电脑报 总策划

连续9年畅销的精品速查口袋书！

电脑宝贝 PC Baby

“PC宝贝”系列图书汇集电脑操作技巧精髓，精心整理最新最实用的电脑应用技巧，帮助读者解决最急最需的疑难问题，是电脑用户必备的速查好帮手。

◎随身带 ◎随时学 ◎随时用

黑客攻防实例与技巧随手查

仲治国 薛淑妙 编

- 网页挂马攻防实例
- QQ、邮箱攻防实例
- 病毒查杀与进程攻防
- 漏洞与端口的攻防技巧
- 木马攻防与远程控制实例

实用操作技巧 7大类300条黑客实例 + 正版杀毒软件 免费使用90天 + 超值电子书 电脑办公技巧速查

书+光盘+附赠=绝对超值的学习套餐

电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

黑客攻防实例与技巧随手查

仲治国 薛淑妙 编

电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

内容提要

本手册采用实例的形式为大家详细地剖析了黑客的攻防手段和攻防要领，同时也讲解了相应的防范方法。主要内容包括聊天软件攻防实例、病毒查杀与进程攻防、端口扫描与欺骗实例、木马攻防与远程控制、加密与解密、漏洞攻防、其他攻防技巧等。在内容选取上非常全面，涉及黑客攻防的方方面面，只要一本，就可以让你完全掌握黑客攻防技术。

光盘要目

- ESET NOD32安全套装
- 杀毒防黑软件精华库
- 黑客攻防技巧速查
- Office 2007办公技巧速查

黑客攻防实例与技巧随手查

编　　者：仲治国　薛淑妙
责任编辑：连　果
责任校对：钟　卫
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
读者服务：023-63658888-13117
对外合作：023-63658933
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：四川省蓥山数码科技有限公司
文本印刷：重庆升光电力印务有限公司
开本规格：880mm × 1230mm 1/56　5印张　70千字
版 本 号：ISBN 978-7-89476-430-0
版　　次：2010年8月第1版　2010年8月第1次印刷
定　　价：13.80元(1CD+配套手册)

前 言

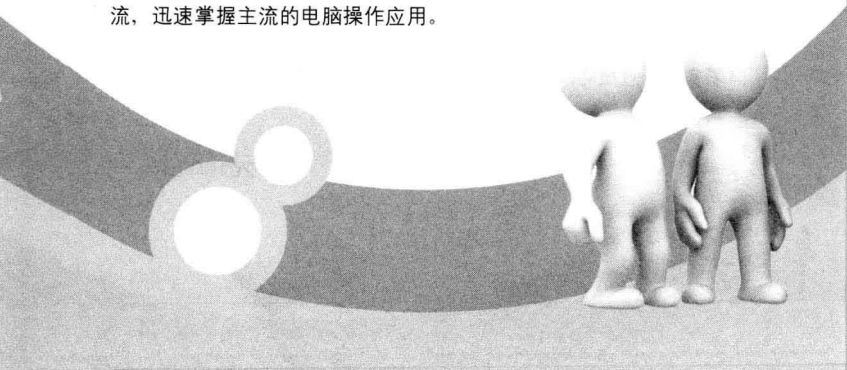
实例技巧 即查即用

PC宝贝系列小开本图书自2002年初版以来，以其丰富的内容，详尽的实例，实用的技巧，以及独具特色的开本受到了广大电脑用户的喜爱，总发行量已达100万册！不仅如此，PC宝贝系列图书还带动了图书出版市场上小开本图书的热潮，众多领域的图书争相采取这种便于读者阅读和携带的开本，该系列图书迅速赢得了众多粉丝的追捧。

2010年，PC宝贝系列图书编辑团队不断创新，从读者的实际需求和使用习惯出发，将该系列图书再次改版，使其无论从实用性、速查性、美观性、便携性等多方面，都超越了往年的版本，为读者奉上了一套新颖、实用、全面、便携的工具宝典。

● 精选热点 崇尚实用

本版系列丛书经过了编辑与专家作者的多次讨论，精心挑选了电脑领域最新、最实用的应用热点。每一个分册都是该领域最受关注的应用热点，这样才能帮助读者掌握最新的电脑应用技巧，紧跟电脑应用潮流，迅速掌握主流的电脑操作应用。



● **实例技巧 强化操作**

本系列丛书不再采用教程的方式讲解，而是将全书的知识点全部以实例、技巧的形式展现出来，便于读者在遇到问题时随用随查，方便快捷。每个技巧实例中多用操作性强的步骤形式来展现，读者逐步操作，易学易用，提高效率。

● **双色图文 轻松阅读**

本系列丛书图文并茂，采用双色印刷，让读者可以轻松阅读，激发学习兴趣，减轻阅读疲劳，使之成为耐用、耐看的工具收藏宝典。

● **全新开本 随手携带**

根据读者对本系列丛书的反馈意见，我们调整了图书开本，使其从翻阅不便的开本，改变为既便携又能轻松翻阅的56开，便于大家使用。读者的阅读感受，正是我们孜孜不倦的追求。

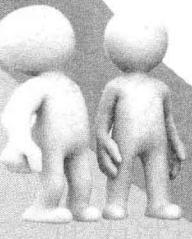
● **超值光盘 精美收藏**

本系列丛书的每个分册都配有一张迷你小光盘，该光盘内容丰富，设计精美时尚。每套光盘中配有丰富的配套软件，并提供视频、音频、网页、桌面屏保、图片等多种形式的资源，实为读者阅读的好伴侣。

看实例、查技巧，活用电脑，必备PC宝贝2010!

编者

2010年8月



目录 CONTENTS

第 1 章 聊天软件攻防实例

第 2 章 病毒查杀与进程攻防

第1章

聊天软件攻防实例

当心“爱Q大盗”盗取 QQ

解析QQ终结者在线盗号

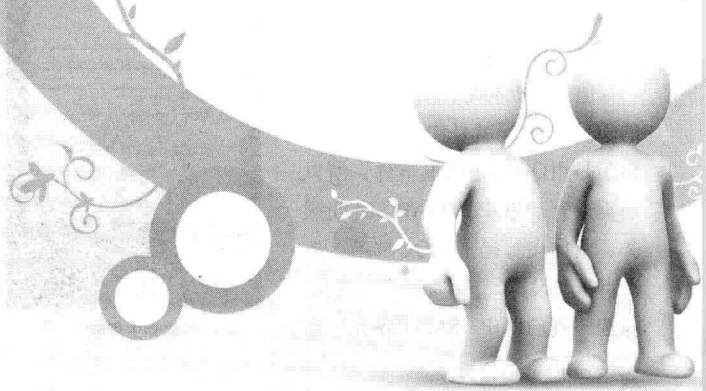
申请密码保护

支付宝安全设置

解读MSN密码被盗

MSN保护盾打造安全环境

……



1.1 QQ攻防实例

例1：当心“爱Q大盗”盗取 QQ

QQ盗取的话题一直受大家高度关注，话不多说，我们直奔主题。由于QQ版本不断更新，因此老点的盗取QQ的工具总会很快失效，针对QQ 2009，这里为大家奉上“爱Q大盗”，软件比较小，能够完美“嗅探”QQ2008和QQ2009，包括QQ2010体验版。以下测试中以QQ 2009 SP3版本为例。

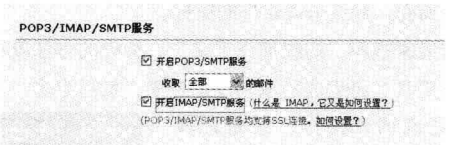
1.配置QQ木马

首先运行“爱Q大盗”，在主界面中，只要设置好收信箱、发信箱，然后输入用户名、密码、发信服务器即可，需要注意的是，目前这款软件只支持QQ邮箱。

值得一提的是，用户名就是你的QQ号，密码就是你的QQ密码，由于是用QQ邮箱收取信件，所以还需要开启POP3/IMAP/SMTP服务，具体设置是进入QQ邮箱，依次点击“设置”、“账户”，然后勾选“开启POP3/SMTP服务”和

软件主界面

“开启IMAP/SMTP服务”。



选项设置

开启相应的服务，并设置好相应选项后，点击“测试发信”按钮，将会提示“测试成功”。

与此同时，你的QQ邮箱将会收到一封测试成功的邮件，内容为“Successed！”。

成功提示

2.突破软件的限制

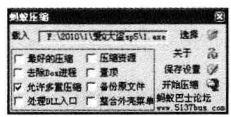
在“爱Q大盗”的主界面上，你会看到，扩展功能中只有“关闭一次QQ”能用，这是由于该版本是试用版本，所以我们需要采用如下的方法来突破。需要用到的工具是“灰色按钮专家”，运行“爱Q大盗”的同时，运行“灰色按钮专家”，将窗口拖到“爱Q大盗”界面上，点击“激活”按钮，你会发现其他几个灰色按钮全部变过来了，包括超级防御、文件夹感染等。

3.运行木马发挥威力

经过以上突破操作之后，点击主界面上的“生成木马”按钮，将会生成木马文件。

但是木马文件刚生成就被江民杀毒软件处理了。有什么办法呢？当然是加壳，躲过杀毒软件的监控。

这里给大家推荐“蚂蚁加壳工具”，加壳的方法就简单了，只要运行这个工具，将生成的木马添加进来，然后点击“开始压缩”按钮即可完成加壳操作。经过此操作，就躲过了江民的监控。经测试，这种加壳还能躲过瑞星、金山、卡巴、360等绝大部分杀毒软件的监控。



加壳操作

完成以上对木马加壳的操作，剩下的就是让对方运行这个木马了，运行后，你只要打开你的QQ邮箱，就等着坐收渔利吧。看，这里很清楚地显示了盗取的QQ号和密码。

接收信件

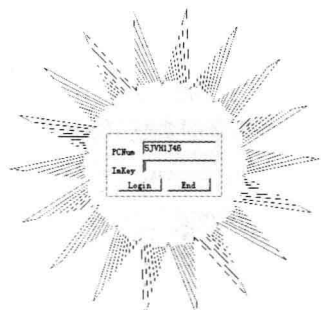
例2：解析QQ终结者在线盗号

关于QQ盗号的问题可谓老生常谈，但是一直有很多人关注。通常的盗取QQ的方法大多都是键盘记录，毕竟暴力破解的方式理

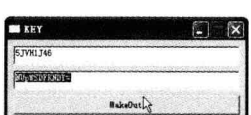
论上可行，但是猜解的时间不是一般人能容忍的。这里介绍的这款盗号工具，完全不采用键盘记录的原理，只要QQ在线就能获取其密码，当然，前提还是对方会运行你“秘制”的某个木马文件。

1.配置盗号木马

第一步 首先，运行QQ终结者，软件会提示我们输入ImKey，类似于一个注册号一类的东西，这个注册号可以通过网上的破解程序来搞定，只要运行MakeOut.exe这个文件，然后将QQ终结者软件界面上的PCNum码复制到MakeOut软件的第一栏中。



PCNum码复制到MakeOut中

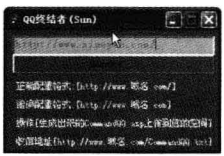


点击MakeOut按钮

第二步 然后点击MakeOut按钮，即可得到QQ终结者的ImKey。将ImKey码复制到QQ终结者中，点击“Login”按钮即可登录成功。

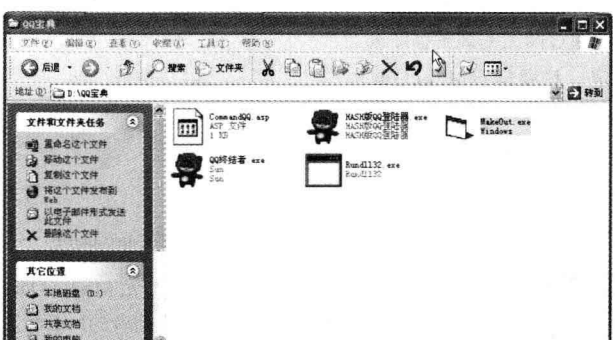
第三步 在QQ终结者主界面上，我们可以看到该软件不支持邮箱收信，只支持ASP网站收信，所以，大家需要有个FTP空间，如今有个人网站的用户应该比较多了，所以这个应该不是问题。

这里只要将域名输入到最上面一栏即可，需要特别注意的是域名“http://www.域名.com/”后面的“/”一定要加上，否则会出错。



输入域名

第四步 配置好个人网站后，只要点击“MakeOut”按钮，就可以在QQ终结者所在目录下生成CommandQQ.asp、Rundll32.exe和HASH版QQ登录器。至此，盗号木马制作完成。



生成的几个文件

2.上传文件收获密码

盗号木马制作完成后，要实现网站收信，需要将CommandQQ.asp上传到你的空间中，从而实现收信。上传完毕后，真正发挥作用