对不起 骇到你 之

招招解救你被黑的电脑

秘密客 编著

- 电子邮箱出现大量的垃圾邮件，如何即时阻止这种危害
- 反追踪、反监控，揪出躲在电脑里的黑客程序
- 隐藏Windows的共享文件夹，增强与保护操作系统安全
- 探究DdoS攻击，修改IIS漏洞，还给您安全的Windows 2000服务器
- 自制算法，防止密码暴露与防止暴力猜码的对策
- 扫除红色代码病毒、快乐时光、思坎病毒，带你远离危险的网络社群
- 反监控与阻断恶意的Sniffer探测网络行经

清华大学出版社

对不起，骇到你之

招招解救你被黑的电脑

秘密客　编著

清 华 大 学 出 版 社

(京)新登字 158 号

内 容 简 介

近几年，由于黑客的肆意破坏，给一些机构或企业带来巨大的损失。本书共分 11 章，重点介绍如何防范网络中各种黑客对电脑的攻击，并针对这些攻击手段介绍解救电脑的主要方法，让用户轻松学会如何对付这些黑客。每章都包含黑客攻击的原理、所使用的黑客工具以及应对实例。

作为一本黑客防范的工具书，本书有着很强的针对性，不仅全面介绍了网络上一般黑客的常用攻击手段，还针对这些黑客行为提出有力的防范措施和解救方法。

本书能让用户在轻松上网这余，免除遭受黑客骚扰的烦恼，因此本书适用于各级电脑用户阅读。

图书在版编目(CIP)数据

招招解救你被黑的电脑/秘密客编著.—北京：清华大学出版社，2002
(对不起，黑到你)
ISBN 7-302-05926-8

I.招… II.秘… III.计算机网络—安全技术 IV.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 074566 号

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：范 晓
印 刷 者：北京牛山世兴印刷厂
发 行 者：新华书店总店北京发行所
开 本：787×960 1/16 **印张**：21.25 **字数**：331 千字
版 次：2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷
书 号：ISBN 7-302-05926-8/TP・3520
印 数：0001～5000
定 价：33.00 元

前　言

黑客，会在我们身边出现吗？

确实我们经常听到黑客的神出鬼没、层出无穷的破坏行径。部分原因是，大多数电脑用户经常忘记为自己的电脑装加保护措施，等到硬盘被奇怪地格式化，重要资料如账号及密码等被别人盗取，病毒入侵，被植入木马程序受人监控，邮件炸弹、网页炸弹等相继而至，或封包资料、邮件遭到拦截盗取时，才开始紧张害怕。

本书主要介绍如何面对、防御和处理这些问题。全书共分为 11 个章节，全面介绍如何解救被黑客攻击的电脑。每章都包含了黑客攻击的原理、所使用的黑客工具以及应对策略。

第 1 章主要讲解如何利用远程或 Web 登录，学完本章的内容，读者就可以自己拆除邮件炸弹，解救被炸弹攻击的电子邮件信箱。

第 2 章介绍解救电脑木马的知识，并详细讲解如何查找可疑文件，清除、追踪及监控被植入电脑的木马程序。另外，还介绍了删除常见的木马病毒的方法。

第 3 章先介绍目前网络上流行的几个重要病毒，然后通过实例讲解如何清除这些网络病毒。

第 4 章专门针对 Windows 98 操作系统方面的漏洞，介绍如何减少在共享资源时造成黑客攻击计算机的机会。

第 5 章补充和扩展了第 4 章的内容，针对 Windows 2000 操作系统，向读者介绍如何修改 DDoS 攻击漏洞、IIS Unicode 漏洞以及其他漏洞。

第 6 章介绍了解救密码被黑的主要方法。同时教会读者有效地自定义编码规则，防止黑客进行暴力猜码。

第 7 章通过实例说明如何解救被别人监控的电脑。

第 8 章针对隐蔽性较高的网页窗口炸弹，介绍如何清除网站/网页的陷阱。

第 9 章通过介绍一个反删除文件的工具，介绍如何解救被删除的资料。

第 10 章通过介绍给 BIOS 加密和给文件夹加密等几个加密手段，让读者更加了解保护电脑主机的重要性。

第 11 章向读者介绍了两个非常可靠的个人防火墙，使您在成功防范之余，迈出抵御黑客的第一步。

本书以实例引导理论的方式介绍，讲解细致，语言通俗，适合各级电脑用户阅读。由于时间仓促，书中错误之处在所难免，敬请各位读者不吝赐教。

编者

2002.8

目 录

第 1 章　解救电子邮件

随着互联网的飞速发展以及电脑的日益普及，电子邮件(E-mail)的使用率已越来越高。一般用户除了用电子邮件的方式与客户进行信息交流、与好友相互问候外，还通过电子邮件的方式阅读免费订阅的新闻，因此可以说收发电子邮件是网络中最常用的功能。

由于电子邮件的广泛应用，它极易成为黑客攻击电脑的主要方式。

黑客攻击电子邮件的最常用方式就是“邮件炸弹”。一般情况下，根据邮件炸弹的攻击类型，将黑客的破坏方式分成以下两种：

- 有附加文件类型
- 无附加文件类型

有附加文件类型的大都是可执行文件(通常是病毒及木马程序)；而无附加文件类型是指垃圾电子邮件和大量轰炸邮件等。这些邮件炸弹最直接的破坏目的，就是让邮件账号不能正常收发电子邮件，甚至使用户的邮件账号陷于瘫痪状态。

要解救被攻击的电子邮件，需要了解邮件炸弹的攻击方式，根据它攻击的特点，找出相应的解救方法。本章将介绍目前常见的邮件炸弹“拆除”方法，并介绍如何恢复被攻击的邮件账号收发信件的功能。

1.1 登录网站清除邮件炸弹

邮件炸弹其实就是大量的垃圾信件，邮件炸弹与垃圾邮件的主要区别表现在，邮件炸弹的目的是破坏邮箱账号，而垃圾信件只是发送广告而已。邮件炸弹的袭击方式通常是向某个信箱发送成千上万的邮件，使其堵塞爆炸。

受到邮件炸弹攻击后，邮件信箱通常会被许多体积很大的垃圾文件塞满，这类垃圾邮件大都以文字形态的方式呈现，当然也有些是以附加的方式呈现。例如，当使用 Outlook 或是 Outlook Express 之类的程序，收取大量邮件或是夹带大型文件的邮件时，就有可能会因为收取信件的时间过长、用户多而分配到的频宽过低等因素，而导致如“超时”、“错误”等的信件收发失败问题，或是已收到的部分邮件在重新收取时，又重复收取一次。

这是因为邮件收发程序并不能判断哪些邮件是正常邮件，哪些是“炸弹”邮

件。从多数资深的网民的经历来看，收到邮件炸弹是很正常的。因此，用户应学会如何正确地面对这样的问题。

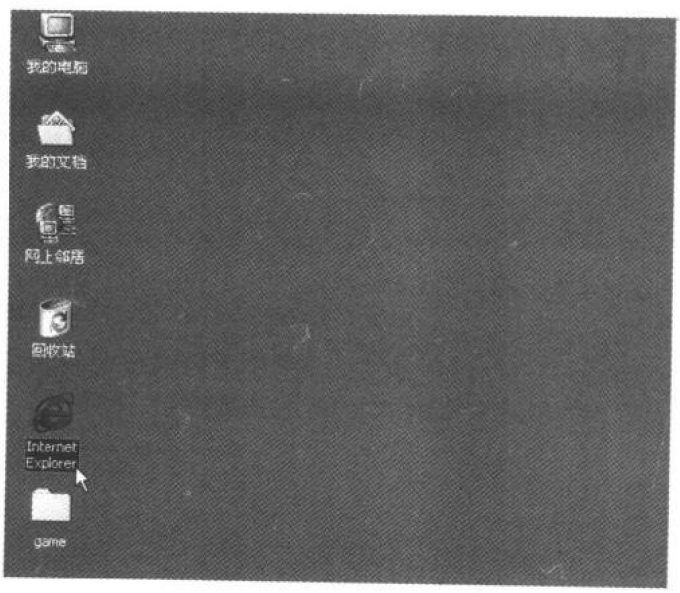
本节将详细介绍如何通过登录网站的方式，在邮件服务器里(Web Mail Server)中删除邮件炸弹。在删除邮件炸弹的过程中，我们将通过浏览器，登录自己的账号信箱，查看收件箱中的邮件，将不需要的邮件及邮件炸弹删除，让邮箱恢复到正常状态。

从互联网中登录自己的邮件账号，并清除邮件炸弹，是解救电子邮件信箱的基本方式。接下来以实例的方式，介绍如何将邮箱中的炸弹“拆除”，具体内容如下：

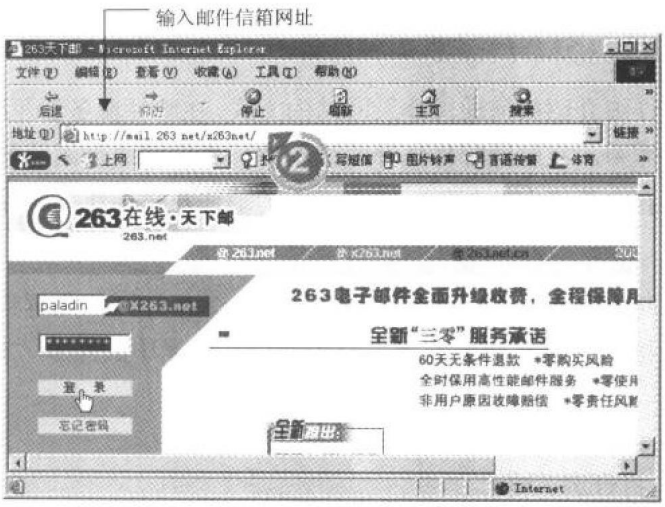
Step 1 打开浏览器

打开 IE 浏览器，输入电子邮件账号所在网站的网址，通常会在网站的首页打开邮件，然后进入自己的邮箱。

❶ 双击画面上的图标，打开 IE 浏览器



❷ 在【地址】下拉列表框中输入邮件所在网站的网址，然后按 Enter 键

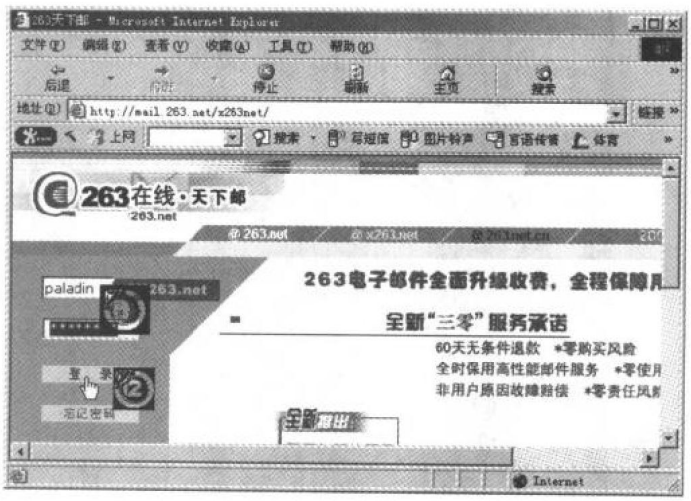


Step 2 登录邮件邮箱

在邮件登录页面中，输入自己的用户名与密码，登录邮件邮箱。

❶ 输入账号名称和密码

❷ 单击【登录】超级链接

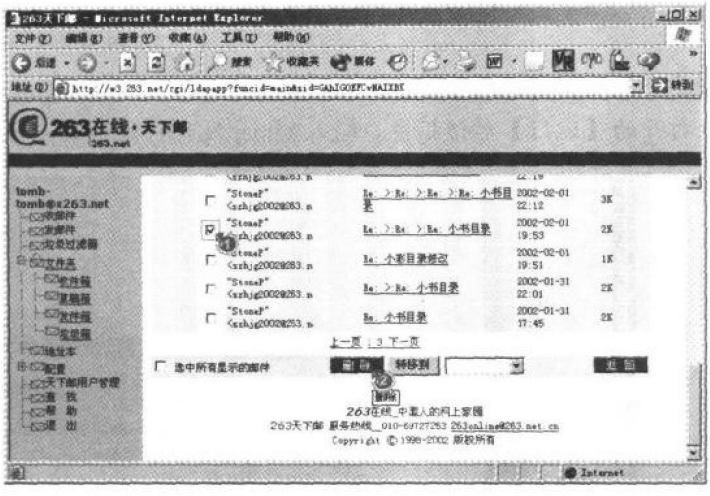


Step 3 清除邮件炸弹

成功进入自己的电子邮件信箱后，查看信箱内容，将不需要的邮件删除。

❶ 单击选中邮件

❷ 单击【删除】按钮



将邮件炸弹清除后，又可以继续使用 Outlook 或 Outlook Express 等程序收发邮件了。为了防止邮箱被“炸”而不能继续使用电子邮件联系，可以多申请几个邮件账号，这样当一个信箱被“炸”后，还可以继续使用其他信箱联系。

1.2 使用 telnet 删除邮件炸弹

受到邮件炸弹的攻击后，除了可以使用直接进入邮件信箱账号的网页，删除垃圾邮件的“拆除”炸弹方式外，还可以使用 telnet(远程登录)的方式删除邮件炸弹。

telnet 也是一种与远程计算机连接的方式，当用户拥有一个邮件账号后，其在邮件服务器内也就有了一个用户账户。这样用户就可以使用 telnet 登录邮件服务器，使用相关命令，将邮件信箱中的垃圾文件删除，即可重新使用邮件信箱了。

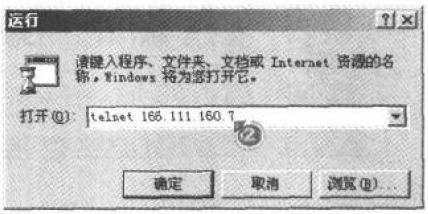
使用 telnet 方式删除邮件炸弹，需要用到 telnet 的相关命令，但操作并不复杂。接下来以具体例子介绍如何使用 telnet 删除邮件炸弹。

Step 1 打开 telnet

选择【开始】|【运行】命令，在打开的【运行】对话框中输入“telnet”，即可启动 telnet。

❶ 选择【开始】|【运行】命令

❷ 在打开的【运行】对话框中，输入 telnet 及邮件服务器命令



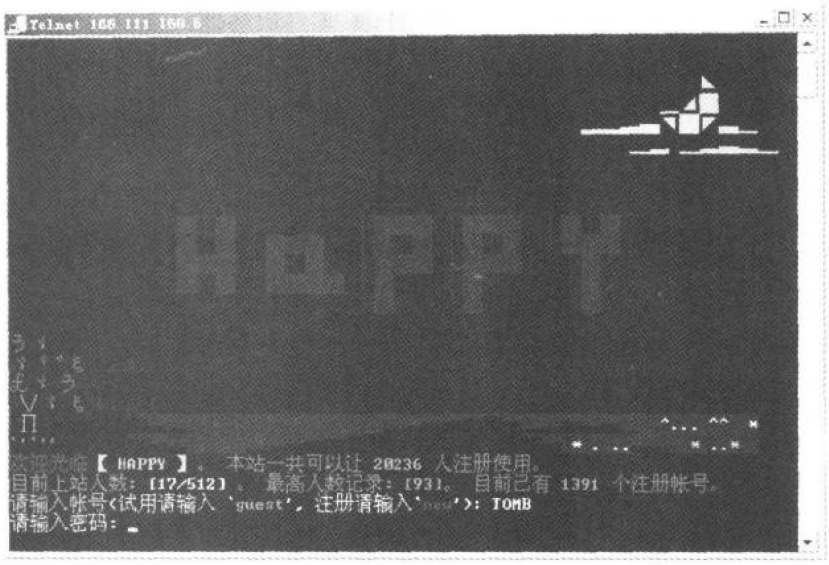
补充说明

telnet 命令说明

利用 telnet 登录服务器之后，在控制台(终端机画面)中输入 help 命令，即可列出全部命令的说明资料。

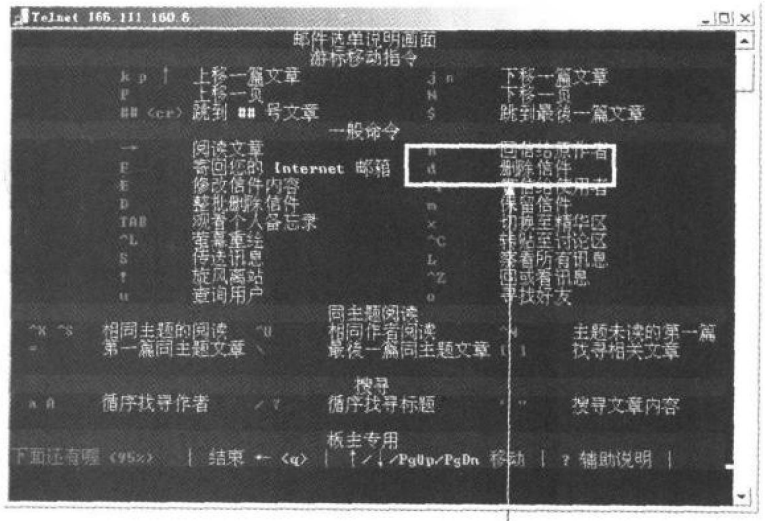
Step 2 登录邮件服务器

使用 telnet 登录到远程的邮件服务器，并进入自己的账号，方法为输入服务器邮件账号和密码。



Step 3 删除文件

登录自己的账号后，将垃圾邮件删除，方法为输入删除垃圾邮件的命令“d”，这样即可恢复邮件信箱。



命令 d 是邮件服务器上默认用来删除邮件的命令

进入自己邮件信箱的网页或登录 telnet 邮件服务器，都可以删除邮件信箱内的垃圾邮件，不过需要自己一步步手动操作。现在已经有很多软件可以帮助我们清理垃圾邮件，比自己手动删除方便多了，在本章的 1.3 节及 1.4 节中，将会介绍如何利用现成的软件拆除邮件炸弹。

1.3 使用 Email Remover 拆除邮件炸弹

在前面两节中，我们介绍了两种拆除邮件炸弹的基本方法。用这两种方式都可以达到拆除邮件炸弹的目的，只是需要我们一步一步手动操作，较为麻烦。使用邮件炸弹拆解软件则可以轻松拆除邮件炸弹，使邮箱恢复收发电子邮件的功能。

Email Remover 就是一个出色的邮件炸弹拆解软件，它可以帮助用户登录到邮件服务器，并显示邮箱内的所有邮件文件及大小。通过这些信息可以查看到邮件炸弹，并删除它。

下面以实例的方式，介绍如何用 Email Remover 软件恢复被炸的邮件信箱。

Step 1) 启动 Email Remover 程序

先确保自己的电脑中安装有这一软件，然后在安装该软件的文件夹中，直接双击 eremove 图标，即可打开 Email Remover 程序。