硬盘分区的显示与隐藏*

邵洪成
(盐城工学院 计算中心,江苏 盐城　224003)

摘　要:由于病毒或计算机操作人员的误操作,安装的软件与数据很容易遭到破坏。采用修改 Windows 中的注册表和修改分区表中的系统标志两种方法,将重要的分区隐藏起来,使操作者无法访问该分区,从而达到保护软件与数据的安全。

关键词:分区;显示;隐藏;Windows;注册表
中图分类号:TP316　　文献标识码:A　　文章编号:1671 - 5322(2002)04 - 0056 - 03

随着计算机的普及,越来越多的人使用计算机来工作、学习、娱乐等,由于病毒与操作者的误操作,很容易破坏计算机硬盘中的软件与数据,严重的会导致计算机不能正常工作,由此可见硬盘中的软件与数据的安全性显得非常重要。如何有效的保护安装的软件及其数据的安全性呢?一是备份软件与数据;二是安装硬件保护卡,笔者现介绍另一种较为有效的方式:隐藏分区。

通常可将硬盘分成若干个分区,如至少 3 个分区(C、D、E)。C 分区安装所有需要使用的软件,D 分区供用户存入数据,E 分区作为软件备份分区。比如用 GHOST 等软件将 C 分区的软件生成镜像文件,放在 E 分区,这样一旦 C 分区遭到破坏,可以通过 E 分区的镜像文件还原 C 分区(具体操作方法可参考有关 GHOST 使用手册)。如果 E 分区也遭破坏,则镜像的意义就不大了。笔者认为隐藏 E 分区是一个比较有效的方法。

下面介绍两种方式来隐藏 E 分区。

1　通过修改 Windows 中的注册表来隐藏 E 分区

大家都知道,在 Windows 中访问某一个驱动器是通过"我的电脑"或"资源管理器"来实现的。如果在"我的电脑"或"资源管理器"中隐藏了该驱动器的图标,一般用户就无法访问该驱动器了。隐藏驱动器只需在注册表[1]中打开 HKEY - CURRENT - USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer 分支,在此分支下新建一个 NoDrives 的二进制键值名,NoDrives 键值为 4 个字节。每个字节的每一位就对应于一个盘符(A ~ Z),即第一个字节(每一个字节用八位二进制表示)代表了从 A 到 H 的八个驱动器,即 01(十六进制,下同)表示 A 驱动器,其对应的二进制为 0000 0001、02 表示 B 驱动器,其对应的二进制为0000 0010、04 表示 C 分区,其对应的二进制为0000 0100、08 表示 D 分区,其对应的二进制为0000 1000、10 表示 E 分区,其对应的二进制为 0001 0000、20 表示 F 分区,其对应的二进制为0010 0000、40 表示 G 分区,其对应的二进制为 0100 0000、80 表示 H 分区,其对应的二进制为 1000 0000。依此类推,第二个字节代表 I 到 P;第三个字节代表 Q 到 X;第四个字节代表 Y 和 Z。下面介绍具体的隐藏分区的操作方法。

先启动注册表编辑器,用鼠标单击"开始"按钮,打开"开始"菜单,单击开始菜单里的"运行",在"运行"对话框中输入 REGEDIT,单击"确定"按钮,打开注册表编辑器窗口[2],如图 1 所示。

然后进入 HKEY-CURRENT-USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer 分支中,在右窗口中新建一个二进制值的键值名"NoDrives"(其操作步骤如下:编辑→新建→二进制值,出现"新值 #1"临时名,输入 NoDrives,再按回车键即可),它对应的键值为

* 收稿日期:2002 - 05 - 11

作者简介:邵洪成(1968-),男,江苏盐城人,盐城工学院讲师。

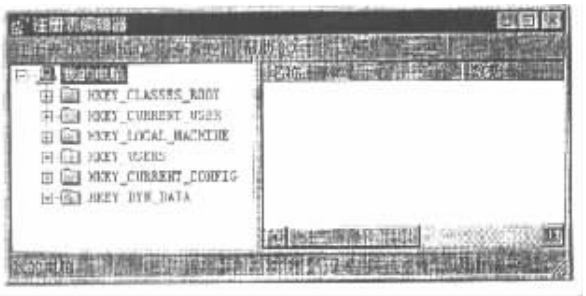

图 1　注册表编辑器窗口

Fig. 1　Editor window of register table

“10000000”(其操作步骤如下:在右窗口中双击“NoDives”,打开编辑二进制值对话框,在该对话框中输入 10000000,单击确定按钮即可,注意 10000000 是十六进制,表示 4 个字节,其中第一个字节 10 表示 E 盘),如图 2 所示。然后关闭注册表编辑器,重新启动计算机后,打开‘我的电脑’或“资源管理器”,会发现 E 盘的图标就看不到了。用这种方法可以隐藏硬盘的盘符,以此用来保护文件资源。另外,同样使用这个方法可以同时隐藏若干个驱动器的图标,如:当它的键值为“05000000”时,可隐藏 A 盘和 C 盘;其中“05000000”的值就是‘01000000”A 盘与‘04000000”C 盘相加得来的,又如‘09000000’可隐藏 A 盘与 D 盘。“11000000’可隐藏 A 盘与 E 盘。将所要隐藏的磁盘驱动器所对应的键值按十六进制相加赋值给‘NoDrives”,这样,就可以在‘我的电脑’或‘资源管理器’内隐藏起所要隐藏的驱动器。又如要隐藏 A 盘、C 盘与 D 盘,则将“0D000000”赋值给“NoDrives”。如果要访问已经隐藏的盘,可以在注册表编辑器[3]上述分支的右窗口中删除二进制键值名‘NoDrives”,关闭注册表编辑器,重新启动计算机即可,当然还有更简便的方法,这里就不作介绍了。

2　通过修改分区表中的系统标志来隐藏 E 分区

硬盘分区表中每个分区用 16 个字节来表示,其中第 5 个字节就是分区表中的系统标志,系统标志 01H 表示基本 DOS 分区,FAT 表项为 12 位,04H 表示基本 DOS 分区,FAT 表项为 16 位,06H 表示基本 DOS 分区容量大于 32M,0B 表示基本 DOS 分区,FAT 表项为 32 位,05H 或 0FH 表示扩展 DOS 分区,FFH 表示非 DOS 分区(Table)等,即将要隐藏的 DOS 分区改为非 DOS 分区,从而达到隐藏分区的目的。那么,如何查找和修改硬盘分区表呢?这可以用调试程序 DEBUG,具体操作如下(最好用系统软盘启动):

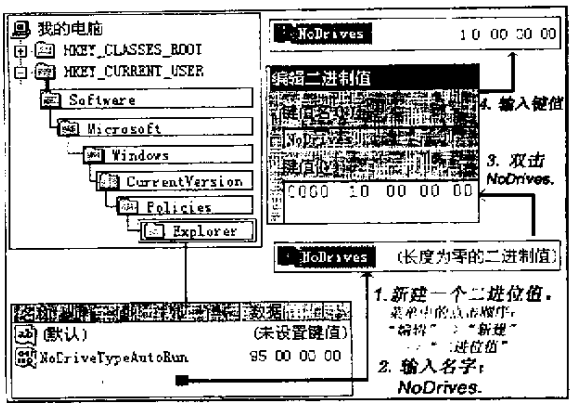

图 2　编辑相应键值

Fig. 2　Edit corresponding key assignments

在 DOS 方式下,键入 DEBUG

- A100
- MOV DX,0080
- MOV CX,0001
- MOV BX,0200
- MOV AX,0201
- INT 13
- INT 20
- ^C
- G = 100
- D380

通过上述操作,读出硬盘的分区表,主要数据如下:

80 01 01 00 0B EF BF A5 3F 00 00 00 21 6C 9C 00

00 00 81 A6 0F EF BF 5E 60 6C 9C 00 90 1E C8 01

其中第一行信息为基本 DOS 分区信息,第二行信息为扩展 DOS 分区信息,各字节的含义如下:

第 1 字节 80 为活动分区指示(可以引导操作系统),

00 为非活动分区指示(不可以引导操作系统);

第 2 至 4 字节为分区起始地址;

第 5 字节为系统标志(上述分区表中加下划线的数据);

第 6 至 8 字节为分区终止地址;

第 9 至 12 字节为相对扇区数;

第 13 至 16 字节为分区大小。

如果用 DEGUG 中的 E 命令修改扩展 DOS 分区的系统标志 0F(或 05)为非 DOS 分区的系统标志 FF,然后用 E 命令修改 AH 中的 02 为 03,即将上述程序代码中的相应行 MOV AX,0201 改为 MOV AX,0301,然后再用 G = 100 执行这个程序,就能将修改后的结果写回硬盘,重新启动计算机,扩展分区就全部隐藏起来了,而且不可访问。如果只想隐藏 E 分区,不隐藏 D 分区,那么可将上述代码段中的相应行 MOV CX,0001 改为 MOV CX A681,然后再用 G = 100 执行这个程序,再次读出如下数据:

00 01 81 A6 0B EF 7F 4B 3F 00 00 00 21 6C 9C 00

00 00 41 4C 05 EF BF 5E 60 6C 9C 00 30 B2 2B 01

用同样的方法再将 DOS 分区的系统标志 05(或 0F)改为非 DOS 分区的系统标志 FF,再将结果写回硬盘,重新启动计算机,D 分区可以正常访问,而 E 分区不能正常访问,也就是 E 分区被隐藏了。如果要访问隐藏的分区,只需将分区表中相应的系统标志由 FF 再改为相应的 05(或 0F)即可。

3 结语

以上两种方法都能很好的隐藏镜像文件分区,使得操作者无法访问隐藏的分区,从而达到保护相应分区上镜像文件的安全性,一旦 C 分区上的软件遭到破坏,很容易通过隐藏分区上的镜像文件来还原 C 分区。

参考文献:

[1] Peter Norton. 中文 Windows98 管理手册[M]. 北京 机械工业出版社,1999.
[2] 刘加明. 学习使用中文 Windows95[M]. 北京 :人民邮电出版社,1997.
[3] Richard Mansfield. Windows95 使用大全[M]. 北京 机械工业出版社,1997.

How to Show and Hide partition of Hard Disk

SHAO Hong-cheng
(Computer Center of Yancheng Institute of Technology, Jiangsu Yancheng 224003, China)

Abstract: The installed software and data are easily damaged because of virus or operators' mistakes. This paper uses the register table in the windows and systematic symbol in the partition table to hide the important so that the operators will fail to visit this partition to prefect the software and data.

Keywords: partition; show; hide; windows; register table

(上接第 18 页)

The Design of Virtual Function Generator with Labview

PANG Wei-zi
(Department of Electrical Engineering of Yancheng Institute of Technology, Jiangsu Yancheng 224003, China)

Abstract: In this paper, the basic principle and the design method of a virtual function generator is introduced, which is developed using the graph programming language "LabVIEW". The function of this function generator and process of development are detailed.

Keywords: Virtual Instrument; Function Generator; Graphical Programming; LabVIEW