逻辑 C 盘防写保护与预防病毒

徐炳亭　（天津大学职业技术教育学院　300072）
刘卓慧　（中国轻工业新技术开发中心　100020）

摘要：本文介绍了对逻辑 C 盘加防写保护以预防病毒的原理，并在文后给出了实用程序。
关键词：硬盘　防写保护　病毒

软盘贴上防写保护签就可以防止对软盘重写，这样就可以防止病毒对软盘所存软件的感染。硬盘能否也象软盘那样加防写保护呢？这样对防止硬盘上系统软件和工具软件感染病毒也是非常有意义的。本文所提供的程序就可以对逻辑 C 盘加防写保护，它就象软盘贴上写保护签一样，盘上的系统程序、应用程序和数据文件均可以读出调用，而当需要向盘上写入内容时，必须先解除防写保护，才能进行写操作，写操作结束后还可以再重新加防写保护。为防止未经授权的人使用计算机，可以再配以硬盘加锁程序，用户必须回答口令解锁才能启动计算机。两种方法互相配合，预防病毒效果更为理想。

系统软件和各种语言及应用软件，最怕病毒对这些软件的可执行文件（.COM 和 .EXE 等）的感染，但大多数的病毒偏偏是感染这些文件。不要说是一般用户，就是对高级用户来说，清除病毒也是一件很头痛的事，至少要化费许多时间去处理，更何况病毒的种类不同，其病毒的特征和表现形式也不同，使清除病毒工作没有一个通用的方法，一般清除病毒的软件也只是能清除已知病毒，而对新出现的病毒则束手无策。因此，对付病毒最好的办法就是加强对病毒的预防，而预防病毒最得力的措施就是对磁盘加防写保护处理。就象软盘贴防写保护签一样，防写并不是不能写或不能修改。一般用户可随时调用存在逻辑 C 盘中的系统软件和各种应用软件（如：DOS、WPS、PCTools、Foxbase＋、C 等），在软驱（A 盘或 B 盘）或逻辑 D 盘上，采用 ASCII 码编写程序或数据文件，病毒一般不会感染这些文件，即使感染上病毒也好清除，而具有源程序的编译程序（.COM 或 .EXE 文件）即使感染了病毒，重新编译也不甚困难；而当需要向逻辑 C 盘拷贝新的应用软件或编译好的程序时，应该对源程序及其磁盘和内存先进行病毒检查，确认无病毒后再解除逻辑 C 盘的防写保护，进行拷贝或修改工作，并且在完成拷贝或修改之后，马上再加上防写保护。下面对照文后所附的源程序，对该程序原理稍作介绍。

大容量硬盘

区情况存储在硬盘 0 柱面 0 磁头首扇区(即主引导扇区)偏移为 01BEH 的分区信息表中，逻辑 C 盘在硬盘上的起止地址分别存在偏移 01BFH～01C1H 和 01C3H～01C5H 处，各占 3 个字节。其中首字节存磁头号，第二字节低 6 位存扇区号，第三字节存柱面号，而柱面号高位存在第二字节的高 2 位中。分区或逻辑盘大小及分界一般都是以柱面号来计算的，因此我们关心的是逻辑 C 盘的终止柱面号，本程序对逻辑 C 盘防写的原理就是当对硬盘进行写操作时，先判断所写的柱面号是否在逻辑 C 盘内，若是则拒绝写盘，否则就可以写盘。由于主引导扇位于逻辑 C 盘起始柱面低方，对逻辑 C 盘防写保护，实际上主引导区也有了防写保护，这就兼而对两者都起到预防病毒的作用。

系统的磁盘操作都是通过 INT13H 中断进行的，INT13H 中断中只有 3 号(写盘)、5 号(格式化)、B 号(写长扇区)功能与写盘操作有关，因此将本程序驻留内存，设法截获 INT13H 中断对逻辑 C 盘的这些操作，并拒绝执行；当然 INT13H 的其他操作应该按原 INT13H 中断继续无误的进行。此外本程序设计不但考虑可以随时加防写保护，也考虑能够随时解除防写保护，于是扩展了原 INT13H 的 0 号(复位)功能，可以根据相应信息将程序走向开关或指向防写保护处理，或直接返回原 INT13H 中断处理。

本程序由安装驻留和防写保护两部分程序组成。其安装驻留部分还使用了防止重复安装的技巧，即在防写保护部分预置安装标志(0FFH)，根据是否返回该标志字再决定是否安装。安装时将硬盘主引导区读入，求出逻辑 C 盘的终止柱面号，连同系统的原 INT13H 中断向量读出都存入防写保护程序中，用防写保护程序在内存的地址向量置换系统的原 INT13H 中断向量，然后驻留防写保护程序退出。

本程序采用汇编语言编译成 .COM 文件，具体编译过程如下：

```
C>MASM CPFH
C>LINK CPFH
C>EXE2COM CPFH.EXE CPFH.COM
```

该程序置于 C 盘根目录中，对逻辑 C 盘加防写保护或重置防写保护时，直接运行本程序即可，即：

```
C>CPFH
```

若解除防写保护，则需加参数/W 运行，即：

```
C>CPFH /W 。
```

即使未预先安装防写保护程序，带参数/W 运行也可进行安装，并同时解除防写保护。

对照源程序用户不难修改、变换为别的参数，以加强解除防写保护的保密性。

该程序最好放在 AUTOEXEC.BAT 文件中执行，同时，也为了利用好逻辑 C 盘中的系统软件和各种应用软件，建议在 AUTOEXEC.BAT 文件中使用 DOS 的路径设置命令 PATH(内部命令)和 APPEND.COM (DOS3.3 以上版本新增加的外部命令，该命令文件必须存在 PATH 指出的某一目录中)，即：

```
C>TYPE AUTOEXEC.BAT
......
PATH C:\;C:\DOS;C:\WPS;C:\GJX;.....<路径名表>
APPEND C:\;C:\DOS;C:\WPS;C:\GJX;.....<路径名表>
CPFH
......
```

这样微机系统启动之后，便可以在任何盘符的任何目录下自由使用逻辑 C 盘上的各种软件了。

参考文献

[1] 刘尊全，计算机病毒防范与信息对抗技术，清华大学出版社，1991

[2] 徐炳亭，硬盘加锁及病毒防治，计算机世界月刊，1994.3