-Q
```

硬盘分区和文件中病毒的清除，本文内容不另赘述。

3.硬盘加锁原理及加锁程序

防治病毒最重要的就是不使用带毒的软盘，特别要注意防止未经授权的人使用计算机，既防止非法拷贝和调用文件，也防止对方的软盘有可能携带病毒。最简便的办法就是用程序给硬盘加锁。加锁程序包括安装程序和主程序，运行安装程序，将主程序加在主引导扇区 OODAH-01B7H 间，改 0018H 处远跳转为 JMP0000:06DA 以便微机启动时让加锁主程序先夺得控制权，将各分区操作系统代码移到 01BAH-01BDH 处保存，并在 01B8H 处设加锁标志字，以防止多次加锁将操作系统代码丢失。此后再启动计算机时，加锁主程序则抢先运行，此时，操作者必须根据屏幕的汉语拼音提示，分别正确回答使用主 DOS 分区(C 盘)和扩展 DOS 分区(D、E 盘等)的口令，才能将操作系统代码转移到原位，再用 JMP 0000:061D 接续运行原主引导程序；否则即使用软盘启动计算机也不能享用硬盘。

本程序设置的口令：C 盘为 abc，D 盘为 DCBA，对照程序读者，不难修改成自己喜欢的口令。初次加锁之后，不再用此程序加锁。只要在工作结束时，再次启动一下计算机，故意不回答口令或答错口令，然后关机即能重新加锁。如果微机工作后忘记加锁，只要非法用户用硬盘启动计算机，也就自动进行了加锁。建议用户将重要数据和程序放在 D 盘或 E 盘，因为根据本程序和口令设置，启用 D、E 盘比 C 盘更困难。当用户必须使用 D 盘时，再准确回答 D 盘口令启用 D 盘，以保护 D 盘的文件免受病毒感染和被非法调用或拷贝。

有兴趣者如果需要调试好的程序，可以与本人联系(300072 天津大学校内 19 斋)，还可以得到键盘与屏幕加锁以及屏幕多种显示模式的图形存盘与打印等程序。