系统管理人员进阶与提高黑皮书

全新推出
精心制作

Windows XP 注册表应用实践与精通

林山 主编

清除木马v1.1

打开注册表编辑器（Regedit）。
定位目录至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
查找以下的两个路径，并删除它们：
C:\Windows\System\kernel32.exe
C:\Windows\System\sysexplr.exe
关闭Regedit。
重新启动计算机，进入到MS-DOS方式下。
删除C:\Windows\System\kernel32.exe和C:\Windows\System\sysexplr.exe木马程序。
重新启动Windows。

清除木马v2.2

服务器程序、路径用户可以随意定义，写入注册表的键名也可以自己定义。因此，不能明确说明
察看注册表，把可疑的文件路径删除。
重新启动计算机，进入到MS-DOS方式下。
删除与注册表相对应的木马程序。
重新启动Windows。

清华大学出版社
http://www.tup.tsinghua.edu.cn

Windows XP 注册表应用实践与精通

林 山 主编

清华大学出版社

（京）新登字 158 号

内 容 简 介

Windows XP 将其配置信息存储在一个被称为注册表的数据库中，该注册表包含计算机中每个用户的配置文件，有关系统硬件的信息，安装的程序及属性设置。Windows XP 在其运行中不断引用这些信息，因此，了解这些信息在注册表中的组成结构、作用对中、高级 Windows XP 用户和计算机专业人员具有重要的意义。本书从实用的角度出发，结合大量的实例，详细地剖析了 Windows XP 的注册表。

本书主要针对中、高级计算机用户，内容翔实、实例丰富、可操作性强。在讲清概念的同时，又给出有很强实用价值的例子，便于读者快速掌握并熟练运用。本书适合广大工程技术人员和计算机爱好者阅读、使用。

书　　名：Windows XP 注册表应用实践与精通
作　　者：林　山 主编
出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
责任编辑：田在儒
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×960 1/16　**印张**：25.5　**字数**：569 千字
版　　次：2002 年 7 月第 1 版　2002 年 7 月第 1 次印刷
书　　号：ISBN 7-302-05539-4/TP・3262
印　　数：0001~5000
定　　价：35.00 元

丛 书 序

操作系统一直以来都是计算机软件部分的核心内容，它既是指挥硬件协调工作的“大脑”，又是承载应用软件功能的“基石”。微软公司的 Windows 系列操作系统软件，在 PC 领域占据着绝对的统治地位；在工作站、服务器领域，也占有很大的装机比例。随着 Windows XP 的推出，其更强大的功能、更安全的特性、更友好的界面、更稳定的性能吸引了越来越多的使用者，无疑这将掀起学习和使用 Windows 最新操作系统的热潮。本《系统管理人员进阶与提高黑皮书》系列丛书正是顺应这个形势而推出的。

无论是对家庭用户、企业用户还是计算机工程技术人员来说，一套全面、实用、深入讲解 Windows XP 及.NET Server 技术的指导性书籍都是大有裨益的。本套丛书共 5 本，分别是：

- 《Windows XP 注册表应用实践与精通》
- 《Windows XP 网络信息服务应用实践与精通》
- 《Windows XP 网络安全应用实践与精通》
- 《Windows XP 规划管理应用实践与精通》
- 《Windows XP 局域网建设应用实践与精通》

本套丛书涉及的内容基本上涵盖了 Windows XP 和.NET Server 的各个方面。为了描述方便，各书内容基本以 Windows XP 为描述核心。但是 Windows XP 作为服务器的应用一般限于家庭和小型网络，具有实验的性质。对于大中型网络而言，Windows XP 是作为客户端操作系统使用的。为了描述上的完整性，本套丛书对于作为典型的服务器端操作系统使用的 Windows.NET Server 及 Windows 2000 Server 的相关内容也进行了详细介绍，并指明了它们在各种应用场合中与 Windows XP 之间的关系。

Windows XP 通过集成 Windows 2000 的强项（基于标准的安全性、可管理性和可靠性）与 Windows 9x 的最佳功能（即插即用、易用的用户界面、创新的支持服务），实现了 Windows 系统的完美统一，给使用者带来了激动人心的新功能。国内越来越多的家庭和企业用户为自己的计算机升级了这个全新的操作系统，因此 Windows XP 的应用、管理、维护、开发等各方面技术知识成为计算机从业人员和技术爱好者兴趣的焦点。

本套丛书的编写者由第一线系统工程人员、程序开发人员，以及大学计算机专业教师组成，所有参与编写的人员都怀着极大的热情，翻阅了大量的最新外文参考资料，力争使本套书做到实用性、全面性和时效性俱佳。

本套丛书的编者们也对 Windows.NET Server 的各个 Alpha、Beta 测试阶段进行了长达

一年的跟踪测试，这个服务器端操作系统具有和 Windows XP 一样漂亮易用的外观界面，具有比 Windows 2000 Server 更强大的功能和更细分的应用市场。本套丛书在大中型网络技术或应用场合把其作为服务器端操作系统进行了介绍，这也是对实际应用中 Windows XP 的局限性的有益补充。

本套丛书的各种术语和定义基本符合大家约定俗成的习惯，为了让大家更好地使用本套丛书，下面对本套丛书中鼠标操作的表达方法做一简要介绍。

- 左键：一般指鼠标左按键。
- 右键：一般指鼠标右按键。
- 单击：按下鼠标左键，随之马上释放（松开）。除特别说明外，“单击”都指单击鼠标左键。
- 双击：快速重复两次单击操作。大多数情况下，双击操作对象等效于先单击选择操作对象，然后再单击“确定”按钮（或按 Enter 键）。
- 三击：快速重复三次单击操作（只在特殊软件的特殊用途中用到）。
- 右击：按下鼠标右键，随之马上释放（松开）。
- 指向：不按鼠标按钮的情况下移动鼠标指针到预期位置。
- 拖动：按住鼠标左键的同时移动鼠标指针。
- 释放：松开按住鼠标键的手指。
- 拖放：按住鼠标左键的同时移动鼠标指针，移到预期位置后松开按住鼠标键的手指（等同于拖动+释放）。
- 选择：选取操作对象。大多数选择操作都可通过单击操作对象进行。选择将使操作对象的外观发生变化，如呈反向显示或其周边出现选择框和选择块。

此外，本套丛书在版面设计上，力求活泼而不失典雅。为了突出书中的某些内容使用了一些特殊符号：

操作步骤

(1) 具体操作步骤一。

(2) 具体操作步骤二。

(3) ……

此处内容是注释部分。对书中涉及到的技术名词、术语和一些概念进行解释，以便于读者更好地理解上下文内容，或学习一些概念和基础知识。

此处内容是技巧部分。通过使用这些操作技巧，可提高读者完成任务的速度，或实现一些常规方法达不到的目的。

此处内容是警告部分。提醒读者需要小心操作的步骤，或者对于非常危险的操作可能产生的不良后果进行解释。

此处内容是疑难部分。主要解释一些需要具有一定计算机基础知识的读者才能理解的内容。一般读者可跳过此部分，不影响上下文的阅读。

经过将近一年时间的紧张编写，本套丛书终于全部完成了，由于作者水平有限，加上编写时间仓促，书中的缺点错误在所难免，恳请专家和广大读者热心指正。

编者

2002 年 6 月

目　录