

硬盘 DOS 分区引导记录的分析及加密

山西长治市人民银行 彭起顺

微机硬盘是用户经常使用的一种外部存储设备,也是计算机病毒赖以生存的温床,目前,由于各种计算机病毒猖狂流行,恶性发作,对硬盘如何进行保护?则成了人们非常关心的问题。

在硬盘的 DOS 分区上有一个引导记录,它是用来负责加载 DOS 系统的。它存在于硬盘的逻辑 0 扇区,由于其具有先入性,所以,一些病毒程序的制造者就盯住了 DOS 操作系统的这一薄弱环节而大作其文章。例如,目前流行甚广的小球病毒就隐藏在此。从分析上看, DOS 分区引导记录大致可分为三部分,第一部分为 BIOS 参数块 BPB,其长度是从 00H 到 2CH(指偏移地址,下同);第二部分为引导记录程序主体,长度从 2EH 到 7DH;第三部分为错误提示信息,其长度是从 80H 到 FFH,读者可利用本文所给出的偏移地址值,使用 DEBUG 的“LI00 201”命令将 DOS 分区引导记录调入内存后,即可以用有关命令查看其内容,下面给出其操作步骤,所查看的内容因其太长故略去,只要读者按以下步骤,即可看到其内容:

```
C> DEBUG      ;运行DEBUG程序
-L100 201     ;将引导记录调入内存
-D100 12C     ;显示BPB
-U12E 27D    ;反汇编引导记录程序
-D280        ;显示错误提示信息
```

读者可将以上所显示的内容打印出来,对其进行详细的分析,将受益非浅。

由于其第二部分为引导程序清单,第三部分为错误提示信息,故读者在打出其内容后可对其自行分析,这里不再赘述。本文只是着重分析一下 DOS 引导记录的第一部分,即 BPB: 00H(3)(注:这里 00H 表示偏移地址为 16 进制的 0, (3)表示其是从偏移地址 0 开始后 3 个字节长度的单元,下同)内是一个无条件转移语句,以绕开 BIOS 参数块,其转移地址为 DOS 分区引导记录程序主体的入口。这是一个浮动地址,在用以上形式的 DEBUG 程序的操作下,其为“JMP 012E”,即 DOS 分

区引导记录程序主体是在偏移地址 12EH 处。注意,若病毒入侵,该地址将变为 11EH(从笔者所接触到的有关病毒程序来看,均是将该入口改为 11EH,特别是小球病毒)。03H(8)为机器属主名和引导程序版本号,如 IBM PC/XT 为“IBM 2.0”,GW0520CH 为“GW 2.0”等,DBH(2)为每个扇区的字节数,对于 DOS 2.0(以下给出的数据均是指 DOS 2.0),每扇区字节数为 512 字节,即为 200H 字节,0DH(1)为每族扇区数,其内容为 10H.0EH(2)是保留扇区数(从 0 扇区开始),为一个扇区,即 01H.10H(91)为 FAT 的个数,为 2 个 FAT,即 02H.11H(2)是根目录项的个数,为 04H.13H(2)为扇区总数(含引导扇区及根目录等),为 F96H,这是把整个硬盘都分配给 DOS 分区的情况(本例是在 GW0520CH-11 机所得出的数据,其硬盘为 30M,其它情况与此数据不符,下同)。15H(1)为介质说明符,内容是 F8H.16H(2)J 是每个 FAT 所占扇区数,内容是 0CH.18H(2)为每道的扇区数,内容为 1AH.1AH(2)为磁头个数,04H.1CH(2)为隐藏扇区数,内容为 01H.1EH(2)存放计算的驱动器号和磁头号.20H(1)为 IBMIO.COM 文件所占的扇区数,内容为 0AH.21H(11)为对磁盘操作的参数组.2CH(2)存放有一个 INT 19H 类中断,其功能是重新引导系统。

以上就是 BPB 的内容及地址划分,了解这些内容,将对用户的开发工作具有极大的帮助。如何利用这些来为我们进行 DOS 的二次开发所用,读者可在实际中逐步摸索。

从以上分析看出,从偏移地址 00H 到 0AH 之间,除前三个字节用于无条件转移指令外,剩下的为机器属主名和版本号。正常情况下,BPB 的其它内容是不允许更改的,否则将引起系统的混乱,而机器的属主名和版本号则是可更改的,这就展示出一个十分有趣也是十分有用的问题,即能否在 DOS 分区引导记录中嵌入一段程

序以对硬盘进行封锁,当机器从硬盘启动时,系统将不象通常那样直接去引导系统,而是要求操作者回答相应的保密字,回答正确,将正常引导系统,否则予以拒绝,答案是肯定的,我们完全可以利用这一段空间将加锁程序嵌入到 DOS 分区引导记录内以得到所期望的要求。可以用如下的设计思想来进行设计:在偏移地址 00H 到 0AH 这段区域内,将无条件转移指令后置,用加锁程序前缀到该转移命令之前,这样,当 DOS 分区引导记录进入内存后,第一条执行的指令将不再是以前的无条件转移指令,而是加锁程序的第一条指令,当口令正确后,再由加锁程序把控制权由后置的无条件转移指令交给 DOS 分区引导记录。另外,由于该段区域十分有限,不能也不可能去编制一个有一定长度的加锁程序。为此,口令的设置只能为单字,但单字口令很容易被人破译,故利用键盘上的特殊键组合可以做的恰如其分,具体做法如下:

```
C> DEBUG ;运行DEBUG程序
-L100 2 0 1 ;读入DOS分区引导记录
-A100 ;从偏移地址0H处嵌入加锁程序
```

```
××××:0100 MOV AH,02 ;调用16H类中断的2号功能
××××:0102 INT 16 ;
××××:0104 CMP AL,04 ;是否按下<Ctrl>+<Shift>键
××××:0106 JNZ 100 ;否,转100H处重新执行
××××:0108 JMP I2E ;是,加控制权交引导记录
××××:010A NOP ;加一空操作,避免混乱
××××:010B ℄ ;
-W100 2 0 1 ;存盘
-Q
```

以上加锁程序是通过调用 16H 类中断的 2 号功能来读取特殊键盘状态,当系统启动时,只有 <Ctrl>和 <Shift> 键同时按下(即 AL = 04),系统才能正常启动,否则,系统将始终循环检测键盘输入而无法开工。

这些特殊键的组合有多种方式,用户当然可以选择其一,下面是这些键的组合数据,供读者参考:

bit0	bit1	bit2	bit3	bit4	bit5	bit6	bit7
01H	02H	04H	08H	10H	20H	40H	80H
RIGHT SHIF	LEFT SHIF	CTL SHIF	ALT SHIF	SCROLL STATE	NUM STATE	CAPS STATE	INS STATE