 平时使用电脑的时候，有时会遇到这样的情况，用鼠标双击磁盘分区图标时，往往无法打开对应分区窗口。比如说，打开D盘时，提示找不到路径或者直接链接到其他地方去了。遭遇类似上述现象时，那几乎就能断定此计算机系统已经感染了一直非常猖獗的闪盘病毒，这种病毒一般通过“ Autorun.inf ”文件进行传播，只要我们双击闪盘分区图标时，该病毒就会通过“ Autorun.inf ”文件中的设置来自动激活病毒，然后将“ Autorun.inf ”文件同时拷贝到其他分区，导致其他分区都无法用双击鼠标的方法打开。下面就和大家一起分享一下解决这类病毒方法。 删除“ Autorun.inf ”文件 当计算机系统感染了“ Autorun.inf ”文件病毒时，该病毒就会自动在本地硬盘的所有分区根目录下面创建一个“ Autorun.inf ”文件，该文件在默认状态下具有隐藏属性，用普通方法是无法直接将它删除掉的。要想删除“ Autorun.inf ”病毒文件，我们可以按照如下方法来操作： 首先用鼠标双击系统桌面中的“ 我的电脑 ”图标，在其后弹出的窗口中依次执行“ 工具 ”/“ 文件夹选项 ”菜单命令，打开文件夹选项设置窗口，单击该窗口中的“ 查看 ”标签，并在对应标签页面中选中“ 显示所有文件和文件夹 ”项目，同时将“ 隐藏受保护的操作系统文件 ”的选中状态取消掉，再单击“ 确定 ”按钮，这么一来“ Autorun.inf ”病毒文件就会显示在各个分区根目录窗口中了；其次用鼠标右键单击“ 我的电脑 ”窗口中的某个磁盘分

区图标，从弹出的快捷菜单中执行“ 打开 ”命令，进入到该分区的根目录窗口，在其中我们就能看到“ Autorun.inf ”病毒文件的“ 身影 ”了；再用鼠标右键单击“ Autorun.inf ”文件，并执行右键菜单中的“ 打开 ”命令将“ Autorun.inf ”文件打开，随后我们就会看到里面的“ open=xxx.exe ”内容，其实“ xxx.exe ”就是具体的病毒名称。倘若这类病毒没有进程保护时，我们只需要将“ xxx.exe ”文件以及各个“ Autorun.inf ”文件直接删除掉，就能将闪盘病毒从系统中清除掉了；下面为了防止病毒再次运行发作，我们还需要将遭受病毒破坏的磁盘关联修改过来。在修改磁盘关联时，必须先依次单击“ 开始 ”/“ 运行 ”命令，打开系统运行对话框，在其中执行注册表编辑命令“ regedit ”，打开本地系统的注册表编辑窗口.在该编辑窗口的左侧显示区域，先用鼠标展开“ HKEY_CLASSES_ROOT ”注册表分支，然后在该分支下面依次选择“ Drive\shell ”项目，在对应“ shell ”项目的右侧列表区域，用鼠标双击“ 默认 ”键值，在其后弹出的数值设置窗口中将“ 默认 ”键值数值修改为“ none ”；接下来再用鼠标展开“ HKEY_CURRENT_USER ”注册表分支，然后在该分支下面依次选择“ Software\Microsoft\Windows\CurrentVersion\Explorer ”项目，在对应“ Explorer ”项目的右侧列表区域，检查一下是否存在一个名为“ ountPoints2 ”键值，一旦发现该键值的话，我们必须及时将它删除掉，最后按一下键盘上的F5功能键，来刷新系统注册表的设置，这么一来闪盘病毒就被我们手工清除掉了，此时当我们再尝试用双击方法打开分区窗口时，就会看到对应分区窗口能被正常打开了。彻底遏制闪盘病毒 倘

若我们的计算机不小心中了闪盘病毒的黑手，尝试使用上面的方法无法删除“ Autorun.inf ”文件，而且重新安装了计算机系统后仍然无法使用双击鼠标方法打开分区窗口时，我们可以选用一款名为“ 费尔木马强力清除助手 ”的工具，来让本地系统摆脱闪盘病毒的“ 干扰 ”，并且有效抑制该类型病毒的继续发作。下面就是抑制闪盘病毒再生的具体操作步骤：首先从网上将“ 费尔木马强力清除助手 ”工具下载到本地硬盘中，并对它进行正确安装.安装完毕后，直接运行“ 费尔木马强力清除助手 ”程序，在其后弹出的程序界面中选中“ 抑制文件再次生成 ”项目，同时在“ 文件名 ”文本框中输入“ Autorun.inf ”文件的具体路径信息，例如笔者在这里输入“ C:\Autorun.inf ”，再单击“ 清除 ”按钮，这么一来C分区下面的“ Autorun.inf ”文件就被清除干净了；按照相同的操作方法，再将其他分区中的“ Autorun.inf ”文件删除干净。 接着我们再按常规方法重新安装一下操作系统，或者直接通过Ghost程序来快速恢复一下系统，相信这么一来重装过后的系统就会摆脱闪盘病毒的侵扰了。 预防闪盘病毒再次袭击 为了防止闪盘病毒再次袭击我们，我们必须采取有效措施，让本地系统远离闪盘病毒。而要预防闪盘病毒再次袭击的方法非常简单，我们只需要在闪盘根目录下面手工创建一个“ Autorun.inf ”文件，这样一来闪盘病毒日后就无法往闪盘根目录下面自动生成“ Autorun.inf ”病毒文件了，那样的话闪盘病毒就无法通过闪盘进行传播了。 另外关闭系统自动播放机制，也可以有效抗击闪盘病毒的入侵。 在“ 开始 ”→“ 运行 ”中输入“ gpedit.msc ”程序，在“ 组策略 ”窗口中展开“ 计算机配置 ”→“ 管理模版 ”→“ 系统 ”分支；在右侧窗

口双击“ 关闭自动播放 ”项，在打开的窗口中选择“ 已启用 ”项，在“ 关闭自动播放 ”列表中选择“ 所有驱动器 ”项，点击“ 确定 ”按钮，就可以禁用闪盘的自动播放功能了。当然，也可以在连接上闪盘后，按下Shift键，即可取消闪盘的自动播放功能。其实，更安全的办法是打开资源管理器，从“ 地址栏 ”中直接选择闪盘盘符，这样再狡猾的闪盘病毒也无法自动运行了。