对不起 骇到你 之

防毒防黑防小人

秘密客 编著

- 病毒如何作怪？帮您将病毒的底细全部翻出来！
- 防毒软件、黑客程序全介绍，多种防身术完整传授。
- 病毒急诊室开张，解答各种病毒攻防秘技。
- 黑客入侵流程、手法彻底剖析，让您知己知彼。
- 有没有听到电脑在求救？最好使用防火墙！
- 系统安全自检、杜绝非法入侵行为，黑客诊疗室大放送！
- 概念扎根及实践双管齐下，给您最有效的防黑解毒秘方。

清华大学出版社

对不起，骇到你之

防毒防黑防小人

秘密客　　编著

清 华 大 学 出 版 社

（京）新登字 158 号

内 容 简 介

网络技术的迅猛发展极大地方便了计算机病毒的传播并使黑客技术有了更大的发展空间。本书从防黑与防毒角度切入，为读者揭开黑客与病毒的真面目，让读者深入了解防毒软件与其功能设置，并了解正确的防病毒知识。本书剖析黑客软件的设计原理并将其扩展到网络安全领域，详细介绍了病毒与黑客的基本知识、相关软件，防毒防黑的方法以及防火墙等内容，并且通过问答的方式解决病毒与黑客的相关问题，有效提高读者对防毒、防黑知识的应用水平。

本书语言生动，示例丰富，适合于想加强计算机安全知识的读者使用，对饱受病毒、黑客侵害的用户有很大的帮助作用。

图书在版编目（CIP）数据

防毒防黑防小人/秘密客编著. —北京：清华大学出版社，2002

ISBN 7-302-06088-6

I.防… II.秘… III.①计算机病毒—防治 ②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 090217 号

北京市版权局著作权合同登记号：图字 01-2002-3569 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.com.cn
http://www.tup.tsinghua.edu.cn
责任编辑：杨作梅
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**：24　**字数**：360 千字
版　　次：2002 年 12 月第 1 版　2002 年 12 月第 1 次印刷
书　　号：ISBN 7-302-06088-6/TP・3634
印　　数：0001～5000
定　　价：33.00 元

前　言

使用计算机的人大都听说过病毒和黑客，然而很多人并不了解病毒和黑客入侵计算机的严重程度。往往在计算机发生问题或在资料被窃取之后才觉察到病毒和黑客的入侵。

网络这个开放空间有许多安全隐患，但也不是完全无从防范。虽然不能百分之百杜绝病毒与黑客的入侵，但是仍然可以采取一些很简单的防范措施。

本书以防毒和防黑为切入点揭示黑客与病毒的真面目，让读者彻底了解防毒软件及其功能设置并掌握正确的病毒知识；剖析黑客软件的设计原理并将其扩展至网络安全领域，通过问答的方式解决病毒与黑客的相关问题，有效提高用户防黑防毒知识。

本书包括 7 章，各章主要内容如下：

第 1 章 解剖病毒：从头认识病毒，包括其定义及组成，使用户了解有关概念和病毒的传播途径，掌握必要且正确的防毒知识。

第 2 章 防毒软件：虽然防毒软件未必会让计算机有百毒不侵的神功，但是至少可以进行基本防护。介绍如何选购适合自己需要的防毒软件，有哪些防毒资源可以增强数字安全，以及如何让防毒软件为计算机架设防御功能强大的保护网。

第 3 章 病毒急诊室：讨论对各种病毒的攻防技巧，利用不同类型问题的问答方式建立基本的防毒概念，使用户循序渐进地成为防堵病毒的高手。

第 4 章 剖析黑客：探讨黑客的入侵手法、黑客与怪客的区别、法律对黑客的约束以及防范黑客的自我检查。

第 5 章 防火墙软件：包括各种防火墙软件的介绍、防火墙的使用及防火墙有别于防毒软件的特殊功能。

第 6 章 黑客程序：黑客的计算机水平与网络知识或许比一般用户高深，但在“黑”人的时候，仍须借助于一些黑客工具程序及木马程序，以便又快又精准

有效地突破封锁线。本章将介绍这些黑客工具。

第 7 章 黑客诊疗室：本章通过一问一答的方式将各种可能会遇到的疑难问题理出一个清楚分明的头绪，并对症下药。

希望本书可以帮助更多的人远离病毒及黑客的侵袭，并具备防毒防黑的正确知识。

编者

2002.8

目 录

第1章　解剖病毒

在网络这个虚拟社会中，处处都有美丽动人的风景，但往往其背后潜在的风险和隐患又令人只敢远观而不敢把玩，计算机病毒便是最明显的例子。

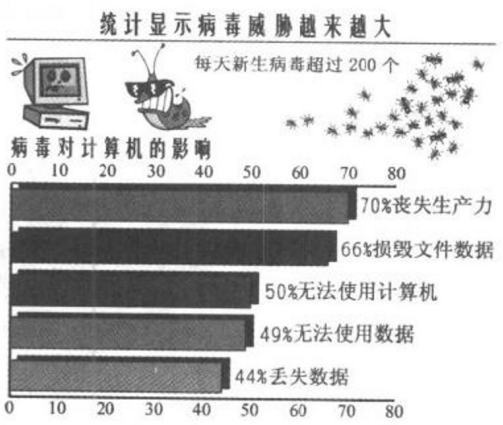
不过，只要提高警惕，有形的伤害还是容易提防的，相比之下，无形的语言暴力反而最为凶险，例如，网络上流传的谣言信件以连锁 E-mail 的方式散播错误的病毒信息：

“若在计算机硬盘里发现 xx 文件名的文件，那么表示您已经中毒了，请立刻删除该文件!!”

类似这样的谣言与未经证实的信件内容，通常称为信息病毒。虽然这类病毒实际上对计算机系统安全不会造成任何实质上的破坏，然而它所带来的伤害却远远比“正宗病毒”要大得多。因为真实的病毒所引发的破坏与伤害是有形的，它最终损坏了哪些数据都可以看得清清楚楚；但是这种信息病毒造成的后遗症无形而且后患无穷，它对网络信息的传播有极负面的影响。

在开始剖析病毒之前，先来看看计算机病毒惹出了哪些麻烦。

据报导，全球大约 70%的计算机系统曾经感染过病毒，当中有不少是企业里的专业服务器，由此可见它的感染范围之大。相关的公司研究(Computer Economics of Carlsbad，Calif)表明，仅在 2001 年 1 月至 9 月，全球信息系统因为计算机病毒肆虐所造成的损失据估算已达 107 亿美元，2000 年全年为 171 亿美元，1999 年为 121 亿美元。病毒危害统计如下图所示。



病毒危害统计图

这些对个人计算机(PC)来说好像太遥远了，计算机感染病毒顶多重装系统、重新建立整理数据而已，根本不值得大惊小怪。下面是一个真实的例子，相信看过之后就会明白，无所不能无所不在的病毒并非与我们毫不相干。

英国伦敦大学里的一位博士生，在最后一个月的学业关键时期，将论文和实验数据存放在笔记本电脑内就等着论文通过后取得学位。不幸的是该名学生不小心运行了病毒程序，恶意的病毒不但删除了所有的数据，而且大举攻击了计算机操作系统，最后该名学生虽然使用了杀毒软件但无济于事，论文也随之化为乌有，因此耽误了该名博士生顺利毕业，这件事对他的前途影响不小。

防治计算机病毒一定先要了解对手的习性和底细，这样才能立于不败之地。下面我们将揭开病毒的神秘面纱，使读者全面认识病毒的每一个方面，以培养读者正确的病毒知识。

1.1 计算机病毒

用户虽然为计算机安装了杀毒软件、设置了防火墙，但新病毒依然不断问世，防不胜防。根据统计，每天都会有新病毒诞生，而且病毒形式和破坏力都非同小可。

在计算机领域里，电子邮件、文本文件、可执行文件、甚至网页都是计算机病毒的活动领域。但说到底，计算机病毒如同正常的文本软件和游戏程序一样，不过是计算机里执行的程序。它们之间的差别就在于正常的程序可以帮助用户省时省力地完成许多工作，而计算机病毒则减慢计算机的运行速度，让文件数据或系统毁于一旦。

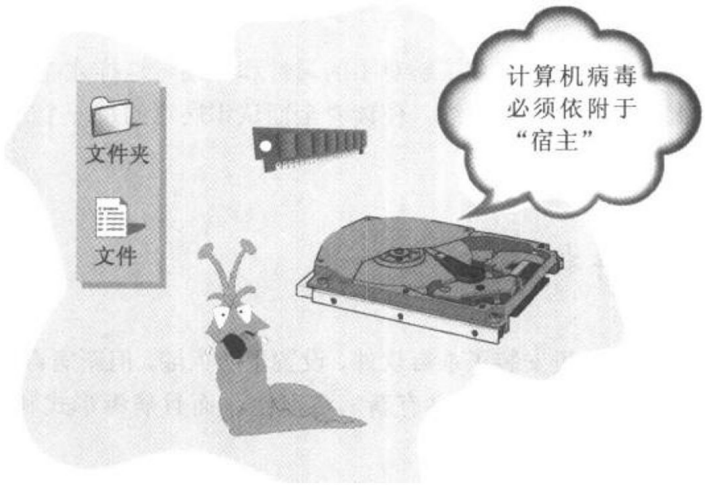
1.1.1 计算机病毒的基本定义

所谓计算机病毒，指的是一段被刻意写成的可执行程序，该程序会自动寻找“宿主”并且依附在它上面，例如计算机的磁盘扇区、可执行文件和内存等。不论寄宿的对象是谁，病毒都会想尽办法延长自己的生命。

正常的程序不会有寻找并依附在宿主上的操作，因此，这种具有传染特性的程序就被称为病毒(Virus)。另外还有一个与病毒相仿，却有别于病毒的程序——

蠕虫(Worm)，虽然它具有传染性，但与病毒相比，它会选择寄居的场所，伺机寻找漏洞发作，严格说，这两者的传染与传播方式是不同的。

许多计算机病毒程序在潜入他人的计算机系统时会对宿主计算机产生破坏作用，因此受害者或媒体报导在谈到病毒时多少会流露出愤恨不平之意。实际上，多数病毒并不具有破坏作用，它们只是潜伏侵入或者开一些无恶意的玩笑罢了。具有强大杀伤力的计算机病毒在所有病毒中所占比例很小，但却容易给人留下深刻印象并造成一定程度的心理恐慌。



此外，有人将“黑客程序”(Hack Program)视为病毒，其实黑客程序本身并不会传染，除非黑客程序已被人动过手脚、加入了具有传染性的病毒代码，大多数的黑客程序充其量只是一套可以用来攻击系统的工具程序而已。

计算机病毒是计算机程序，而且是一种具有“传染”和“繁殖”能力的程序。计算机病毒不会凭空产生，一定是有人故意制造和传播。其他有害的计算机程序，如蠕虫、黑客程序和逻辑炸弹等，尽管同样出自他人之手，但因为程序本身不具有“传染性”，故不能称之为“病毒”。

1.1.2 计算机病毒的危害

多数病毒并不以破坏为目的，但是病毒程序具有传染性，会间接导致操作系统运行速度变慢、兼容性变差、浪费磁盘空间等许多副作用。而少数恶性病毒删