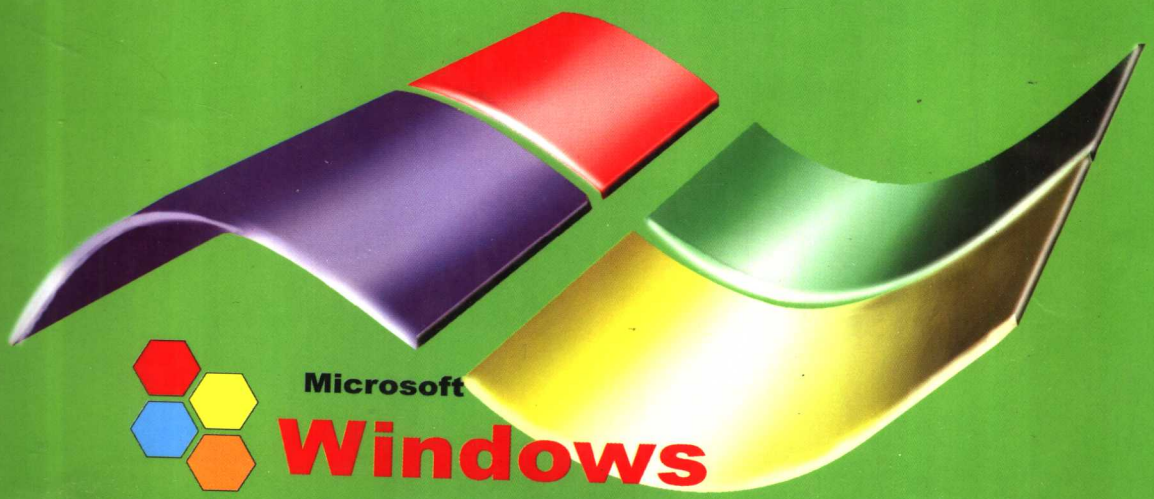
电脑报 总策划 http://www.yesky.com

Windows系统真经 ③

系统文件、数据安全绝密档案

系统文件　注册表漏洞　恶意代码全防护

柴璟
彭睿 编著



云南人民出版社

Windows系统真经③

Windows系统文件、数据安全绝密档案

柴 璟 彭 睿 编著

云南人民出版社

图书在版编目（CIP）数据

Windows系统真经／电脑报社编．－昆明：云南人民出版社，2003.8
ISBN 7-222-03850-7

Ⅰ.W… Ⅱ.电… 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069845号

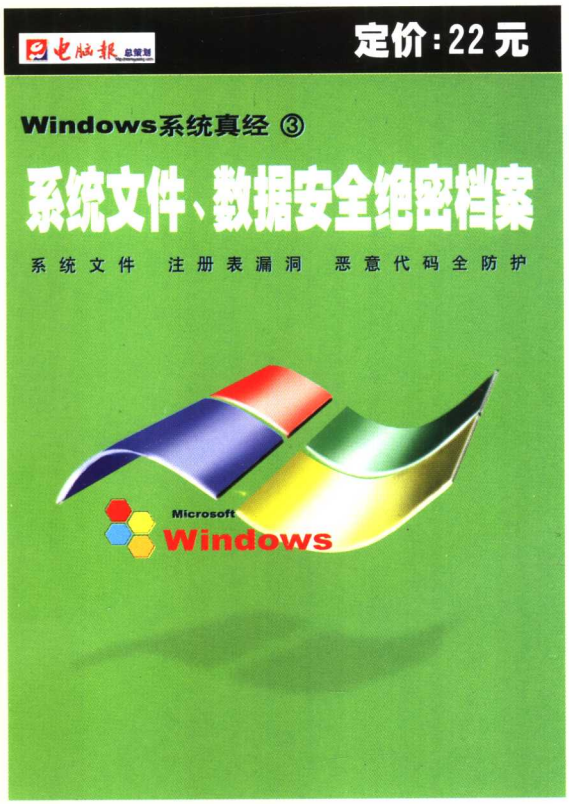
责任编辑：西　捷　王　梅
技术编辑：黄继东
封面设计：意　在
版式设计：李品娟

书　　名：Windows系统真经——Windows系统文件、数据安全绝密档案
作　　者：柴　璟　彭　睿
出　　版：云南人民出版社
发　　行：云南人民出版社
社　　址：昆明市环城西路609号
邮　　编：650034
电　　话：0871-4113185　4194569　4194559
E－mail：YNPPDZ@vip.km169.net
开　　本：787mm×1092mm　1/16
印　　张：17
字　　数：430千
版　　次：2003年9月第1版第1次印刷
印　　数：1-5000
印　　刷：重庆现代彩色书报印务有限公司印刷
书　　号：ISBN 7-222-03850-7
定　　价：66.00元／套（本册定价：22.00元）

电脑报 总策划

Windows 系统真经③

系统文件、数据安全绝密档案



全新上市

面对脆弱的 Windows，如何来保护你的文件、数据安全？

本书分注册表安全设置、防范恶意代码、Windows 应急与恢复、重要资料的备份与恢复、系统的加密保护、防堵系统漏洞、多操作系统防崩溃、木马与病毒百毒不侵八个章节，全方位地介绍了 Windows 系统可能出现的各种安全隐患并有针对性地提出解决方案。

Chapter 1 注册表安全设置
介绍了注册表的备份与恢复、Windows 9x/Me 注册表的备份与恢复、Windows 2000/XP注册表的备份与恢复、限制注册表的方法。

Chapter 2 防范恶意代码
介绍了恶意代码以及恶意代码修改IE的方法，带你恢复被修改的 IE 标题栏、恢复 IE 默认主页、恢复被禁用的 IE 选项、恢复被恶意网站修改的 IE，让你学会修改 IE 右键弹出菜单等技巧。

Chapter 3 Windows 应急与恢复
介绍了 Windows 98 的应急与恢复、Windows 98/2000/Me的备份、Windows XP的应急与恢复、系统设置与文件的备份和恢复，引导你学会驱动程序的备份。

Chapter 4 重要资料及文件的备份与恢复
介绍了 Internet Explorer 的备份与恢复、Outlook Express 的备份与恢复、Foxmail数据的备份、QQ资料的备份、ICQ重要数据的备份与恢复、下载工具的备份和恢复、CuteFTP工具的备份和恢复、输入法数据的备份和恢复、Office设置的备份和恢复、杀毒软件的备份与恢复等方法。

Chapter 5 系统的加密保护
介绍了利用“回收站”进行加密、利用“类标识符”进行加密和解密、利用“自定义文件夹”选项进行加密、利用“加密档案系统 EFS)”进行加密、利用“注册表”进行加密、利用“文件管理器”进行加密、利用“加密档案系统(EFS)”进行加密等方法。

Chapter 6 防堵系统漏洞
介绍了系统漏洞的发现以及防堵技巧，使你的Windows 更加安全地运行。

Chapter 7 多操作系统防崩溃
介绍了多操作系统的安装、多操作系统文件夹共享、多操作系统防止崩溃的详细方法。

Chapter 8 木马与病毒的防治
介绍了目前常见的木马破解与清除方法，教你学会系统防黑与查杀病毒，保障电脑更安全。

内 容 提 要

面对脆弱的Windows，如何来保护你的文件、数据安全?

本书分注册表安全设置、防范恶意代码、Windows 应急与恢复、重要资料的备份与恢复、系统的加密保护、防堵系统漏洞、多操作系统防崩溃、木马、病毒百毒不侵八个章节，全方位地介绍了windows 系统可能出现的各种安全隐患并有针对性地提出解决方案。

全书内容丰富，实用性强、易学易用，适用于各层次读者阅读，特别适合电脑爱好者及初学者阅读收藏。

目　录

第一章 注册表安全设置

1.1 注册表的备份与恢复

大家知道，Windows 3.x 是用扩展名为.ini 的配置文件来保存系统及应用程序的各种初始化信息的。每次系统启动时，都会从两个重要的.ini 文件，即 system.ini 和 win.ini 里读取各种初始化信息来对整个系统的软硬件环境进行配置。其中 system.ini 存储系统配置信息，win.ini 存储应用程序配置信息。从 Windows 95 开始，原来保存在以上两个初始化文件中的有关信息，都被移到了系统的注册表中，这样注册表就成了 Windows 系统关键信息的集中存放地。原来的两个文件为了兼容老的 16 位 Windows 应用程序也依然保留着。

在 Windows 9x/Me 中，注册表由两个文件组成：system.dat 和 user.dat。它们不是文本文件，而是由二进制数据组成，因而不能通过文本编辑器查看和修改。注册表编辑器是用户用于更改系统注册表设置的高级工具，只有通过它我们才能看到注册表的组成和结构。注册表是 Windows 系统的一个巨大的核心数据库，它包括：

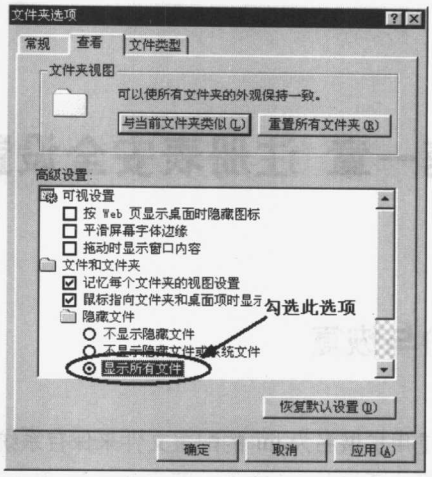
- 软、硬件的有关配置和状态信息。
- 计算机的网络设置和各种许可，文件扩展名与应用程序的关联，硬件部件的描述、状态和属性。
- 性能记录和其他底层的系统状态信息，及其他数据。

注册表作为 Windows 的数据配置核心，对软件的运行和硬件的管理都是举足轻重的。操作系统利用注册表存取计算机系统的软、硬件信息，因此注册表的好坏将直接关系到整个系统的启动、应用软件的正常运行和各种硬件驱动程序的装载。如果注册表由于各种原因受到破坏，轻则导致系统运行不稳定，重则可能导致整个系统的瘫痪。因此正确的认识、使用以及备份、恢复注册表对用户而言就显得十分重要。

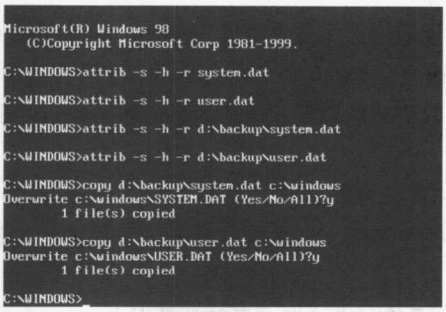
1.1.1 Windows 9x/Me 注册表的备份与恢复

一、自己动手备份恢复

前面我们已经介绍了 Windows 9x/Me 中注册表是由两个数据库文件 system.dat 和 user.dat 构成的，前者用来存储本地计算机的系统信息，后者保存用户信息。为防系统不测，平时只要对这两个文件进行手动备份，保存在一个比较安全的地方，系统一旦出了问题，利用它就可使系统起死回生。不过在默认情况下，这两个文件具有隐藏、系统、只读的属性，在资源管理器中是找不到的。手工备份时，在 Windows 资源管理器的界面下点击“查看/文件夹选项”弹出“文件夹选项”对话框，切换到“查看”选项卡，在“文件和文件夹/隐藏文件”选项中勾选“显示所有文件”，如图：



点击“确定”按钮返回后即可在“Windows”文件夹中找到这两个文件。这时用户可以用复制、粘贴命令将这两个文件备份到一个较安全的地方，如 d:\backup。因为系统故障需要对系统进行恢复时，在启动计算机进行完自检之后，按下 F8 键，在启动菜单中选择“Safe mode command prompt only”进入安全模式下。执行如下命令（假设系统安装在 C 盘），如图:

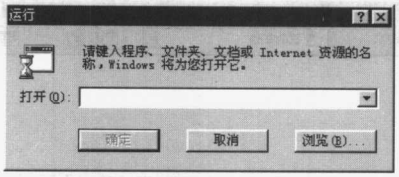


attrib -s -h -r system.dat	* 去掉 system.dat 系统、隐含、只读属性
attrib -s -h -r user.dat	* 去掉 user.dat 的系统、隐含、只读属性
attrib -s -h -r d:\backup\system.dat	* 去掉 backup 文件夹中备份的 system.dat 系统、隐含、只读属性
attrib -s -h -r d:\backup\user.dat	* 去掉 backup 文件夹中备份的 user.dat 的系统、隐含、只读属性
copy d:\backup\system.dat c:\windows	* 将备份的 system.dat 复制到 windows 目录中
copy d:\backup\user.dat c:\windows	* 将备份的 user.dat 复制到 windows 目录中

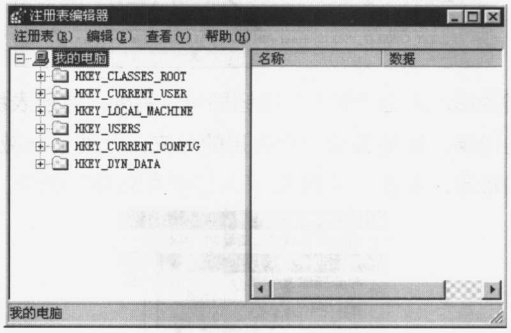
当然，d:\backup 的位置只是一个例子。此外，复制文件时系统会提示是否覆盖原文件，按“Y”确认将备份的注册表文件恢复到系统中即可。

二、利用注册表编辑器自带的导出及引入功能

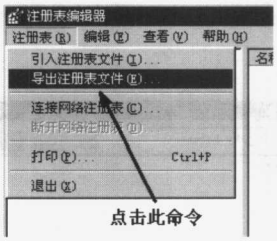
点击“开始/运行”弹出“运行”对话框，如图:



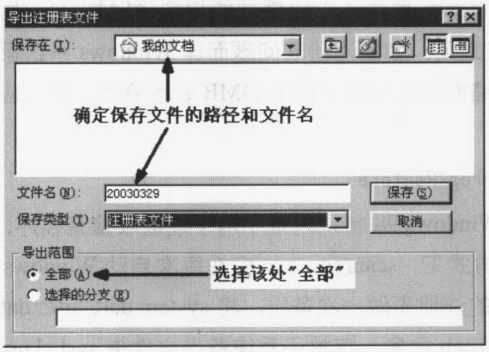
输入“regedit”后，点击“确定”按钮即可打开注册表编辑器，如图:



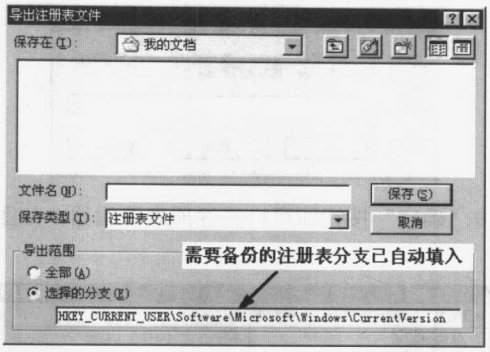
如果用户需要导出整个注册表文件，点击“注册表/导出注册表文件”命令，如图:



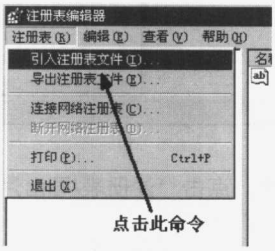
在出现的“导出注表文件”对话框中，键入欲备份注册表的文件名及其保存路径，在“导出范围”中选择“全部”，再按“保存”按钮即可，如图:



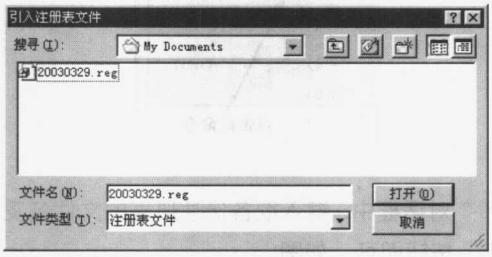
如果用户需要导出注册表中的某个分支，则需先在注册表编辑器中切换到该分支，再点击“注册表/导出注册表文件”命令，在出现的“导出注表文件”对话框中的“导出范围”中已经自动填写了用户需要导出的注册表分支，如图:



确定好文件名和保存路径后，点击“保存”按钮即可。另外，注册表编辑器在导出注册表时还能修复注册表中的一些简单的错误，并能去掉一些无用的分支，让注册表减减肥。需要恢复注册表时，用同样的方法打开注册表编辑器，点击“注册表/引入注册表文件”命令，如图：



在出现的“引入注册表文件”对话框中选中所需恢复的备份文件，再按“打开”按钮即可将该注表备份恢复到 Windows 系统中，如图：

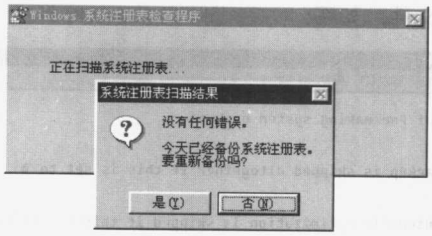


该方法主要适合于 Windows 系统还未瘫痪或能用启动时按 F8 键的方法，选择安全模式启动 Windows 98 系统时恢复注表之用，如因注册表问题而连 Windows 系统都进入不了时，则该法就无法应用了。此外因备份无法压缩而其大小又超过 1.44MB 软盘容量，所以应用该法也只能将备份保存在硬盘里了。

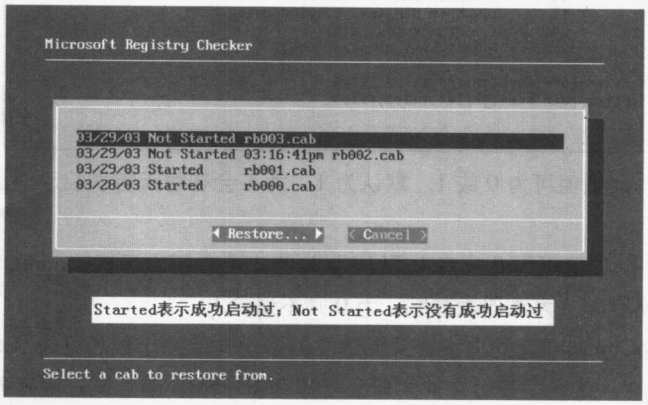
三、使用 Scanregw 和 Scanreg/Restore

由于注册表的重要性，Windows 98 特别内置了两个注册表检查程序，scanregw.exe 和 scanreg.exe，分别用于 Windows 和 DOS 方式下。scanregw.exe 会在每次启动 Windows 时自动运行，对系统注册表进行检查，并对该次启动时的注册表做一次备份，将 system.dat、user.dat、system.ini、win.ini 四个文件打包成 cab 文件，以 rb00?.cab 命名，存放于系统备份文件夹 sysbckup 中，默认为保存最近 5 次备份的文档。在“开始/运行”中输入“scanregw”，确定后注册表检查器就会对注册表进行扫描，当检查到注册表出错时，它就可以用备份进行恢复，如果没有错误，它还会提醒用户当天已经备份了注册

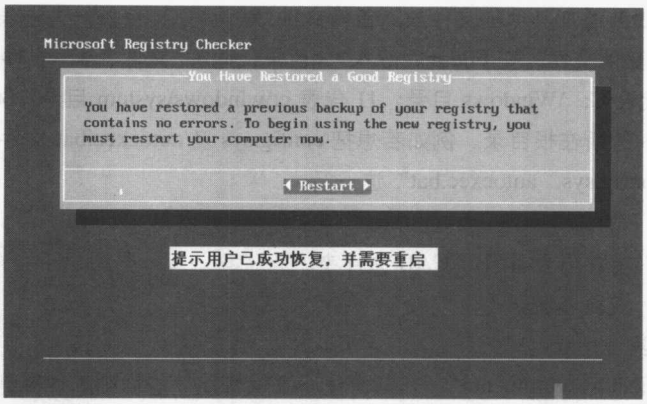
表，是否重新备份，如图：



注册表恢复时需要用到“scanreg”，需要注意的是，该命令必须在 MS-DOS 模式下运行。而且运行环境必须是纯 MS-DOS，而不是在 Windows 下运行的仿真 MS-DOS 模式。当操作系统无法正常启动时，用户可以先启动到纯 MS-DOS 下，然后在 DOS 下键入“scanreg/restore”命令，其中“scanreg”是注册表检查器命令，“/restore”为按照备份的时间以及日期显示所有的备份文件。回车后来到“Microsoft Registry Checker”画面，在该画面中用户可以看到压缩备份的文件以.cab 文件列出，在显示备份时间的后面单词是“Started”或者是“Not Started”，如图：



“Started”表示这个备份文件能够成功启动 Windows，是一个完好的备份文件；“Not Started”表示文件没有被用来启动 Windows，不知道是否是一个完好的备份。选择一个时间最近、可以“Started”的备份文件，点击“Restore”按钮或敲下键盘上的“R”按键，不一会注册表就成功恢复了，如下图：



最后单击“Restart”或敲下键盘上的“R”按键，重新启动计算机问题就会迎刃而解。

默认情况下，注册表数据库只有 5 个备份记录，如果备份超过 5 个时，新的备份文件就会覆盖旧的备份文件。如果用户感觉 5 个备份文件不够多的话，可以通过修改“scanreg.ini”文件将“Windows