

谁动了我的电脑

华师傅资讯 ◆ 编著

查一知百

从蛛丝马迹查看谁动过我的电脑

知己知彼

了解黑客要对你干什么

层层设障

打造系统铜墙铁壁

坚壁清野

让破门而入者一无所获

软硬兼施

从硬件入手锁定你的电脑

有备无患

从系统灾难中神奇地恢复数据

精彩光盘

卡巴斯基反病毒软件

金山木马专杀工具

各类数据备份修复工具荟萃



山东电子音像出版社出版

Figure 1

谁动了我的电脑

编著 华师傅资讯



148 275

得分均以材料與預中島光景照年本
用此號作代
上各款均係用此號作代
此以各。容因志未去不，知所辭謝並置費
周旋公謝戶向和立對，略內忘年莫史書
，煩幸天
照此號

山东电子音像出版社出版

第1章 蛛丝马迹——三招两式看谁动过我的电脑 ... 1

1.1 看看在我的系统上干了什么 ... 2

1.1.1 用Windows事件查看器看使用记录 ... 2

1. 查看上网时间 ... 2
2. 查看计算机开关机记录 ... 3
3. 查看黑客入侵记录 ... 4

1.1.2 查看更多系统记录 ... 4

1. 查看程序运行记录 ... 4
2. 查看TEMP文件夹记录 ... 5
3. 查看Windows搜索记录 ... 5
4. 查看开始菜单中的文档记录 ... 6
5. 查看访问网上邻居留下的信息 ... 6
6. 查看剪贴板查看器记录 ... 6
7. 查看回收站 ... 7
8. 查看添加删除程序记录 ... 7
9. 查看注册表编辑记录 ... 7
10. 查看软件使用后留下的记录 ... 8

1.1.3 查看聊天记录 ... 9

1. 查看QQ聊天记录 ... 9
2. 查看MSN聊天记录 ... 9

1.1.4 查看WEB记录 ... 10

1. 查看Cookies记录 ... 10
2. 查看Internet临时文件记录 ... 12
3. 查看历史记录 ... 13

1.2 随时随地监视我的系统 ... 13

1.2.1 使用系统监视工具 ... 13

1. 用“系统开机记录”查看开机 000 档案	13
2. 用“了如指掌”查看系统使用记录	16
1.2.2 随时不忘监视屏幕	17
1. 用“屏幕间谍”监视屏幕	17
2. 用“监视精灵”监视系统运行	19
1.2.3 利用“NiceSpy”进行远程查看	23

第 2 章 注册表访客——谁动了我的注册表 25

2.1 形形色色的注册表访客	26
2.1.1 日常操作中对注册表的访问	26
2.1.2 软件安装中对注册表的访问	28
2.1.3 危险的注册表启动	30
2.1.4 黑客远程操作注册表	33
1. 开启终端服务	33
2. 远程冲破 telnet 中 ntlm 权限验证	34
2.2 恶意代码对注册表的修改及清除	34
2.2.1 恶意代码对注册表的修改	34
2.2.2 恶意代码对注册表的篡改与修复	35
1. 开机自动弹出的网页	35
2. 系统启动时弹出对话框	36
3. IE 标题栏被修改	36
4. IE 默认连接首页被修改	36
5. 篡改 IE 的默认页	37
6. 修复被锁定的注册表	37
7. IE 浏览器缺省主页被修改，设置项被锁定	38
8. IE 右键菜单被修改	38
9. 查看“源文件”菜单被禁用	38
10. IE 中鼠标右键失效	39
11. IE 默认搜索引擎被修改	39
12. IE 地址栏下多出了文字	39

13.	操作系统被修改	40
14.	IE 窗口定时弹出	40
15.	IE 工具栏(菜单)被添加网站链接	40
16.	桌面上的图标全部消失	41
17.	“我的电脑”下的一系列文件夹名称被更改	41

2.3 木马对注册表的修改及清除 41

1.	清除 AcidShiver V1.0+1.0Mod+lmacid	42
2.	清除 DarkShadow	42
3.	清除 DonaldDick V1.52-1.55	42
4.	清除 Drat V1.0-3.0b	43
5.	清除 Eclipse2000	43
6.	清除 IndocTrination V0.1-v0.11	43
7.	清除 Malicious	44
8.	清除 MastersParadise	44
9.	清除 Naebi V2.12-2.40	44
10.	清除 NetSphere V1.0-1.31337	45
11.	清除 Prayer V1.2-1.5	45
12.	清除 PRIORITY (Beta)	46
13.	清除 Prosiakbeta-0.70b5	46
14.	清除 SatansBackDoor V1.0	46
15.	清除 SetupTrojan (Sshare)+ModSmallShare	47
16.	清除 ShareAll	47
17.	清除 ShitHeap	47
18.	清除 Thing V1.00-1.60	47
19.	清除 YAT	48
20.	杀除木马要点	48

2.4 打好注册表防御战 49

2.4.1 不得不做的IE防御 49

1.	用“IE 修复专家”捍卫 IE	49
2.	用“IE 恶性代码杀手”维护 IE	51

2.4.2 注册表安全管理 53

1.	注册表的备份和恢复	53
----	-----------	----

2. 注册表编辑器锁定管理	54
3. 注册表文件导入管理	55
4. 注册表远程访问管理	56

第9章 黑网来客——网络上黑白两派的对抗 59

3.1 谁在扫描我的端口 60

3.1.1 黑客攻击过程全解 60

3.1.2 端口安全的管理 62

1. 端口的安全意义 62

2. 开放要使用的端口 65

3. 关闭不用的端口 66

3.1.3 用天网在线检测端口安全 67

3.1.4 使用天网防火墙防范端口安全 68

3.2 谁窃取了我的ID——木马 70

3.2.1 木马盗号解析 70

3.2.2 六招防范传奇盗号 72

3.2.3 QQ盗号安全策略 73

1. 防盗策略 73

2. 使用QQKav工具防止QQ盗号 75

3.3 谁在对我远程控制——木马 76

3.3.1 看透形形色色的木马 76

1. 分清木马的类别 76

2. 识别木马的伪装 78

3. 了解木马的启动 79

3.3.2 做好木马预防工作 80

3.3.3 杀除木马 81

1. 用反木马软件杀木马 81

2. 遭遇木马之后的应对之策 82

3.4	谁在向我推销广告——间谍软件	82
3.4.1	悄悄潜入的间谍软件	82
1.	一则令人震撼的新闻	82
2.	间谍软件——新型网络杀手	83
3.4.2	间谍软件克星点评	84
1.	知名度最高的 AD-aware	84
2.	专门清理间谍软件的“SpyBot Search&Destory”	85
3.5	谁在破坏我的系统——病毒	88
3.5.1	病毒故事——病毒的陷阱	88
3.5.2	杀毒软件使用技巧	90
1.	实时监控系统状态	90
2.	用任务管理定时杀毒	91
3.	合理设置杀毒选项	92
4.	在线升级杀毒软件	92
3.6	谁在挤占我的邮箱——垃圾邮件	93
3.6.1	Foxmail垃圾邮件过滤设置	93
1.	设置自动过滤垃圾邮件	93
2.	给 Foxmail 设置黑名单	95
3.	让 Foxmail 学会识别垃圾邮件	96
4.	清除邮件炸弹	97
3.6.2	Outlook Express垃圾邮件过滤设置	97
1.	设置邮件自动过滤	97
2.	防范邮箱炸弹	99
3.6.3	网上免费邮箱防垃圾邮件设置	100
1.	新浪垃圾邮件过滤设置	100
2.	搜狐垃圾邮件过滤设置	101
3.6.4	用“邮件探针”防止垃圾邮件	102
1.	“邮件探针”的专有名词	103
2.	选项设置与邮件处理	103
3.	取信与信件的处理	106

3.7 安全漏洞大检查..... 107

1. 瑞星的漏洞扫描工具..... 107
2. 用FixBig找漏洞补丁..... 109

第4章 层层设障——小小招术防止他人使用电脑. 111

4.1 我的电脑你别开..... 112

4.1.1 开机BIOS密码的设置..... 112

1. 明确BIOS 密码类别..... 112
2. BIOS 密码设置方法..... 112
3. BIOS 密码应用的范围..... 113
4. 取消BIOS 密码..... 113

4.1.2 系统登录安全策略..... 114

1. Windows 98 系统“个性化”登录口令设置..... 114
2. Windows 2000 系统安全登录设置..... 116
3. Windows XP 系统安全方案..... 119

4.1.3 利用组策略的开机策略..... 122

1. 设置帐户锁定策略..... 122
2. 设置密码策略..... 122
3. 更改默认系统管理员 Administrator 帐户..... 122
4. 设置用户权限..... 123
5. 不允许SAM帐户的匿名枚举..... 123

4.1.4 注册表的开机策略..... 124

1. 隐藏用户登录名..... 124
2. 开机自动进入屏幕保护..... 124
3. 设置Windows 口令的最小长度..... 124
4. 屏蔽从CD-ROM或软盘安装程序..... 124
5. 禁用远程编辑注册表..... 125

4.2 我的系统你别动..... 126

4.2.1 注册表之禁..... 126

1. 禁止显示注销菜单..... 126
2. 禁止使用Windows 默认方式登录..... 126

127	3. 禁止运行修补程序	127
127	4. 禁止 Windows Installer	127
127	5. 禁止从可移动媒体安装程序	127
128	6. 禁止使用“添加/删除程序”程序	128
128	7. 禁止从 CD-ROM 或软盘安装程序	128
129	8. 禁止使用“添加/删除”项中的“添加新程序”	129
129	9. 禁止使用添加/删除项中的“更改或删除程序”	129
130	10. 禁止使用“控制面板”所有设置项目	130
130	11. 禁止使用控制面板中“密码”下的“远程管理”	130
130	12. 禁止使用屏幕保护程序保护选项	130
131	13. 禁用显示面板中的屏幕保护程序设置	131
131	14. 禁止修改桌面主题	131
132	15. 禁止使用控制面板	132
132	16. 禁止使用“网络”属性	132
132	17. 禁止使用控制面板中的“用户”和“密码”设置	132
133	18. 禁止使用 LanMan Hash	133
133	19. 设置当系统从睡眠或挂起状态恢复时是否需要输入密码	133
134	20. 禁止使用打印机共享	134
134	21. 禁止使用“组策略”管理单元	134
135	22. 禁止访问驱动器内容	135
135	23. 禁止使用资源管理器安全选项卡	135
136	24. 禁止使用 MS-DOS 方式	136
136	25. 禁止查看指定磁盘驱动器	136
137	26. 禁止某些指定程序运行	137
137	27. 禁止使用回收站	137
137	28. 禁止使用我的文档	137
137	29. 禁止使用 MMC 管理单元	137
138	30. 禁止使用安全模板管理单元	138
138	31. 禁止使用安全配置和分析管理单元	138
139	32. 禁止使用路由和远程访问管理单元	139
139	33. 禁止使用远程桌面管理单元	139
139	34. 禁止使用本地用户和组管理单元	139
139	35. 禁止使用磁盘管理单元	139
140	36. 禁止使用计算机管理	140
140	37. 禁止使用远程访问管理单元	140
140	38. 禁止使用设备管理器单元	140

39. 禁止使用管理模板（计算机）管理单元	141
40. 禁止使用管理模板（用户）管理单元	141
41. 禁止使用安全措施设置管理单元	141
42. 禁止使用软件安装（计算机）管理单元	142
43. 禁止使用软件安装（用户）管理单元	142
44. 禁止使用组策略管理单元	142
45. 禁止使用远程安装服务	143
46. 禁止使用 Internet Explorer 维护功能	143
4.2.2 组策略之禁	143
1. 用组策略禁止使用文件夹选项	143
2. 禁止更改显示属性	144
3. 禁止更改开始菜单和任务栏	144
4. 禁用注册表管理器	144
5. 限制使用应用程序	145
6. 禁用“添加/删除程序”	146
7. 禁止访问“控制面板”	146
8. 禁止对桌面的某些更改	146
9. 禁止访问指定驱动器	146
10. 禁止建立新的拨号	146
11. 限制 IE 浏览器的保存功能	147
12. 禁止修改 IE 浏览器的主页	147
13. 禁止 IE 插件骚扰	148
4.2.3 使用软件防护系统	148
1. 用 PC 万能防改精灵保护系统	148
2. 用百艺程序锁定器进行程序管理	150

第 5 章 坚壁清野——消灭一切不能泄漏之密 153

5.1 清除隐私	154
5.1.1 你可能泄漏的隐私	154
5.1.2 清除隐私隐患	154
1. 系统操作清痕	154
2. 软件操作清痕	156
3. 网络操作清痕	159

081	4. 使用清理工具清除隐私	160
081	5.2 隐藏资源	161
181	5.2.1 盘符隐藏	161
881	1. 使用注册表隐藏盘符	161
181	2. 使用软件隐藏盘符	163
481	3. 使用磁盘管理隐藏盘符	164
481	5.2.2 文件隐藏	165
481	1. 使用注册表隐藏文件	165
281	2. 用 COPY 命令隐藏文件	166
881	3. 自定义文件夹隐藏文件	166
881	5.2.3 使用工具隐藏资源	167
081	1. 文件夹隐藏大师	167
081	2. 超级文件隐形家 2004	168
081	5.3 铜墙铁壁	170
881	5.3.1 重要文档的保护	170
881	5.3.2 重要文件夹的保护	171
081	5.3.3 用“SIA”对上网隐私的保护	172
001	1. 隐藏上网 IP 地址	172
001	2. 加密收藏夹	174
001	3. 删除上网痕迹	174
101	5.4 全副伪装	175
101	5.4.1 认识类标识符	175
501	1. 设置伪装	176
001	2. 恢复伪装	176
101	5.4.2 用文件夹伪装专家伪装文件夹	177
401	5.5 彻底销毁	178
001	5.5.1 用文件粉碎机将资料彻底删除	178
001	5.5.2 用 File Wipe 粉碎文件	179

5.6	禁用共享	180
5.6.1	取消共享	180
5.6.2	隐藏共享文件夹	181

第6章 软硬兼施——双管齐下防守秘密 183

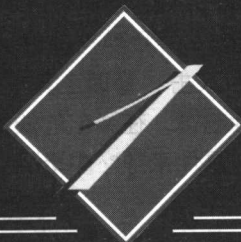
6.1	指纹鼠标器	184
6.1.1	指纹滑鼠的原理解析	184
6.1.2	各种指纹滑鼠产品	185
	1. SecuGen OptiMouse 指纹辨认光学滑鼠	185
	2. PMC 指纹认证鼠标	185
6.2	用身份验证硬件防止资料外泄	186
6.2.1	U盘身份验证	186
6.2.2	用声纹识别保护隐私	188
	1. 声纹识别技术与应用	188
	2. 声纹S锁——数据安全的卫士	189
6.3	硬盘加密	190
6.3.1	硬盘加密的几种方法	190
	1. 修改硬盘分区表信息	190
	2. 对硬盘启动加口令	191
	3. 对硬盘实现用户加密管理	191
	4. 对某个逻辑盘实现写保护	191
6.3.2	用加密卡为硬盘加密	192
	1. 加密卡（锁）是如何工作的	192
	2. 如何使用加密卡（锁）	192
6.3.3	具有硬盘加密技术的主板	194
6.4	做好反盗窃工作	196
6.4.1	使用防盗电脑机箱	196

6.4.2 用USB电脑锁锁电脑	197
1. PC-Lock USB 电脑锁	197
2. ControlKey PC 锁	197
3. iKey USB 加密设备	198
6.4.3 自制电控机械锁	199
1. 需要准备的元件和材料	199
2. 制作步骤	200
6.4.4 笔记本防盗锁	201
1. 钢缆锁 (Cable Lock)	201
2. 扣式锁	202
6.5 监视我的电脑	203
6.5.1 远程摄像监视	203
1. 视频监视种类	203
2. 使用QQ充当监控软件	204
3. 用USB摄像头来做视频监控	206
第7章 有备无患——系统数据备份先行	209
7.1 10种绝版备份	210
7.1.1 BIOS备份	210
1. 主板BIOS的备份与还原	210
2. 显卡BIOS的备份与还原	211
7.1.2 驱动备份	212
7.1.3 硬盘备份	213
1. 硬盘分区表的备份与还原	213
2. 主引导记录的备份与恢复	214
7.1.4 注册表备份	216
1. 备份全部完整的注册表	217
2. 备份单个注册表键	219
7.1.5 IE收藏夹的备份	219
7.1.6 “我的文档”备份	221

7.1.7	OUTLOOK数据的备份	221
1.	对注册表的相关部分备份	221
2.	对目录文件进行备份	222
3.	通讯簿的备份	222
4.	导出个人文件夹 (.pst) 文件数据	223
7.1.8	输入法自定义词组的备份	223
1.	中文五笔输入法中自定义词组的备份	223
2.	智能拼音输入法中自定义词组的备份	224
3.	微软拼音输入法中自定义词组的备份	224
7.1.9	Office 设置备份	225
1.	WPS 设置备份	225
2.	Microsoft Word 设置备份	225
7.1.10	聊天记录备份	226
1.	QQ 聊天记录备份	226
2.	ICQ 数据的备份	227
3.	MSN 自定义图示备份	228
7.2	系统备份工具	229
7.2.1	用WinRescue XP进行系统备份	229
7.2.2	用Folder Watch进行实时备份	230
7.3	数据恢复工具	232
7.3.1	用EasyRecovery恢复数据	232
1.	EasyRecovery 数据修复原理	232
2.	用软件修复还原数据	233
7.3.2	用FinalData恢复数据	237
1.	软件恢复原理	238
2.	用软件恢复数据	238

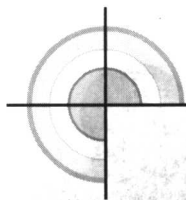


第



章

蛛丝马迹—— 三招两式看谁动过我的电脑



1.1

看看在我的系统上干了什么

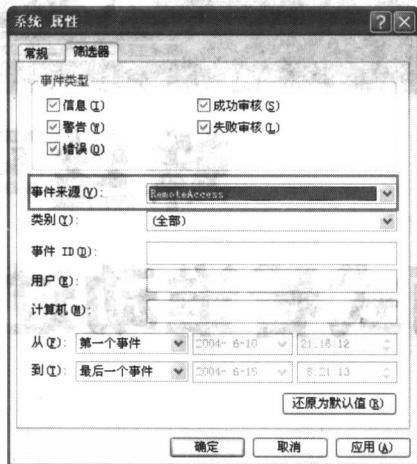
仿照我们大脑的记忆功能，微软也为它的视窗操作系统设计了记忆功能，从启动登录记录，到程序运行记录应有尽有。要查看系统的变动情况，我们总有足够的蛛丝马迹可循，如同案发现场总会留下痕迹，只要你细细搜寻就一定会发现。



1.1.1 用 Windows 事件查看器看使用记录

1. 查看上网时间

在 Windows XP 中，通过“事件查看器”可以查看我们过去的上网时间。方法为：打开“控制面板”，双击“管理工具”，然后打开“事件查看器”。在左侧的窗口中选择“系统”选项，单击鼠标右键，在弹出的快捷菜单中选择“属性”，在“系统属性”窗口中选择“筛选器”选项卡，在“事件来源”中选择“RemoteAccess”，如下图：



查看上网时间

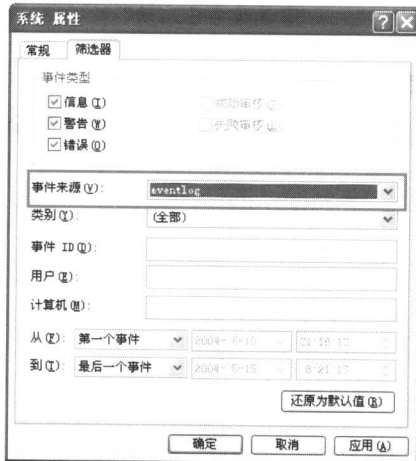
单击“确定”，回到“事件查看器”主窗口，在右边的窗口中就会显示出上网的开始时间和结束时间，相邻的两个时间中较早的就是你开始上网的时间，较晚的则是下线的时间。

2. 查看计算机开关机记录

在Windows XP中,我们可以通过“事件查看器”的事件日志服务查看计算机的开、关机时间。因为事件日志服务会随计算机一起启动和关闭,并在事件日志中留下记录。

在这里有必要介绍两个ID号:6006和6005。在事件查看器里ID号为6006的事件表示事件日志服务已停止,如果你没有在当天的事件查看器中发现这个ID号为6006的事件,那么就表示计算机没有正常关机,可能是因为系统原因或者直接按下了计算机电源键,没有执行正常的关机操作造成的。当你启动系统的时候,事件查看器的事件日志服务就会启动,这就是ID号为6005的事件。

通过这两个ID号保存的信息,我们可以轻松查看计算机开、关机记录。方法为:打开“控制面板”,双击“管理工具”,然后打开“事件查看器”,在左边的窗口中选择“系统”选项。单击鼠标右键,在弹出的快捷菜单中选择“属性”,在打开的“系统属性”窗口中选择“筛选器”选项卡,在“事件来源”列表中选择“eventlog”选项,如下图:



查看计算机开关机记录

继续设定其他条件后,单击“确定”,即可看到需要的事件记录了。双击某条记录,如果描述信息为“事件服务已启动”,那就代表计算机开机或重新启动的时间,如果描述信息是“事件服务已停止”,即代表计算机的关机时间,如下图: