电脑报 东方工作室

彭爱华 汤惠莉 编著

还魂PC术

PC HUANHUN SHU

- 死“机”能当活马医
  - 排除死机深层因素
  - 清除黑客病毒困扰
- 重要数据常“备”重要
  - GHOST数据备份还原天书
  - 驱动程序也备份
- 重装系统一条龙
  - PARTITION MAGIC无损坏分区天书
  - 多操作系统全新安装手册
  - 玩转虚拟机

重庆出版社

PC 还魂术

编　著：彭爱华　汤惠莉

重庆出版社

图书在版编目（CIP）数据

PC 还魂术 ／彭爱华，汤惠莉编著.—重庆：重庆出版社，2003
ISBN 7-5366-6045-6

I.P… Ⅱ.①彭…②汤… Ⅲ.窗口软件，Windows-基本知识 Ⅳ.TP316.7

中国版本图书馆 CIP 数据核字（2003）第 093681 号

编　　著：彭爱华 汤惠莉
责任编辑：谢　先 刘爱民

PC 还魂术

重庆出版社出版、发行
新华书店经销
重庆升光电力印务有限公司印刷

*

开本：787 × 1092　1/16　印张：18.5 字数：444 千
2003 年 1 月第 1 版　　2003 年 1 月第 1 次印刷
印数：1 ~ 5 000

*

ISBN 7-5366-6045-6/TP · 106
定价 25.00 元

前 言

给您的电脑穿上“铁布衫”

置身于信息化时代的你，是否会经常经历电脑死机、系统崩溃？确实Windows的脾气不大好，经常会板个“蓝脸”给你看，尤其是Windows 9X/Me，更是三天两头就会罢工。而且所有版本的Windows都有一个从娘胎里带出来的遗传病，就是使用时间长了，系统运行速度就会越来越慢。网上流传着这样一个笑话来夸张Windows速度之慢：鼠标单击某个Word文档，然后上街逛上两圈，等你回来时，这个Word文档才刚打开……

好了，已经够煽情了，那么应该如何解决这些问题呢？《PC还魂术》这本书正是为解决这个目的而诞生的。不管你用的是爷爷级的Windows 98，还是当红小生Windows XP，本书都能给你带来有益的启发。更值得一提的是，本书绝不仅仅局限于概念、理论的阐述，而是以实例为驱动，佐以大量的实景图片，手把手地教你实现每个操作。你是老鸟？也没关系，书中亦有很多可能你还没有见过的“猛料”，值得你去拥有它。

第1章：一旦发生系统崩溃，很多朋友会选择把当前系统“格杀勿论”（格式化重装），其实大多时候无需那么麻烦。本书的第1章将会给您分析系统故障的软、硬件原因以及解决方案。只有实在是“病入膏肓”的系统才需要进行祭起“系统重装”这个绝招。

第2章：笔者的一个朋友，由于不堪忍受Windows蜗牛般的速度，一气之下，没作任何准备工作就重装系统，结果发现显卡、声卡的驱动程序没有了。这下可好，游戏也玩不成了。本书的第2章将帮助你备份系统的重要数据，例如QQ聊天记录、邮件、应用程序设置等等，保证这些关键数据不会跟随老系统一起“殉葬”。

第3章：硬盘的分区和格式化一向是初级用户所头疼的事情，你知道Windows自带的磁盘工具也能实现有限的无损分区吗？你知道有个DOS程序可以让你5秒钟之内就可以格式化一个刚分区的硬盘吗（绝非DM之类的低格工具）？本书的第3章从最常用的FDISK、Partition Magic说起，介绍多种功能强劲的磁盘工具，让这些磁盘管理工具来个“华山论剑”！

第4～第6章：是本书的核心部分，讲述了主流操作系统、驱动程序、应用程序的安装及其注意事项，不管你是菜鸟还是老鸟，相信都能从中获取自己所需的重要信息。

第7章：一提到系统克隆，很多朋友会条件反射似的联想到GHOST，其实系统恢复工具绝非仅GHOST一家，PowerQuest DriveImage和“联想拯救者”都是GHOST的强敌。还有利用某些软件、或者硬件技术，几乎不费什么磁盘空间就能轻松恢复系统……

第8章：病毒、木马一直是系统的心腹大患，本书的第8章将告诉你如何对付这些讨厌的东西，让你的系统百毒不侵。

好了，就介绍到这里吧，想要了解更多的实际内容吗？想要摘掉自己头上的菜鸟帽子吗？想要让自己的计算机水平更上一层楼吗？那就把这本书“娶”进家门吧！

本书由彭爱华、汤惠莉夫妇编写，刘晓辉先生审校。由于著、校者的能力有限，书中难免有谬误和疏漏，恳请读者诸公能够批评指正。

作者：彭爱华 汤惠莉

2002年12月于上海

目 录

contents

第1章

系统瘫痪的原因分析与恢复方法

俗话说“自古机器谁无死”，相信绝大多数人和我一样，用的是Windows操作系统。Windows乃微软公司的旗舰产品，虽然是系统软件里的王者，但是不管是老一辈的Windows 3.X/9X，还是新一代的Windows 2000/XP，都有一个从娘胎里带出来的遗传病——不稳定。

1.1 导致系统瘫痪或运行不畅的原因

比起操作系统新贵Linux来，Windows虽然生得俊俏，但是“脾气”实在不好，说翻脸就翻脸，动辄就板个蓝脸给你看。造成系统瘫痪或运行不畅的原因很复杂，由于组成电脑的配件分别来自于不同的厂商，更何况上面还运行着那么多的程序（操作系统和应用程序），这么多组成部分稍有一个地方“头疼脑热”，整个电脑就要“发烧流鼻涕”。

既然整个电脑系统由硬件和软件组成，那么造成死机的原因也就分为软件原因和硬件原因。

1.1.1 软件故障及其原因

1. 弹尽粮绝——资源不足

资源不足是导致系统崩溃或运行不畅的重要原因，下面介绍如何利用不同的Windows平台所提供的工具来分析造成系统资源不足的原因，以便对症下药、更好地优化系统。

（1）症状

我们可能经常遇到下面这些叫人头痛的提示信息。Windows 9X系统中经常出现提示：“内存不足”、“General Fault Protection（一般保护性错误）”；而Windows XP则经常出现“XX程序遇到问题需要关闭，我们对此引起的不便表示抱歉”（见图1.1）。

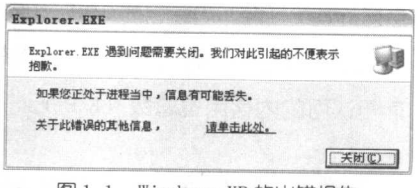

图1.1 Windows XP的出错报告

（2）诊断

如果你的爱机不是“家大业大”（Pentium 4+512MB 内存＋高速硬盘），而你又贪心不足，在桌面上打开了过多的窗口，那么系统很快就会由于虚拟内存告急而瘫痪，于是就会出现上面的情况。

也许有的朋友可能会说，我的机器可是超豪华级配置啊！怎么也会犯这些平头百姓才犯的错误呢？原因在于，JS（奸商）为了鼓动你掏腰包，会拼命吹嘘，说什么奔腾 4 电脑云云，其实，一台配置为“Pentium 4＋128M 内存＋5400 转／分的硬盘”的电脑，它的性能决不比配置为“Pentium Ⅲ＋256M 内存＋7200 转／分的硬盘”的电脑高。道理很简单，假设一个木桶由多块长短不一的木板组成，那么它的最大储水量不会由那块最长的木板决定，而取决于那块最短的木板，这就是“最小决定原则”。如果我们能够找出限制系统整体性能的瓶颈，那么就能够采取相应的措施，优化系统性能。

（3）分析工具

有两种查看系统资源使用情况的方法：定性分析和定量分析。通过定性分析，可以知道当前资源是否“吃紧”，甚至还能知道哪个进程霸占的资源多（在Windows2000/XP 下）；通过定量分析，你可以查出系统的瓶颈所在。

图1.2 任务管理器

▲定性分析

在Windows 2000/XP 下，可以用“任务管理器”来查看。具体的操作步骤如下：

第 1 步，用鼠标右键单击任务栏空白处，在快捷菜单中选择“任务管理器”，显示见图 1.2 所示“Windows 任务管理器”窗口。

第 2 步，选择“性能”选项卡（见图 1．3），动态显示当前的系统性能，内容包括 CPU 和内存使用情况的图表，计算机上正在运行的句柄、线程和进程的总数，物理内存、核心内存和认可的内存用量总数（KB）。

图1.3 任务管理器的“性能”选项

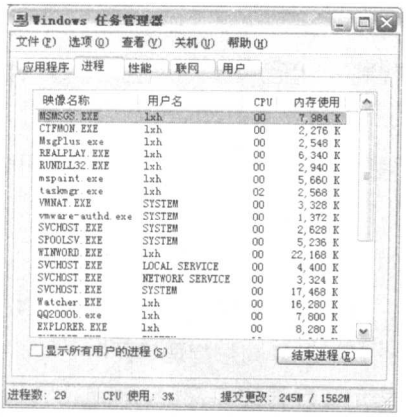

图1.4　查看“进程”

第3步，切换到“进程”选项卡（见图1.4），可查看单个系统进程的资源消耗情况。

第4步，在“查看”菜单选择“选择列”命令，打开“选择列”对话框（见图1.5），选中“虚拟内存大小”和“线程计数”复选框，然后单击“确定”按钮。

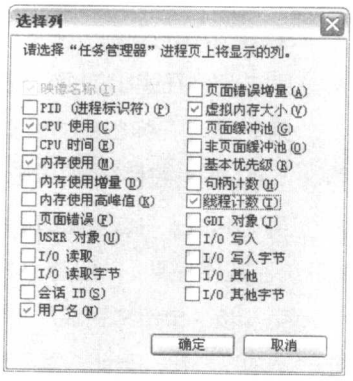

图1.5　“选项列”对话框

图1.6　查看各“进程”的情况

第5步，切换回“进程”选项卡（见图1.6），可以很清楚地看到每一个当前正在运行的进程所消耗的内存、虚拟内存，所占用的CPU时间以及当前运行的线程数。

在Windows 98下可以使用“资源状况”工具。尽管这个“武器”比起Windows XP的“任务管理器”来确实有点简陋，但也有一定的作用。具体操作步骤如下：

依次单击“开始”→“程序”→“附件”→“系统工具”→“资源状况”，资源状况实用程序就会启动并驻留内存，开始自动实时监测当前系统内部资源的使用情况。

“资源状况”对话框以百分比和进度条两种表示方法显示当前的资源使用情况。“资源状况”工具显示的资源包括“系统资源”、“用户资源”和“GDI资源”（见图1.7）。

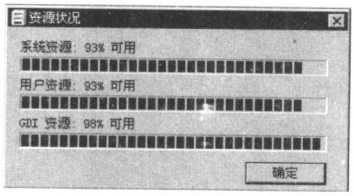

图1.7　查看资源状况

▲定量分析

仅靠定性分析这种表面功夫是诊断不出“腠理之疾”的。为了监视关键子系统，从而发现系统瓶颈、优化系统，就必须对系统进行“血检”，这里推荐一个专业工具——“性能”控制台（Windows 2000/XP自带）。这个“性能”控制台带有两个用来跟踪和监视系统性能工具——系统监视器、性能日志和警报。

有两种访问“性能”控制台的方法：第一种方法是鼠标单击“开始”→“管理工具”→“性能”菜单，即可打开“性能”控制台。第二种方法是构造一个自己的控制台，里面包含“系统监视器”、“性能日志和警报”两个工具。

下面，以Windows XP为例介绍定量分析步骤（还在使用“老枪”—Windows 98的朋友请稍安勿躁，后面会讲到）。

- 创建控制台。

第1步，选择“开始”→“运行”，在运行对话框里输入“MMC”，单击“确定”按钮。

第2步，在弹出的空“控制台”窗口上，选择“文件”→“添加/删除管理单元”。

第3步，在弹出的对话框里单击“添加”按钮，弹出“添加独立管理单元”对话框，选择“ActiveX控件”，再单击“添加”按钮。

第4步，在“插入ActiveX控件”对话框里，依照提示选择“System Monitor Control”（系统监视器控件），把它命名为“我的系统监视器”。

第5步，单击“完成”按钮回到“添加独立管理单元”对话框，选择“性能日志和警报”，单击“添加”按钮。至此，属于我们自己的系统性能控制台就构造好了，你可以把它保存起来（文件名为“我的控制台.msc”），今后就可以从“管理工具”里访问它了。

- 配置控制台。

第1步，从“管理工具”里打开“我的控制台.msc”，显示“我的系统监视器”主窗口。首次打开系统监视器时，我们必须对它进行配置（增加计数器），让它对系统活动进行跟踪。

第2步，单击“我的系统监视器”工具栏上的“添加”按钮，打开见图1.8所示的“添加计数器”对话框。然后我们就可以选择要监视的性能对象了。可能造成系统瓶颈的不外乎是Processor（处理器）、Memory（内存）、PhysicalDisk（硬盘子系统）。

对于处理器，我们要监视它的%Processor Time（测试CPU响应系统请求所用的时间百分比）、Interrupt/Sec（每秒钟CPU收到的硬件中断数）。如果要增加一个Processor>%Processor Time计数器，只须在图1.8所示对话框的“性能对象”下拉列表框里选择“Processor”，然后单击“从下拉列表里选择计数器”单选按钮，选择“%Processor Time”，再单击“添加”按钮即可。其他计数器的添加方法与此相同。

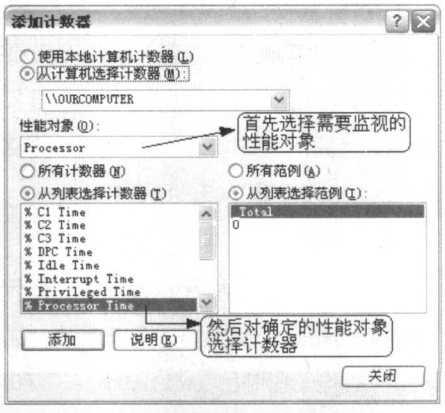

图1.8 给“我的系统监视器”添加计数器

对于内存，我们要监视它的Available Mbytes（当前的自由内存数）、Pages/Sec（每秒钟发生的页面错误的次数，也就是所请求的页不在内存中，而需要到硬盘里去读取的计数）。

对于硬盘子系统，我们要监视它的%Disk Time

(硬盘为读或写入请求提供服务所用时间的百分比。)、Avg.Current Disk Queue Length(硬盘在设定时间间隔里读写请求队列的平均数)。

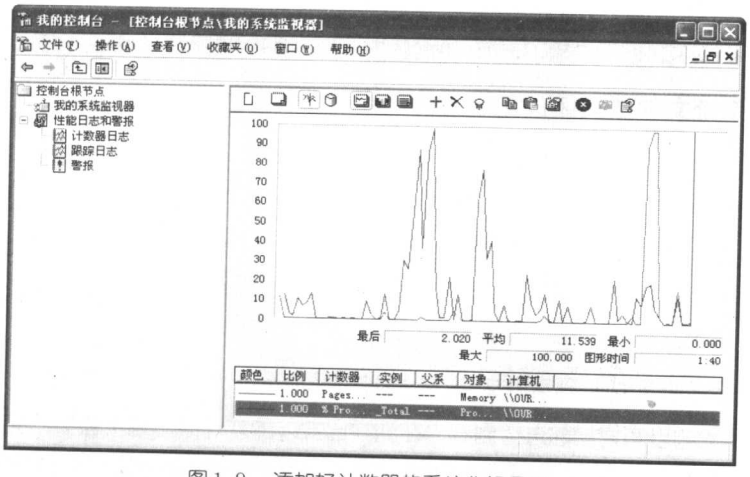

图1-9 添加好计数器的系统监视界面

第3步，最后的界面见图1.9所示，每个计数器都用图表的形式显示实时数据跟踪情况，也可以改成自己喜欢的视图格式（比如说直方图、报表图等）。

现在“血检化验单”已经出来了，但你总得读懂它呀，这样才能找出系统性能瓶颈的所在。下面对所监视的性能对象分别阐述：

- 处理器：通常不会成为系统瓶颈。你可以打开一个3D的屏幕保护程序，可以看到%Processor Time计数器迅速达到峰值。如果%Processor Time计数器经常大于80%才可能有处理器瓶颈，如果Interrupt/Sec计数器经常高于3500，则可能是程序或硬件有问题，以至于产生大量的“伪中断”。
- 内存：最有可能造成系统瓶颈。如果内存容量太低，那么需要经常读写硬盘，由于硬盘速度远低于内存，从而导致整个系统性能低下。如果Available Mbytes的值经常小于4MB，则需要增加内存，而Pages/Sec的值应该小于20，最好是在4~5之间。
- 硬盘：你可以用一些引起磁盘活动的事件来验证，比如说在不同分区之间粘贴、拷贝一些文档，如果%Disk Time计数器的平均值小于90%而Avg.Current Disk Queue Length计数器的平均值小于2，则说明没有对硬盘产生过量请求。

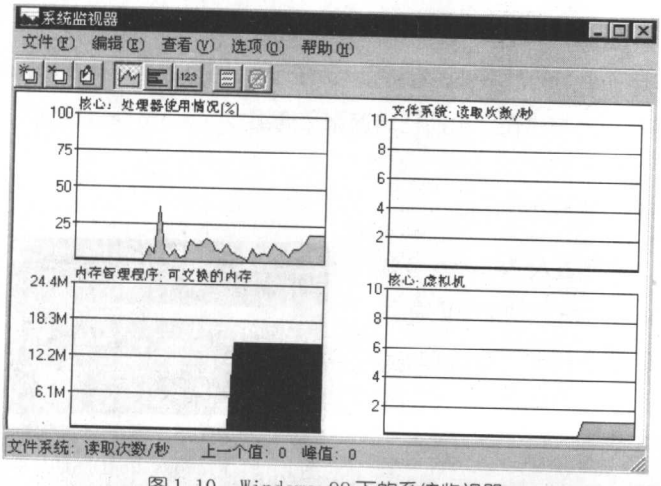

图1.10 Windows 98下的系统监视器

现在该说说Windows 98的定量分析方法了。单击“开始”→“程序”→“附件”→“系统工具”，打开里面的系统监视器，单击“编辑”→ “添加项目”，可以增加要监视的系统项目，监视的内容比Windows 2000/XP中控制台的内容要相对简单一些（见图1.10）。

2. 损兵折将——系统文件被破坏

这也是Windows的一种多发病，而且诱因很多，经常增删应用程序，非正常关机，人为的误删操作，都有可能会导致系统文件被破坏，严重的话，还会导致系统崩溃。而且，尽管Windows 9x/Me和Windows 2000/XP是一奶同胞，但是内核不一样，所以产生问题的原因也不尽一致。

（1）Windows 9X/Me的系统文件被损坏

▲症状与诊断

症状1：启动后出现“I/O error,press any key to replace”的错误提示，不管是Windows还是DOS都进不了。

诊断：自家人进不了自家门，你肯定会非常着急。其实原因很简单，这应该是C盘根目录下的重要启动文件被破坏了。

症状2：能进入系统，但是启动时提示找不到某个文件，一般扩展名是vxd和dll。

诊断：出现这种情况，主要是因为没有把删除进行到底。在删除已安装的软件时，如果直接把应用程序的安装目录删除，而没有清除注册表里对某个文件的调用，自然会导致误报文件丢失。

症状3：系统闹罢工，刚启动就出现“可以安全地关闭系统”，或者提示找不到某个系统文件(dll、drv、sys等)。

诊断：刚启动就出现“可以安全地关闭系统”，这多半是VMM32.VXD被毁损了。提示找不到某个文件嘛，自然是被误删除或者遭到了破坏。

症状4：提示说系统文件版本不对。

诊断：这是由于安装某些应用程序而造成的。有些应用程序因为设计上的问题，只要是自己需要的共享文件，不问青红皂白就给安装上了，这样就可能用安装程序中的旧版本文件替换了系统中已有的新版本，从而导致其他程序运行不正常。如果在Config.sys或Autoexec.bat文件里设置了一些遗留的DOS驱动程序或内存驻留程序的加载项，也可能会导致系统出现这种错误。

▲分析工具

系统出了问题，还能给出提示，这真是不幸中的万幸（尽管提示不尽正确，而且多半不得要领）。很多时候，连个提示都没有，就把你晾在一边，不过有了启动日志这张“通缉令”，还是可以找到问题的元凶。

方法如下：

第1步，在系统启动时，按住F8按钮，直到进入“Microsoft Windows 98 Startup Menu”(Windows 98启动菜单)为止。

第2步，在启动菜单里选择第二个选项“Logged (\Bootlog.txt)”(见图1.11)，然后回车。

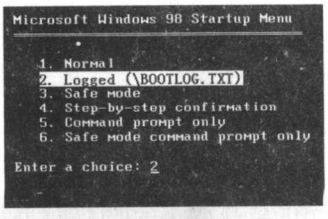

图1.11 Windows 98的启动菜单

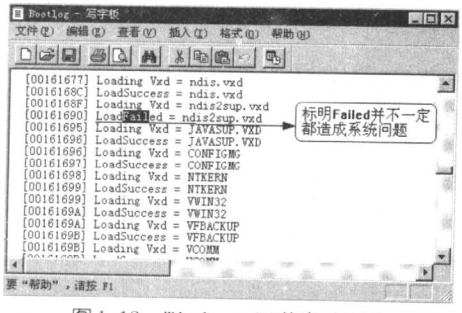

图1.12 Windows 98的启动日志

第3步，如果能够进入系统，那么就要检查启动日志文件，由于启动日志文件具有隐藏属性，所以要先作一下设置。打开“我的电脑”，单击“查看”→“文件夹选项”，切换到“查看”标签页，选择“显示所有文件”单选按钮。这样日志文件Bootlog.txt就乖乖现出了原形，可用写字板打开它(见图1.12)。

第4步，单击“编辑”→“查找”，在对话框里输入“Failed”来查找所有加载错误的项，不过并不是所有标明Failed的加载项都是造成系统错误的“罪魁祸首”。

如果在第2步操作后不能进入系统，那就只能求助于超级替补DOS了，重新回到图1.11所示的启动菜单，选择“Command Prompt only”，用纯DOS方式进入系统，然后键入命令“attrib -r -h -s C:\bootlog.txt”来清除启动日志的隐藏、系统、只读属性，然后用DOS下的编辑程序edit.exe来打开它即可。

(2) Windows 2000/XP的系统文件被损坏

尽管比尔吹嘘Windows 2000/XP是有史以来最稳定的视窗操作系统，但显然，它并非固若金汤，尽管不像它的前辈Windows 98一样拿死机当家常便饭，但是一旦摊上了这种倒霉事也不是闹着玩的。

▲症状与诊断

症状1：丢失了重要文件，比如Ntldr (NT引导管理器)、Ntoskrnl (NT内核文件)、Boot.ini (启动文件)等，造成无法进入系统。

诊断：这可能是由于有些朋友为了节省磁盘空间，用SFC/Disable命令禁用系统文件自动恢复，从而导致系统文件被误删、替换等。

症状2：有些安装了双系统的朋友在重装了Windows 98以后，导致没有多重启动菜单了。

诊断：在安装双系统时一定要记住最新版本的操作系统最后安装，如果后装Windows 98，会把Windows 2000/XP的启动文件破坏掉。

▲分析工具

Windows 2000/XP的这些问题也可以用启动日志来判断造成错误的加载项，不过Windows 2000/XP下的启动日志文件位于C:\WINNT (Windows 2000)或者C:\WINDOWS (Windows XP)目录下，文件名是Ntbtlog.txt，其他方法与Windows 98/Me中的差不多。

3. 病入膏肓——注册表损坏

注册表是Windows的心脏地带，保存着系统、应用程序和硬件的关键数据，如果注册表生了“病”，轻者无法正常运行应用程序、无法正常使用硬件设备，重者导致系统瘫痪、死机。注册表损坏是Windows 9X/Me的一种常见病，造成的原因有很多。如果系统出了故障，实在找不到原因，那么你

可以试试还原注册表，说不定能柳暗花明（具体方法见本章第 3 节）。

值得庆幸的是在 Windows 2000/XP 下几乎不会发生注册表被破坏的悲剧，这主要是因为 Windows 2000/XP 把注册表化整为零，分散在数个不同的文件里。而 Windows 9X/Me 注册表对应的文件存放在 %SystemRoot%\ 下，包括用户配置文件 User.dat 和系统配置文件 System.dat（Windows Me 里还包括 Classes.dat）。因此，这里主要是讲 Windows 9X/Me 下可能发生的注册表损坏迹象。

症状 1：无法进入 Windows 系统，只能用 MS-DOS 启动，或者自动进入安全模式。

诊断：这可能是因为某些应用软件本身的 Bug 造成了注册表和系统重要文件的损坏。所谓人无完人，就算是软件巨鳄微软，其产品也是谬误多多，一些共享软件自然更是有过之而无不及。就算是本身没有致命的错误，但和其他软件相处就有可能导致冲突。

症状 2：文件关联丢失，当你单击某个文档时，提示你“找不到应用程序打开这种类型的文档”，虽然你已经安装了正确的应用程序并且文档扩展名也正确。

诊断：在注册表里添加了错误的数据文件，破坏了应用程序与对应文档之间的关联性。比如说，有两个视频播放程序都能打开 rm 格式视频文件，平时倒也能相安无事，一旦删除了其中一个播放软件，它就会自作主张把 rm 文件的关联性给破坏掉，让 rm 文件成为“没娘的孩子”。

症状 3：明确提示“注册表损坏”。

诊断：这可能是在注册表里添加了错误内容。某些应用程序在安装的时候，出于种种目的，可能会在注册表里增加错误的内容，或者强制性地将原来正确的注册表内容给改错了。

症状 4：控制面板项目丢失，开始菜单项目丢失或者变灰处于不可用状态。

诊断：这很有可能是用户手工修改注册表而造成的。用户自己修改注册表也是导致注册表损坏的重要原因，在一台机器上进行修改没问题，但是到了另一台上就有可能导致致命错误。

另外，硬件问题也是产生注册表问题的一个“大户”。现在硬件的更新换代特别快，迫于竞争对手的压力，常常是驱动程序还没有完善就急于推向市场。我们在装硬件驱动的时候，经常会得到“该驱动程序未经微软测试”的警告，安装这样的驱动就要冒一定的风险。如果你把 16 位版本的硬件驱动安装到 32 位的 Windows 系统上，或者同一个硬件的 16 位和 32 位驱动程序共存，都可能会造成注册表损坏。

4．狡兔三窟——木马和病毒入侵

Windows 家族虽然人丁兴旺，但是它们的安全性，实在不怎么样，尤其是 Windows 9X 系列，简直是千疮百孔，只需用十个字符就可以让它崩溃，不信？试试在“运行”对话框里输入“c：\con\con”，然后按回车，嘿嘿，是不是蓝屏了。既然 Windows 主动“开门揖盗”，病毒和木马自然乐得乘虚而入，这也是造成系统死机的重要原因，最近还有愈演愈烈之势。一旦你的机器“中了奖”，被这些恶意代码“下了蛊”，那就会落入万劫不复的境地，它们可以掌握文件的生杀大权，把你的电脑变成 FTP 服务器（这样黑客就可以肆意增删你的文件了），获取你的隐私，最不济也能让你奔腾 4 的电脑变成老爷车。

下面简单介绍一下一些常见的被木马或病毒侵袭后的症状。

症状1：系统的启动时间变长。

诊断：这有可能是病毒或木马程序修改了系统启动时所调用了相关文件。比如System.ini文件，它们可能会在[boot]小节里修改类似于这样的设置项：

```
[boot]
shell = Explorer.exe 恶意程序
```

这是指Windows加载外壳程序（Explorer.exe）的时候必须运行病毒或木马程序，如果你直接到木马或病毒的黑据点里（一般是C:\Windows或者\windows\system下）把它们赶跑非但于事无补，反而会导致Explorer.exe加载错误。

对于Win.ini文件，会在[windows]小节里添加如下的设置：

```
[windows]
load =恶意程序 （或者run =恶意程序）
```

这样每次系统引导的时候，这些恶意程序就会自动搭上Windows的“早班车”。

批处理文件，如Autoexec.bat和Winstart.bat文件也可能被修改，对于Autoexec.bat大家很熟悉了，此处不再赘述，Winstart.bat是Windows 98自启动的一扇非常隐蔽的后门，它位于C:\WINDOWS下，可以完全替代Autoexec.bat的批处理功能。

症状2：每次拨号上网时都会弹出防火墙的警告。

诊断：拨号上网的用户会用到rasapi.dll这个动态链接库文件，一些恶意代码就会用自己的DLL文件来一个狸猫换太子（代码里含有指向真正rasapi.dll文件的语句），当你运行拨号上网程序的时候，恶意代码就会先行启动，然后再调用真正的rasapi.dll。

症状3：删除多余的Explorer.exe后，桌面变成一片空白。

诊断：SubSeven2.2这一类的木马程序，会把它的“马甲”安放在C盘根目录下，在该目录里就会多出一个Explorer.exe文件，这就是安装后的服务端程序，大小是55KB，乍一看好像是Windows自带的explorer（注意，真正的Explorer位于“C:\WINNT”下，大小是233KB），而且注册表里所有调用Explorer的键值都变成了“C:\Explorer.exe”，也就是指向了木马的服务端程序，所以如果不分青红皂白直接删除了那个“李鬼”Explorer，则会导致系统无法加载Explorer，屏幕会变得“白茫茫一片”。用Norton的最新版杀毒软件查是能查出来，但没法彻底清除。

症状4：清除了某种依附在EXE文件中的恶意代码后，EXE文件却不能用了。

诊断：有些木马程序除了在“C:\WINDOWS”下增加一个带恶意代码的主程序外，还会将注册表HKEY_CLASSES_ROOT\exefile\shell\open\command\的键值从原来的“"%1"%*”变成了“恶意代码"%1"%*”。这意味着要运行任何一个EXE文件，必须先运行这个恶意代码，这一招非常恶毒，就算你把恶意代码的主程序踢出硬盘，也会发现所有的EXE文件都无法运行。此外，也有和TXT文本文件关联的，无奇不有。