

警惕免费的午餐，保护个人与公司的知识财富

读者对象：

本书是一本讲述安全使用个人电脑的普及读物，适合广大初、中级电脑用户阅读参考，既可作为普通电脑用户提高电脑安全防范意识、补充电脑安全知识的指导书籍，也可供大中专院校有关专业的在校学生作为辅助教材。

主要内容：

电脑的开机安全

密码设置与管理

数据加密与数字签名

数据备份与恢复

捍卫个人电脑隐私

局域网中共享资源的保护

安全使用 Office 办公软件

IE 遭遇攻击后的修复

安全的浏览网页

E-mail 的安全措施

QQ 软件攻防战

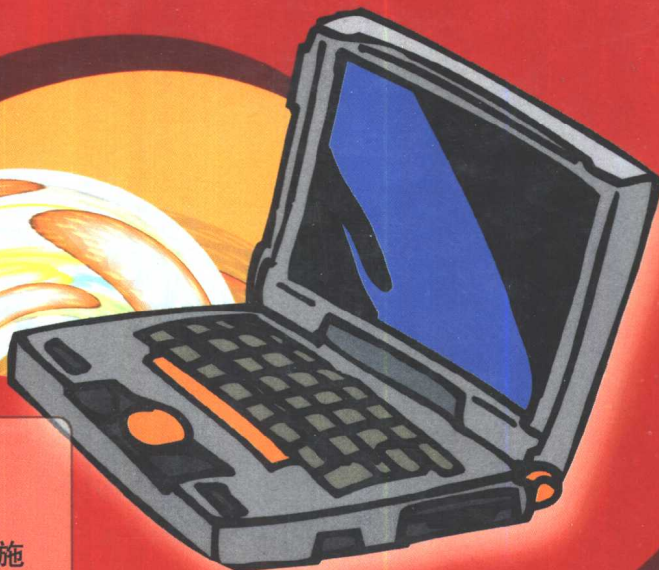
防御可怕的木马攻击

计算机典型病毒防治

个人电脑操作安全

安全屏障——防火墙

电脑的监控与反监控



谁动了我的电脑

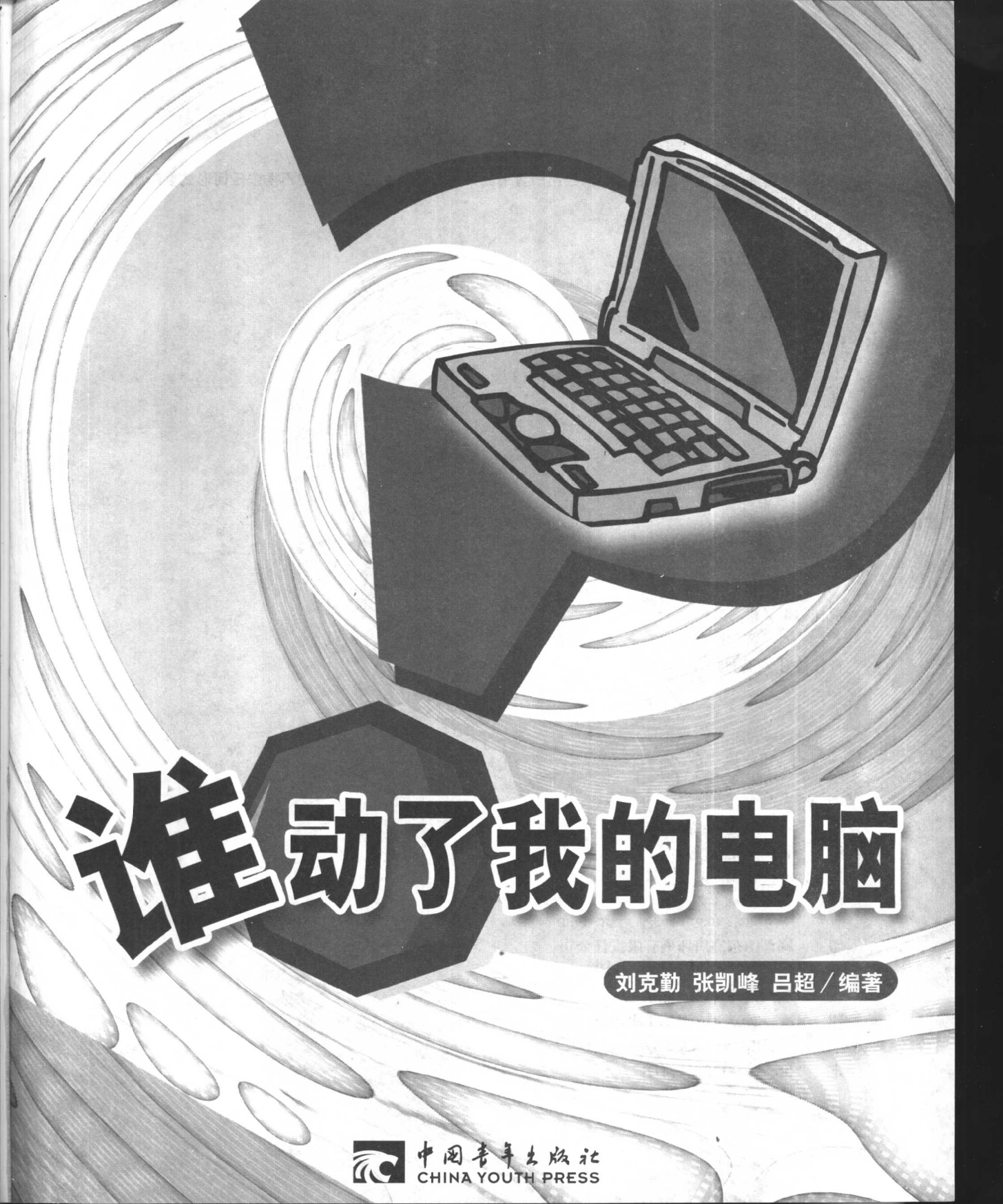
刘克勤 张凯峰 吕超 / 编著



本书附赠光盘内含各章涉及的国内外常用安全软件与相关资料



中国青年出版社



谁动了我的电脑

刘克勤 张凯峰 吕超 / 编著



中国青年出版社
CHINA YOUTH PRESS

(京)新登字 083 号

本书由中国青年出版社独家出版。未经出版者书面许可,任何单位和个人不得以任何形式复制或传播本书的部分或全部。

图书在版编目(CIP)数据

谁动了我的电脑? / 刘克勤等编著. — 北京: 中国青年出版社, 2003

ISBN 7-5006-4983-5

I. 谁... II. 刘... III. 电子计算机 — 安全技术 IV. TP309

中国版本图书馆 CIP 数据核字(2002)第 105858 号

总 策 划 / 胡 守 文

王 修 文

郭 光

责任编辑 / 肖 辉

黄 谊

责任校对 / 王志红

书 名: 谁动了我的电脑?

编 著: 刘克勤 等

出版发行: 中国青年出版社

地址: 北京市东四十二条 21 号 邮政编码: 100007

电话: (010) 84015588 传真: (010) 64053266

印 刷: 山东高唐印刷有限责任公司

开 本: 787 × 1092 1/16 印张: 27.5

版 次: 2003 年 2 月北京第 1 版

印 次: 2003 年 2 月第 1 次印刷

书 号: ISBN 7-5006-4983-5/TP · 295

定 价: 39.90 元 (ICD)

前言



随着人类步入 21 世纪，电脑已经成为我们日常工作、生活中不可替代的有力工具。同时伴随着电脑的普及、网络技术的发展，人们已经不满足于“孤立”电脑的使用，而是想通过网络实现信息的交互和资源的共享。但是，任何事情都有其两面性，电脑、网络在为我们提供帮助和便利的同时，也为那些不法之徒入侵我们的电脑、盗取我们的隐私、破坏我们的数据打开了方便之门。可以说信息安全问题与能源问题、人口问题、环境问题一样，已经成为摆在人类面前需要迫切解决的问题之一。

有这么严重吗？这可能是大多数读者共同的疑问。但事实上，可能要比我们想像的严重得多。如果您是一个地地道道的电脑用户，面临这些安全问题是无疑的。如果您不经常使用电脑，那么只要您使用手机联络亲友，用 MP3 随身听欣赏音乐，使用数字摄像机拍摄影片，驾驶带有全球定位系统的轿车，甚至在家里使用微波炉做饭，都有可能与个人隐私和安全隐患沾上边。这可不是耸人听闻，有些读者可能已经遇到过类似的问题了。

目前市面上关于信息安全、黑客攻击的书籍足以让人眼花缭乱，其中大部分都是为网络专家、安全专家那些专业人士所准备的，却很少关照电脑的普通用户，而往往电脑的初、中级用户却是安全问题的最大受害者。大部分书都沿用“从技术角度出发，由技术、原理及漏洞引出安全隐患，随之介绍防御方法和功能软件”的写作模式，这样就要求读者要对信息安全的概念有一个清楚地认识和具备扎实的计算机理论知识，显然，这不太适合广大计算机普通用户阅读。而本书立足于计算机的大众用户，紧紧抓住隐私保护与电脑安全这两个中心，以通俗的语言和清晰的表述，向广大读者介绍了计算机系统的安全知识和有关应用实例及软件实用技术，并从实际操作出发，用具体的实例引出信息安全的相关概念，力图用简单、有效的方法解决用户所面临的实际安全问题。希望通过阅读本书可以帮助读者建立起电脑隐私保护、安全防范意识及应对突发危急事件的能力。

全书共分为 20 章，每章一个主题，本书的一个亮点即是每个主题帮您解决一个面临的实际安全问题。具体内容涉及开机安全、密码设置与管理、数据加密技术、数据备份与恢复、个人隐私保护、局域网安全、Office 办公资料的保护、浏览器的攻击与防御、安全收发电子邮件、



QQ 安全问题、木马攻击、病毒防护、电脑硬件操作安全、防火墙技术，以及监控与反监控的方法、工具介绍等。本书的另一个亮点在于提出了个人电脑隐私保护的观点，在整本书的写作中都贯穿了这一思想，目的在于提高读者自身的安全、保护意识，也许电脑已经变成了告密者，您的操作直接决定了它们到底站在哪一方？

本书是集体智慧的结晶，我们的许多研究生参加了编写工作。其中徐洪斌参加了第 1、2、5、6、8 章的编写，李莉敏参加了第 3、4、19 章的编写，张凯峰参加了第 7、10、11、13、18 章的编写，林媛媛参加了第 14、15、17 章的编写，常新苗参加了第 16 章的编写，吕超参加了第 9、12、20 章的编写工作。

本书适合广大初、中级计算机用户阅读、参考，既可作为普通电脑用户提高电脑安全防范意识、补充电脑安全知识的指导读物，也可供大中专院校有关专业的在校学生作为辅助教材。在向读者推荐本书的同时，我们也认识到计算机系统安全技术发展十分迅速，以我们的现有水平很难将所有计算机安全问题在书中全面、准确地反映出来，因此书中难免会有疏漏、错误之处，在此恳请读者及有关专家批评指正。

刘克勤

2002 年 12 月 于华北电力大学（北京）

目 录

第1章 警惕免费午餐

- 1.1 我的电脑怎么了? 2
- 1.2 故障分析 2
- 1.3 模拟攻击实例 4

第2章 掀开电脑安全的神秘面纱

- 2.1 基本知识 12
- 2.2 谁“威胁”着我的电脑 13
 - 2.2.1 黑客 13
 - 2.2.2 病毒 14
 - 2.2.3 木马 14
 - 2.2.4 蠕虫 15
 - 2.2.5 陷门 16
 - 2.2.6 信息泄露 16
- 2.3 基本安全技术 16
 - 2.3.1 身份鉴别 16
 - 2.3.2 存取控制 17
 - 2.3.3 完整性验证 17
 - 2.3.4 加密 17
 - 2.3.5 防火墙 18

第3章 安全第一关——CMOS 密码设置与破解

- 3.1 认识BIOS和CMOS 20
 - 3.1.1 BIOS 20
 - 3.1.2 CMOS 21
 - 3.1.3 BIOS 和 CMOS 的区别 21
- 3.2 开机密码 21
 - 3.2.1 设置 21
 - 3.2.2 破解 23

第4章 守好你的大门—— 密码设置

- 4.1 Windows操作系统密码 30
 - 4.1.1 Windows 登录密码 30
 - 4.1.2 电源管理密码 43
 - 4.1.3 屏幕保护程序密码 44
 - 4.1.4 用注册表限制密码格式 46
- 4.2 密码巧设置 46
 - 4.2.1 正确设置密码的原则 47
 - 4.2.2 巧记巧存密码 47



第5章 数据加密与数字签名

5.1 利用PGP进行数据加密和数字签名	52
5.1.1 数据加密概述	52
5.1.2 PGP 加密流程	52
5.1.3 PGP 密钥的生成	53
5.1.4 利用 PGP 加密文件	56
5.1.5 通过网络安全传输加密文件	57
5.1.6 利用 PGP 加密当前文本窗口	59
5.1.7 利用 PGP 对剪贴板进行加密	60
5.1.8 利用 PGP 进行数字签名	61
5.2 利用WinXFiles进行文件加密	64

第6章 数据备份与恢复

6.1 系统信息的备份与恢复	70
6.1.1 Windows 注册表的备份与恢复	70
6.1.2 硬件配置文件的备份	72
6.1.3 紧急修复盘的建立	73
6.1.4 整个系统的备份与恢复	74
6.2 普通文件与文件夹的备份与恢复	74
6.2.1 普通文件和文件夹的备份	74
6.2.2 普通文件和文件夹的恢复	77
6.3 常用备份与恢复工具	78
6.3.1 利用 FolderWatch 进行文件夹的备份	78
6.3.2 利用 FinalData 进行数据恢复	81

第7章 捍卫个人绝对隐私

7.1 手动保护系统隐私	86
7.2 网上保护个人隐私	91
7.3 补救IE隐私漏洞	93
7.3.1 Cookie, 网络上的小甜饼	93
7.3.2 IE 访问FTP 站点时的漏洞	99
7.3.3 IE 图像 URL 重定向漏洞	99
7.3.4 通过 IE 查看文件的漏洞	99
7.3.5 IE6 “隐私报告”安全漏洞	100
7.4 消除电脑操作痕迹	100
7.4.1 如何手工消除系统操作的痕迹	100
7.4.2 如何手工消除软件操作的痕迹	104
7.4.3 如何手工消除网络操作的痕迹	105
7.5 隐私保护软件简介	110
7.5.1 隐私保护神	110
7.5.2 绝对隐私保护者 SurfSecret	111

第8章 局域网中共享资源的保护

8.1 解析“网上邻居”的工作原理	120
8.2 共享资源的设置	120
8.3 共享原理剖析	124
8.4 安全防范技巧	125
8.4.1 利用带密码的只读共享保护共享资源	125
8.4.2 利用“\$”隐藏共享资源	125
8.4.3 利用“用户级访问控制”保护	



共享资源	127
8.4.4 不要轻易将打印机共享	128
8.4.5 通过禁止编辑注册表保护共享资源	128
8.4.6 通过编辑注册表禁止文件共享	129
8.4.7 利用“网络监视器”管理共享资源	129
8.4.8 为 Windows 2000/XP 设一个好的管理员密码	132

第9章 Office办公软件的安全

9.1 WPS Office加密	136
9.2 Word 的安全防范	137
9.2.1 隐藏和躲避	137
9.2.2 Word 密码设置	139
9.2.3 其他安全措施和技巧	143
9.3 Excel 的安全防范	144
9.3.1 Excel 的加密	145
9.3.2 Excel 的解密	147
9.3.3 Excel 的数据保护	147
9.4 保护 Access 数据库安全	150
9.4.1 数据库的安全管理	151
9.4.2 设置和修改用户与组的权限和账号	153
9.5 压缩软件 WinZip 和 WinRAR 的加密技巧	156
9.5.1 WinZip	156
9.5.2 WinRAR	157

9.6 破解PDF文档	158
9.7 微软Office文件恢复及数据备份技巧	159

第10章 谁动了我的IE

10.1 修复IE的页面显示	162
10.1.1 修复IE的标题栏	162
10.1.2 修复IE的打开页面	165
10.1.3 恢复默认页的设置功能	167
10.2 修复IE快捷菜单	168
10.2.1 清除右键菜单中的网址	168
10.2.2 恢复查看源代码功能	170
10.3 修复IE窗口显示	171
10.4 修复IE地址栏	173
10.5 修复IE的默认设置	173
10.6 修复被篡改的IE默认搜索引擎	175
10.7 修复网页篡改的系统设置	177
10.8 时刻防范恶意代码修改你的IE	181

第11章 网站浏览安全

11.1 美萍反黄专家	184
11.2 网站过滤专家	190
11.3 广告杀手	191
11.4 广告窗口终结者	193
11.5 Ad-aware Plus	193



11.6 PopUp Killer	195
11.7 NoAds	197

第12章 E-mail的安全使用

12.1 E-mail的实现	200
12.2 E-mail的安全问题及解决办法··	201
12.2.1 Web 信箱	201
12.2.2 防火墙	201
12.2.3 E-mail 炸弹	202
12.2.4 E-mail 乱码	203
12.2.5 同E-mail有关的病毒	203
12.2.6 其他漏洞	203
12.3 Outlook Express安全电子 邮件	204
12.3.1 Outlook Express 用户密码的 设置	204
12.3.2 加密邮件的设置与发送	206
12.3.3 Outlook Express 邮件的安全 措施	209
12.4 安全使用FoxMail	213
12.4.1 建立FoxMail 账户	213
12.4.2 对账户和邮箱进行加密	216
12.4.3 Foxmail 的安全隐患	217
12.4.4 口令被破的后果	218
12.4.5 防范的方法	221
12.4.6 FoxMail 的其他使用技巧	222

第13章 聊天的安全

13.1 ICQ聊天的安全问题	226
13.2 mIRC聊天的安全问题	228
13.3 Web聊天的安全问题	230

第14章 QQ软件安全

14.1 QQ软件常识	234
14.1.1 什么是QQ	234
14.1.2 QQ 的工作原理	234
14.2 保护好你的QQ密码	236
14.2.1 怎样设置安全的QQ 密码	236
14.2.2 如何防止QQ 密码被破译	237
14.2.3 防范QQ 木马	238
14.2.4 使用软件保护你的QQ	239
14.2.5 当心QQ 骗子	243
14.3 防范IP探测	244
14.4 防范QQ炸弹攻击	247
14.4.1 QQ 炸弹的攻击原理	247
14.4.2 怎样防范QQ 炸弹	249
14.5 QQ个人信息的保护与备份	250
14.5.1 QQ 个人信息的保护	250
14.5.2 如何手工备份QQ 数据	251
14.5.3 QQ 资料备份软件——爱Q精灵··	252
14.6 QQ安全小技巧	254
14.6.1 如何删除多余的QQ 登录号码 ···	254



谁动了我的电脑

14.6.2 改变 QQ 默认端口	256
-------------------------	-----

第15章 木马

15.1 何谓“木马”	260
15.2 木马工作的原理	260
15.2.1 木马的隐身方式	260
15.2.2 木马的特性	263
15.3 我中奖了吗?——木马的检测 ...	263
15.4 几种常见的木马及清除	268
15.4.1 冰河	268
15.4.2 黑洞 2001	270
15.4.3 网络精灵	271
15.4.4 超级黑客 BO2000	271
15.4.5 网络神偷	272
15.4.6 广外女生	273
15.4.7 聪明基因	273
15.4.8 GOP 木马	274
15.4.9 其他木马的清除	275
15.5 怎样防范木马	279
15.6 使用软件清除木马	279
15.6.1 木马杀手——The Cleaner	279
15.6.2 木马克星——IParmor	284
15.6.3 木马终结者	286

16.1.2 计算机病毒的特征	290
16.1.3 计算机病毒的破坏行为	292
16.2 如何判断自己的计算机是否感染了病毒	293
16.3 计算机病毒的工作机制	296
16.3.1 病毒的引导机制	296
16.3.2 计算机病毒的传染机制	297
16.3.3 计算机病毒的触发机制	299
16.3.4 计算机病毒的破坏机制	300
16.3.5 病毒如何隐藏自己	300
16.4 如何防治计算机病毒	301
16.4.1 个人注意事项	301
16.4.2 技术预防措施	303
16.4.3 杀毒的方法技巧和注意事项	304
16.5 一些典型病毒及其防治	307
16.5.1 CIH 病毒	307
16.5.2 宏病毒	312
16.5.3 网络蠕虫病毒	316
16.5.4 近期常见热门病毒的识别与防治 ...	322
16.6 反病毒软件介绍	334
16.6.1 当今流行的反病毒软件	335
16.6.2 反病毒软件搭配方案	336
16.6.3 瑞星杀毒软件 2002 版的安装和设置	337

第16章 计算机病毒防治

16.1 走近计算机病毒	290
16.1.1 什么是计算机病毒	290

第17章 其他网络攻击

17.1 警惕网页黑手	344
17.2 小心炸弹攻击	348





17.2.1 邮件炸弹	348
17.2.2 QQ炸弹	352
17.2.3 新闻组炸弹	352
17.2.4 聊天室炸弹	353
17.2.5 混客绝情炸弹	353
17.3 拒绝服务攻击和DDoS攻击 ...	355
17.3.1 拒绝服务攻击	355
17.3.2 DDoS攻击	355
17.4 缓冲区溢出	357

第18章 个人电脑操作安全

18.1 硬盘操作安全	360
18.1.1 怎样安装双硬盘	360
18.1.2 何谓硬盘分区表?	361
18.1.3 硬盘分区表的备份和修复	361
18.1.4 主引导记录的备份和修复	364
18.1.5 未雨绸缪,防患未然	364
18.1.6 硬盘坏道及修复方法	365
18.1.7 USB移动硬盘的使用	371
18.2 光驱操作安全	372
18.2.1 光驱的不当操作	372
18.2.2 光驱的日常维护	373
18.3 显卡/声卡操作安全	374
18.4 显示器操作安全	375
18.5 内存操作安全	376
18.6 Modem操作安全	376
18.7 软驱操作安全	377

第19章 网上冲浪的安全屏障—— 个人防火墙

19.1 你的PC需要防火墙吗	380
19.2 防火墙简介	381
19.2.1 何为防火墙	381
19.2.2 防火墙如何工作	382
19.2.3 个人防火墙的主要功能	383
19.3 如何选购个人防火墙	384
19.3.1 选择原则	384
19.3.2 几款常用个人防火墙简介	386
19.4 网络知识初步	387
19.5 阻止黑客的防线——天网个人 防火墙的使用	389
19.5.1 安装和注册	389
19.5.2 使用说明	390
19.5.3 规则设置	394
19.5.4 天网安全检测修复系统	397
19.6 防黑工具BlackICE Defender 的使用	397
19.6.1 下载与安装	398
19.6.2 使用说明	399
19.7 高效实用的网络安全伙伴Zone Alarm	405
19.7.1 下载和安装	405
19.7.2 使用说明	406
19.8 Norton Internet Security 2001 (家庭版)使用简介	412





第20章 监控与反监控

20.1 监视活动	418
20.1.1 监视的目的	418
20.1.2 监视方法	418
20.2 反监视的技巧和方法	421

20.2.1 将被侵入的系统从网络上断开 ...	421
20.2.2 备份被侵入的系统	421
20.2.3 入侵分析	421
20.2.4 恢复系统	424
20.2.5 加强系统和网络的安全	425
20.3 监视软件	425

谁
动了
我的
电脑



警惕免费午餐

近年来，Internet 在我国有了飞速的发展。上网冲浪仿佛成了当今的一种时尚。可是，网民也同现实社会中的人一样，良莠不齐。朋友们可曾遇到过这样的情况——当你正在聊天室里高谈阔论时突然被莫名其妙地“踢”出聊天室；使用从网上下载的软件后发现自己的电脑变得不那么“听话”了；最要命的情况是，当你交网费的时候发现拿到的是天文数字的账单，所有的这些迹象表明你受到了网上的非法侵害。面对着这些你无法容忍的侵害行为，许多初级网友只能暗气暗憋，毫无招架之功。不过，我劝这些朋友不要气馁。正所谓“千里之行，始于足下”，我相信在读了本书之后，你就会对电脑安全有一个初步的认识了。好了，不再讲这些空话浪费大家宝贵的时间了，现在就让我们从一个入侵实例开始，步入个人电脑安全的神秘殿堂吧！

本章主要内容：

- 我的电脑怎么了？
- 故障分析
- 模拟攻击实例



1.1 我的电脑怎么了？

许多网友在上网时可能会遇到这样的情况——自己刚从网上下载了一幅美丽的图片，或发现自己的电子信箱里有一封匿名邮件，打开后渐渐发觉一向对你“唯命是从”的“爱机”仿佛此刻不再听命于你。有时你明明要打开一个文本文件，可它偏偏却要打开另一个图片文件；有时你可能会发现自己的重要文件“神秘”地不翼而飞了；更糟糕的是，有时只要你一上网，电脑就会不断地重新启动，害得你无法享受冲浪的快感，而不上网时，电脑又变回了你亲密的朋友。

1.2 故障分析

面对这一系列的“不解之谜”，缺乏电脑基础知识的朋友的第一反应就是——电脑坏了。其实，电脑硬件出现故障的几率是非常小的，有的朋友自从买了电脑到几年后升级换代，都不曾光临过电脑维修部。电脑故障的大部分原因都是由于用户的不当操作或是软件本身的 Bug 所致。更何况这些故障都是在你上网的时候才发生，这一点就提醒了我们，故障肯定与网络有关。误操作亦或是软件 Bug？仔细回想一下，也不像，若是的话，故障现象应该一致，而且也不应该是时有时无的。那么，回想到所有的故障都是在你第一次打开了那张图片或那封匿名信后发生的，所以那张图片或匿名信才应该是罪魁祸首。



Bug 是对软件漏洞的一种说法。

有一些电脑基础的朋友可能马上会说：“是病毒作祟！”，的确有这个可能。在如今的网络环境中，安全机制还不是很健全，当病毒被释放到网络中的时候，你根本无法也不能预测到它的扩散能力有多么强。再加上如今的电脑病毒花样不断翻新，有的病毒可以让你拒绝服务、有的病毒可以损坏你的数据、有的病毒可以把你的 PC 变成“公用”的、而有的病毒可以让你的 PC 进入坟墓……。所以，拥有一套良好的杀毒软件（如金山毒霸、瑞星等）并定期为自己的电脑“消毒”不失为一个明智之举。但你千万不要为自己拥有一套性能优越的杀毒软件而沾沾自喜，我想告诉你的是病毒程序总是走在反病



毒工具的前面，你不要完全依赖杀毒程序为你查杀一切病毒。关于几种流行电脑病毒的机理及查杀办法，我们会在专门的章节里向你阐明，在此我们不做过多的解释。

除了电脑病毒之外，最有可能的原因就是黑客入侵。

提示

在英文原意里，Hacker（黑客）最初的意思是指一类计算机高手，这类人有喜欢研究系统漏洞的嗜好，他们并不入侵别人的系统；而真正入侵别人系统的人被叫作 Cracker（骇客）。

其实，黑客也分为初级黑客和高级黑客，大多数的初级黑客多是利用网上提供的现成的黑客工具来入侵他人系统，此系统多是个人用户的电脑。因为多数现成的黑客工具都已被现有的杀毒工具或防火墙系统所封杀，利用这些工具入侵大型服务器系统，其成功的可能性几乎是微乎其微的。而且多数个人用户的安全意识并不是很高，至今仍有许多网友没有为自己的电脑装上个人防火墙系统。因此，个人电脑系统自然而然成了这些初级黑客的首选。而真正的黑客高手是耻于入侵个人电脑的，他们往往利用自己编写的入侵程序侵入拥有大量有用信息的服务器系统，只有这样才能满足他们的欲望。

知道了这些后，朋友们也许会问：“那么，那些初级黑客是利用什么工具入侵的我的系统呢？”其实，现有的入侵工具数量非常多，但其基本原理大都是利用木马来实现。

木马，又名特洛伊木马，它是一种基于远程控制的黑客工具，当黑客骗取你下载并执行了含有木马的程序后，它就潜入你的电脑系统，通过种种隐蔽的方式在系统启动时自动加载并在后台执行，通过客户 / 服务器模式，以“里应外合”的工作方式，达到当你上网时控制你的电脑，窃取你的密码、游览你的硬盘资源，修改你的文件或注册表、偷看你的邮件等目的。

!! 注意

在客户 / 服务器模式中，我们将请求服务的一方称为客户，将提供某种服务的一方称为服务器。客户提出请求发送给服务器，服务器响应客户请求并提供相应的服务。

谁
动了
我的
电脑





基于这种模式的应用程序都由客户端程序和服务器端程序组成，木马就是这样的一种程序。发送给别人执行的就是服务器端程序，而自己则利用客户端程序与服务器端程序取得联系，从而获得相应的“服务”。

1.3 模拟攻击实例

了解了木马的概念后，你一定会对木马产生极大的好奇心吧。好吧，那就让我们以一个实际的木马为例，模拟一次木马攻击，让你见识一下木马的威力。（此实例仅供我们学习之用，若以此攻击其他网友，所产生的一切后果，笔者概不负责。）

我们此次模拟所用的木马程序叫做“网络精灵”，目前它的最高版本为 3.0 版，相信在网上你一定能够找到它，赶快下载一个吧。（不过下载的时候一定要打开个人防火墙哟，否则，下载木马却中了别人的木马，那真是一种讽刺呀。）为了让大家看清楚木马的整个工作过程，我们这次在局域网的环境中模拟，此时木马的工作原理等同于 Internet 环境。

好了，首先将下载的木马解压缩（不要告诉我你不会解压缩，若真的不会，在网上找找相关资料学习一下吧）。解压后，你会在解压的文件夹内找到 `netmonitor.exe` 和 `netspy.exe` 两个文件。其中，`netmonitor` 为“网络精灵”的客户端程序，也就是你用来控制别人系统的工具，而 `netspy` 则为“网络精灵”的服务器端程序也就是你要发送给别人，要别人来运行的程序。你可千万不要在你的机器上运行它呀，否则你就会为自己的电脑“种”上木马。

下一步就是要把“网络精灵”的服务器端程序 `netspy` 发送给你想控制的电脑。在这里，我们直接把 `netspy` 拷贝到另一电脑 C 盘根目录下。当然，这在实际的 Internet 环境中是不可能做到的。现实中，黑客们经常将木马的服务器端程序与另一个应用程序文件（如当今流行的游戏或好看的美眉照片）利用文件合成软件进行合成，再配上一个好看的图标，然后哄骗我们这些善良的网友下载这样的程序。这样，大部分网友都不会注意到木马的存在。当然，这也要以对方的系统中没有安装防火墙为前提，如果有防火墙，“网络精灵”就会被封杀在系统之外。由此可见防火墙在个人电脑安全领域中的重要性。如果不幸你没有防火墙，那么，只要你运行了刚刚下载的程序，“网络精灵”就会悄悄地潜入你的系统，而且，在你每次启动系统时，它都会自动加载并在后台运行，即使在 Windows 2000 / XP 的任务管理器中也不能找到它的踪影。怎么样，够隐蔽吧！



谁动了我的电脑

为了清楚地向朋友们展示 netspy 程序是如何在你的系统中隐藏的，我们这里没有将之合并到其他文件中，试着在目标计算机上（没有 netmonitor 程序的计算机）运行一下 netspy 程序（双击图标），你会惊奇的发现，它的图标“神秘”的消失了。那么它到底“跑”到哪里去了呢？我们用 Windows 的查找工具来查找一下，单击“开始/搜索/文件或文件夹”，出现图 1-1 所示的查找结果。

此时，我们发现它自动地“跑”到了 C:\WINDOWS\SYSTEM 目录下。这是在 Windows 98 系统上的结果，若是 Windows 2000 / XP 结果会有所不同。好，我们进入 C:\WINDOWS\SYSTEM 目录看一看，结果正如我们所料，它确实在那里。

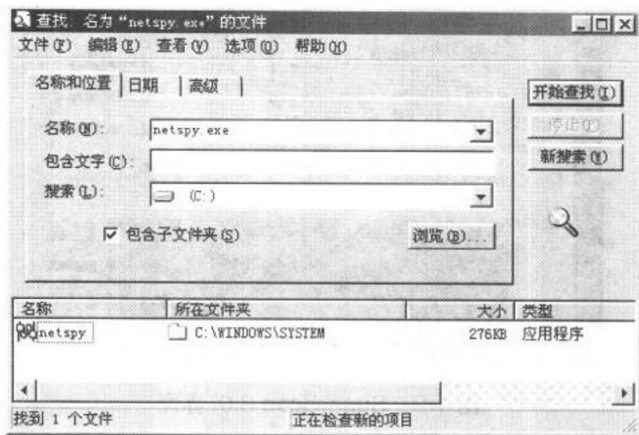


图 1-1 Windows 查找工具

好了，此时我们的木马“网络精灵”已“安全”潜入目标计算机。接下来我们要做的工作就是端口扫描。

提示

如果我们把 Internet 比作路，而你的个人电脑比作路边的房屋，那么端口就是你房屋的门，只有通过门，你才能从屋里上路。我们的电脑可以有 256×256 扇门，即从 0 到 65535 号，每一个号都是一个端口。

什么？你问为什么要进行端口扫描？答案当然是要从端口进入你的电脑。由于我们的电脑有 256×256 个端口，但只有当某一端口被打开时，黑客才能从这一端口进入你