电脑报总策划

黑客特警110

电脑安全X档案

防毒 反黑 数据恢复指南

杨锦川 张 熙 编著
龚鹏飞 刘春梅

黑客防御技巧
典型病毒查杀实战
数据备份与恢复全攻略
杀毒软件使用设置详解
防黑工具使用技巧大放送
系统安全防范实战技巧揭秘
数据加密与解密技巧全剖析

云南人民出版社

黑客特警110

《黑客特警110——电脑安全X档案》

本书内容丰富、结构清晰，基本涵盖了电脑安全各个方面的内容，从硬件、系统、磁盘管理、文件、网络等层面全面讲述了电脑安全防范知识。本书不但讲解了常见病毒和黑客的防范与清除技巧，还讲解了数据维护、数据备份、灾难恢复等实际操作，力求为电脑用户提供一个完整的安全解决方案。

《黑客特警110——黑客攻防实战100例》

本书从普通用户的网络安全的角度出发，向读者介绍了个人安全设置与防范的相关知识，系统全面地介绍黑客的攻击手段和网络安全防范技术，主要涉及OICQ、电子邮件的安全使用、病毒防护、操作系统安全、木马防范、防火墙、浏览网页、共享资源、通讯工具、账号密码、代理跳板等内容，每部分内容都紧扣“实战”这一主题，紧紧围绕普通个人用户安全这一思路，以实践性与指导性为基本出发点，针对广大读者朋友日常上网过程中所遇到的棘手问题，详细地进行了分析解答，逐步揭开读者心中的安全疑点与难点，同时指导读者及时做好安全防备。

《黑客特警110——电脑密码完全解密》

本书从基础应用技巧开始讲解：首先，介绍不同CMOS的开机密码设置、管理以及密码丢失或遗忘时的破解方法，使初学者初步了解密码使用；接下来详细讲解系统密码的加密与解密技巧、网络密码的完全精通及进阶、常用软件的简单加密与解密，最后还介绍了密码相关问题的处理，便于读者随学随用，即查即知。

ISBN 7-222-03849-3

9 787222 384934

ISBN 7-222-03849-3

定价:26.00元

黑客特警110

电脑安全X档案

——病毒、黑客、数据恢复指南

杨锦川　张　熙
龚鹏飞　刘春梅　编著

云南人民出版社

图书在版编目（CIP）数据

电脑安全X档案 / 杨锦川，张熙编，-昆明：云南人民出版社，2003.8
ISBN 7-222-03849-3

Ⅰ.电… Ⅱ.①杨…②张… Ⅲ.电子计算机-安全技术—普及读物 Ⅳ.TP309-49

中国版本图书馆CIP数据核字（2003）第069844号

责任编辑：西 捷 李 桁
技术编辑：李 勇 黄 斌 周 鹏
封面设计：刘学敏
版式设计：郑 兰

书 名：电脑安全X档案
作 者：杨锦川 张 熙 龚鹏飞 刘春梅
出 版：云南人民出版社
发 行：云南人民出版社
社 址：昆明市环城西路609号
邮 编：650034
电 话：0871-4113185 4194569 4194559
E-mail：YNPPDZ@vip.km169.net
开 本：787mm × 1092mm 1/16
印 张：25
字 数：350千
版 次：2004年3月第1版第1次印刷
印 数：1-5000
印 刷：重庆科情印务有限公司
书 号：ISBN 7-222-03849-3
定 价：26.00元

目录 CONTENTS

目录 CONTENTS

目录 CONTENTS

目录 CONTENTS

目录 CONTENTS

目录 CONTENTS

引子——个人电脑安全综述

Internet 在全球范围内的快速发展将我们带入了一个光怪陆离的网络世界，它的出现极大地改变了人类的生产生活方式。在信息化社会中，计算机、网络以及相关的应用系统在人们的日常生活中起着越来越重要的作用。这些网络信息系统都依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理与控制。

然而，犹如一把双刃剑，Internet 也带来了许多前所未有的忧患——网络的安全问题已经成为不可回避的现实。在色彩缤纷的互联网背后，病毒的泛滥、黑客的攻击、日益猖獗的网络犯罪、还有个人隐私的泄漏……凡此种种，不胜枚举，已经严重影响了正常的网络系统运行。越来越多的个人电脑用户开始意识到抵御病毒入侵、防范黑客攻击、保障操作系统和个人数据安全的重要性。

一、个人电脑安全问题不容忽视

网络安全已经成为信息时代的头等大事。据 FBI 估计，美国每年因为网络安全问题造成的损失高达数百亿美元，整个 Internet 上平均十余秒就有一次入侵行为发生。而且，计算机网络这种先进的技术手段已经同传统的犯罪行为结合起来，形成了对整个人类社会网络秩序的挑战。

许多人认为，个人电脑的重要性与那些大型的政府网、科研网、军用网以及企业网相比，远远不可同日而语，所以个人电脑的安全问题是微不足道、无关大局的。其实不然，越来越多的攻击案例显示，个人电脑安全已经成为网络安全一个很重要的隐患，由于大部分个人用户安全意识的淡薄，大量对政府企业网络的攻击往往首先从个人用户开始突破的。

(1)首先，大型网络的安全问题已经引起足够的重视，他们依托专门的技术、专门的设备、专业的网络安全技术人员以及足够的资金，通过购置各类网络安全专用软硬件、及时修补各种系统漏洞、进行各种安全配置、委托专门的网络安全公司进行安全检测等安全措施，系统坚固性愈来愈得到强化，黑客已经很难象以前那样可以通过一些简单的手段直接侵入了。对个人用户而言，其条件有限，明显不能象专业的网络安全人员一样天天关注着最新的网络漏洞，可以及时发现情况并且修补它，这就使得网络中的个人电脑的安全性非常脆弱，攻击者轻易就可以得手。

(2)其次，个人电脑容易受到黑客青睐的另一个原因是黑客需要隐藏自己，聪明的人决不会利用自己的机器直接攻击其他网络系统，因为被攻击系统的日志文件和防火墙记录文件有可能记录下他们的 IP 地址。所以大多数时候，黑客们发起攻击时一般会去找一些跳板，他们把这些跳板称作“肉鸡（肉机）”。因为个人用户的机器相当容易被攻破，常常被黑客用作“肉鸡”。这些被控制的主机大多是防护不严密的个人电脑，很多用户甚至根本没有觉察到自己的电脑参与了攻击。

(3)另外，很多个人用户都会说，我的电脑中没有什么东西会值得黑客感兴趣，谁会来攻击我？

但是黑客们的攻击很多时候并不是特定针对政府企业或者军方网站的，他们经常使用扫描软件对某一地址段进行大规模的端口扫描，这些程序扫描速度是非常快的，它只是机械重复寻找 Internet 上所有打开的端口，从这一点来说，个人用户和政府企业用户受攻击的的概率是相同的。

由于黑客技术和攻击工具的扩散，许多水平一般的攻击者出于好奇或者尝试的动机，经常漫无目的地发起攻击，他们的攻击在防卫严密的系统面前往往不能奏效，但是很多上网的个人电脑却成了无辜的牺牲品。现在的黑客群体已经是鱼龙混杂，很多道德低下的攻击者经常以肆意破坏别人的系统为乐，甚至被利益所驱动，盗取你的各种密码及个人隐私信息，如上网账号密码、信用卡账号密码、邮箱账号密码等等。

面对严峻的网络安全形势，你随时都得担心你的个人信息是否会被窃取，你的账号号密码是否会被盗用，你的系统是否会被植入木马和病毒，甚至你还可能成为一个无辜的帮凶，被黑客改造成一台 DoS 攻击机器。所以我们必须对个人电脑的安全问题保持警惕，不能掉以轻心，必须为自己寻找网络保护，防御各种各样的攻击行为，以免成为黑客们的猎物。

二、个人电脑安全所面临的种种威胁

许多网友可能有过这样的经历：突然感染莫名其妙的病毒；正在上网的机器突然蓝屏；受到大量垃圾邮件的骚扰；上网账号被人盗用；甚至自己的机器被远程控制，数据遭到破坏等等。当你在没有任何安全保护措施的情况下在网上尽情冲浪之时，层出不穷的病毒、蠕虫、木马、黑客等等随时都可能向你伸出黑手。

1. 病毒泛滥

随着 Internet 的发展，人们对网络的依赖性越来越强，病毒的扩散途径、扩散速度、表现形式以及造成的破坏都愈演愈烈，网络成了计算机病毒的第一传播途径。除了传统的文件型计算机病毒以文件下载、电子邮件的附件等形式传播外，新兴的电子邮件计算机病毒则是完全依靠网络来传播的，甚至还有利用网络分布计算技术将自身分成若干部分、隐藏在不同的主机上进行传播的计算机病毒。除此以外 BBS 访问（文件的交换）、WWW 浏览（利用 Java Applets 和 ActiveX Control 编写的计算机病毒）、FTP 文件下载以及新闻组访问都成了计算机病毒扩散的途径。“快乐时光”、“炭疽热”、“红色代码”、“CIH”、“尼姆达”、“中国一号”、“求职信”等病毒令网友们谈毒色变，电脑病毒已经成为网络的“第一杀手”。

电脑病毒和别的程序一样，它也是人编写出来的。既然病毒也是人编的程序，那就会有办法来对付它。对付病毒有两条措施：一就是防，采取各种安全措施预防病毒，不给病毒以可乘之机；二就是杀，我们可以使用各种杀毒程序，把病毒从电脑中清除出去。

2. 黑客攻击

Internet 的普及造就了一大批伪黑客，他们不必特别精通网络通讯技术，仅仅使用从网上下载的现成的黑客软件就能对他人造成损害，从而使互联网安全出现了许多危机。黑客进行攻击的手

法很多，比如端口扫描、IP 欺骗、E-mail 炸弹、特洛伊木马等等，我们将在后面安排了专门的章节来讲述黑客入侵的原理、技术手段、常用工具以及防御方法。

3. 个人隐私泄漏

我们在计算机上打开文件或访问网站时，都会在机器上留下踪迹。若是在网吧等公共场所使用，那么就有一定的危险。你的计算机会向外透露你正在进行的工作，窥探者可以从你的机器中获取很多信息：包括已经被你删除的收到或发出的邮件、你访问过的 Internet 网站、搜索规则及你在网页表单中输入的数据等等。大家可能都知道，在网上只要花费不多的钱就能买到大批用户的个人资料，如姓名、地址、电子邮件、电话号码，甚至是信用卡号码等。所以，保护自己的个人信息非常重要。为安全起见，我们应该注意在下线的时候抹去我们的上网痕迹。

4.WWW 浏览安全

随着网络的不断发展，众多的攻击手法层出不穷，现在就连普通的浏览网页也存在着不安全的因素，轻则使系统混乱，重则暴露自己的隐私，甚至使硬盘上的数据遭到破坏。最典型的浏览安全问题是对于 IE 的恶意修改，或把自己的网站强硬推荐给别人，或修改 IE 右键菜单，手法时时换新，令人防不胜防！还有 Web 欺骗，它是一种具有相当危险性且不易被察觉的黑客攻击手法，它针对浏览网页的个人用户进行欺骗，非法获取或者破坏个人用户的隐私和数据资料。

5.E-mail 安全

电子邮件是 Internet 上除了 WWW 浏览之外最普及的应用，已经成为人们相互沟通不可缺少的工具，但是它也给网络安全造成了很大的隐患。Internet 上的 E-mail 采用的是明文传输，在经过各个路由器的时候很容易被黑客所截获，造成信息泄密。针对电子邮件的攻击主要有两种方式：一是电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串），或在貌似正常的附件中加载病毒或其他木马程序，诱骗用户执行。

6. 各种网络活动安全

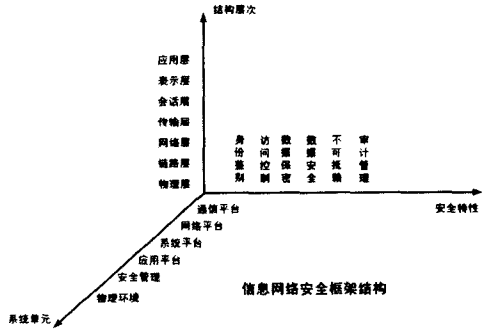
网虫们在聊天室中和 BBS 论坛上也非常易受攻击。我们在 Internet 上参与 IRC 聊天的时候很容易遭到别人的攻击，机器就会产生莫名其妙的问题，比如死机、断线、弹出窗口等等。像 ICQ/OICQ/MSN Messenger 之类的即时通讯软件也存在极大的安全漏洞，别有用心的人可能利用它盗取你的机密和破坏你的机器。

三、个人电脑安全基本策略

在 Internet 上，可以说，没有任何一个主机是 100% 绝对安全的，计算机里面任何一个无意的不恰当配置都有可能被攻击者加以利用。网络的安全问题，始终是一个比较棘手的事情，它既有硬件的问题，也有软件的问题；既涉及复杂的技术问题，又涉及相关法律和管理措施。网络安全

追求的不是完成某些事，而是避免某些事发生，这是非常困难的。因为计算机网络是基于开放互连架构发展起来的，网络安全和效率与便利之间的平衡不好把握。

要比较好地解决计算机网络的安全问题，必须从网络安全涉及的所有领域出发，构造一个完整的解决方案，一个系统组织的整体安全是十分重要的。典型的信息网络安全框架结构如图所示。



信息网络安全框架结构

从上图我们可以看到，要解决网络安全需要从三个方向入手，每一个方向的问题又分为很多层次。对个人电脑用户而言，当然涉及的问题不会如此复杂，参照网络安全体系，可以简单地将个人电脑安全基本策略划分为下列几个问题:

(1)硬件级安全策略——从物理环境角度考虑，主要指电脑设备的物理防护，防止盗用或毁坏，包括机器使用授权、网络接入设施、防火墙设施、加密卡设施、内外物理隔离设施、防电磁泄漏设施以及防火、防雷、防静电设施等等内容，这其实就是网络基础设施建设的相关问题。除了一些军用保密单位，大部分上网的个人电脑是不必考虑这些东西的，顶多也就是设置开机密码、装加密狗以及硬盘加密等等。

(2)系统级安全策略——从安全的操作系统和应用软件系统角度考虑，包括用户认证、操作系统加固、漏洞修补、数据存储加密等等内容。

(3)网络级安全策略——从安全的网络通讯角度考虑，包括网络通信协议、数据通信加密、访问授权、审计监控等等内容。

(4)数据安全策略——从灾难紧急响应的角度出发，包括数据备份与恢复、数据灾难修复等内容。

第一章 初识计算机病毒

第一节 计算机病毒相关概念

一、计算机病毒的发展和特征

1. 计算机病毒的概念

计算机病毒(Computer Virus)是指编制或者在计算机程序中插入的破坏计算机功能、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

详细的来讲，计算机病毒是指一个程序，一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

除复制能力外，计算机病毒还有其他一些共同特性：一个被传染的程序能够传送病毒载体。当用户看到病毒载体似乎仅仅表现在文字和图像上时，它们可能已毁坏了文件或引发了其他类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存储空间给用户带来麻烦，并降低用户的计算机性能。

2. 计算机病毒发展史

(1)最早的计算机病毒只是一些天才程序员在实验室做出的高级智力电子游戏。早在1949年，距离第一部商用电脑的出现还有好几年时，德国科学家冯·诺伊曼(John Von Neumann)在他所提出的一篇论文《复杂自动装置的理论及组织的进行》中，就已把病毒程式的蓝图勾勒出来了，当时绝大多数电脑专家都无法想像这种会自我繁殖的程式是可能的。只有少数几个科学家默默地研究冯·诺伊曼所提出的概念。直到十年后，在美国电话电报公司(AT&T)的贝尔(Bell)实验室中，三个年轻的程序员道格拉斯·麦基尔罗伊(H.Douglas McIlroy)、维克多·维索特斯克(Victor Vysottsky)以及罗伯特·莫里斯(Robert T. Morris)，当时三人年纪都只有二十多岁，常在工作后留在实验室里玩起他们自己创造的电子游戏，这种电子游戏叫做“核心大战(core war)”。

(2)1983年11月3日，弗雷德·科恩(Fred Cohen)博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼(Len Adleman)将它命名为计算机病毒(Computer Virus)，并在每周一次的计算机安全讨论会上正式提出，8小时后专家们在VAX11/750计算机系统上运行，第一个病毒实验成功，一周后又获准进行5个实验的演示，从而在实验上验证了计算机病毒的存

在。在那些日子里，由于电脑都没有联网，因此并不会引起病毒瘟疫。如果某台电脑受到“感染”失去控制，工作人员只须把它关掉即可。但是当电脑网络逐渐成为社会结构的一部份后，一个自我复制的病毒程序便很可能带来无穷的祸害了。因此长久以来，懂得玩“核心大战”游戏的电脑工作者都严守一项不成文的规定：不对大众公开这些程序的内容。

(3)1983 年，这项规定被打破了。科恩．汤普逊(Ken Thompson)是当年一项杰出电脑奖得奖人，在颁奖典礼上，他作了一个演讲，不但公开地证实了电脑病毒的存在，而且还告诉所有听众怎样去写病毒程序。

(4)1988 年 3 月 2 日，一种苹果机的病毒发作，这天受感染的苹果机停止工作，只显示“向所有苹果电脑的使用者宣布和平的信息”，以庆祝苹果机生日。

(5)1988 年 11 月 2 日，美国六千多台计算机被病毒感染，造成 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即作出反应，国防部成立了计算机应急行动小组。这次事件中遭受攻击的包括 5 个计算机中心和 12 个地区结点，连接着政府、大学、研究所和拥有政府合同的 250，000 台计算机。这次病毒事件，计算机系统直接经济损失达 9600 万美元。这个病毒程序设计者是罗伯特·莫里斯(Robert T.Morris)，当年 23 岁，是在康乃尔大学攻读学位的研究生。罗伯特·莫里斯设计的病毒程序利用了系统存在的弱点。由于罗伯特·莫里斯成了入侵 ARPANET 网的最大的电子入侵者，他被获准参加康乃尔大学的毕业设计，并获得哈佛大学 Aiken 中心超级用户的特权。但他也因此被判 3 年缓刑，罚款 1 万美元。

3．病毒发展阶段

在病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统进行升级时，病毒也会调整为新的方式，产生新的病毒技术。它可划分为：

(1)DOS 引导阶段

1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”和“石头”病毒。

当时的计算机硬件较少，功能简单，一般需要通过软盘启动后使用。引导型病毒利用软盘的启动原理工作，它们修改系统启动扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，影响系统工作效率，在系统存取磁盘时进行传播。1989 年，引导型病毒发展为可以感染硬盘，典型的代表有“石头 2”。

(2)DOS 可执行阶段

1989 年，可执行文件型病毒出现，它们利用 DOS 系统加载执行文件的机制工作，代表为“耶路撒冷”、“星期天”病毒，病毒代码在系统执行文件时取得控制权，修改 DOS 中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加。1990 年，发展为复合型病毒，可感染 COM 和 EXE 文件。

(3)伴随、批次型阶段

1992年，伴随型病毒出现，它们利用DOS加载文件的优先顺序进行工作。具有代表性的是“金蝉”病毒，它感染EXE文件时生成一个和EXE同名的扩展名为COM伴随体，它感染COM文件时，把原来的COM文件改为同名的EXE文件，再产生一个原名的伴随体，文件扩展名为COM。这样，在DOS加载文件时，病毒就取得控制权。这类病毒的特点是不改变原来的文件内容，日期及属性，清除病毒时只要将其伴随体删除即可。在非DOS操作系统中，一些伴随型病毒利用操作系统的描述语言进行工作，典型的代表是“海盗旗”病毒，它在得到执行时，询问用户名称和口令，然后返回一个出错信息，将自身删除。批次型病毒是工作在DOS下的和“海盗旗”病毒类似的一类病毒。

(4)多形阶段

1994年，随着汇编语言的发展，实现同一功能可以用不同的方式进行完成，这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点，每感染一次就产生不同的代码。例如“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，加大了查毒的难度。

(5)生成器，变体机阶段

1995年，在汇编语言中，一些数据的运算放在不同的通用寄存器中，可运算出同样的结果，随机地插入一些空操作和无关指令，也不影响运算的结果，这样，一段解码算法就可以由生成器生成。当生成的是病毒时，这种复杂的称之为病毒生成器和变体机就产生了。典型的代表是“病毒制造机VCL”，它可以在瞬间制造出成千上万种不同的病毒，查解时需要在宏观上分析指令，解码后查解病毒。

(6)网络，蠕虫阶段

1995年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改进。在非DOS操作系统中，“蠕虫”是典型的代表，它不占用除内存以外的任何资源，不修改磁盘文件，利用网络功能搜索网络地址，将自身向下一地址进行传播，有时也在网络服务器和启动文件中存在。

(7)视窗阶段

1996年，随着Windows和Windows 95的日益普及，利用Windows进行工作的病毒开始发展，它们修改NE、PE文件，典型的代表是DS.3873，这类病毒的机制更为复杂，它们利用保护模式和API调用接口工作，解除方法也比较复杂。

(8)宏病毒阶段

1996年，随着Word功能的增强，使用Word宏语言也可以编制病毒，这种病毒使用类Basic语言，编写容易，感染Word文档文件。在Excel和AmiPro出现的相同工作机制的病毒也归为此类。

(9)互联网阶段

1997年，随着因特网的发展，各种病毒也开始利用因特网进行传播，一些携带病毒的数据