附教学光盘

从零开始

防治电脑病毒

老虎工作室 赵亮 李卫华 编著

人民邮电出版社
POSTS & TELECOM PRESS

从零开始

—— 防治电脑病毒

老虎工作室 赵 亮 李卫华 编著

人民邮电出版社

图书在版编目（CIP）数据

从零开始：防治电脑病毒 / 赵亮，李卫华编著. —北京：人民邮电出版社，2005.9

ISBN 7-115-13991-1

Ⅰ. 从… Ⅱ. ①赵…②李… Ⅲ. 计算机病毒—防治 Ⅳ. TP309.5

中国版本图书馆 CIP 数据核字（2005）第 096435 号

内 容 提 要

本书是一本关于电脑病毒防治和清除的实用书籍。全书共 8 章，第 1、2 章介绍电脑病毒的基本概念及相关知识，为后续章节奠定基础；第 3、4 章着眼于电脑病毒的预防，从操作系统、个人网络防火墙、反病毒软件三个层面介绍了电脑病毒预防的各种方法和手段；第 5、6、7 章着重介绍电脑病毒的清除方法，从反病毒技术讲起，在此基础上引入一些典型的反病毒案例，并对木马病毒的查杀单独设置章节进行讲解；第 8 章对黑客相关知识进行介绍。

本书以实用性为主导，在书中使用了多幅图片对实际问题进行分析，并在所附光盘中对部分实际操作进行视频演示。本书适用于普通家庭用户、掌握一定计算机技术的学生、中小企业的安全维护人员阅读，也可作为学习安全知识和电脑病毒防治的培训教材和自学用书。

从零开始——防治电脑病毒

◆ 编　　著　老虎工作室　赵　亮　李卫华

责任编辑　李永涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号

邮编　100061　　电子函件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京鸿佳印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：787×1092　1/16

印张：20.5

字数：493 千字　　2005 年 9 月第 1 版

印数：1－6 000 册　　2005 年 9 月北京第 1 次印刷

ISBN 7-115-13991-1/TP・4963

定价：34.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223

老虎工作室

主　编：沈精虎

编　委：许曰滨　黄业清　姜　勇　宋一兵　高长铎
田博文　谭雪松　杜俭业　向先波　毕丽蕴
郭万军　宋雪岩　詹　翔　张　琴　周　锦
冯　辉　王海英　蔡汉明　李　仲　马　震
赵治国　赵　晶　张　伟　朱　凯　臧乐善
郭英文　计晓明　张艳花　孙海侠　姜继红

关于本书

内容和特点

随着电脑的普及和网络的迅猛发展，电脑病毒作为电脑技术的“副产品”也深深影响着人们的生活，特别是近年来，电脑病毒呈现出愈演愈烈的趋势，给人们使用电脑带来了严重困扰。无论是谁，只要使用计算机，就必定会和电脑病毒打交道，也就必须了解相关的电脑病毒知识和各种防范处理措施。

本书写作思想来自电脑病毒讨论区中用户提出的各种问题，以及用户在电脑病毒防杀中的各种误区。作者在此基础上进行了总结，并在一定程度上自成体系，主要讨论了电脑病毒的“防”和“杀”两大方面。“防”主要从操作系统、个人网络防火墙和反病毒软件三个层面进行阐述；“杀”则从如何发现电脑病毒和如何清除电脑病毒两方面进行阐述。

全书共分 8 章，各章具体内容简介如下。

- 第 1 章：介绍电脑病毒的基本概念、由来、特征和分类等，以及最新的技术和动态。
- 第 2 章：介绍电脑病毒防杀中需要掌握的一些基础电脑知识，并举例阐述了电脑病毒的原理。
- 第 3 章：从操作系统和个人网络防火墙层面阐述电脑病毒的防范方法。
- 第 4 章：从反病毒软件层面阐述电脑病毒的防范方法。
- 第 5 章：介绍怎样发现电脑病毒和如何清除电脑病毒。
- 第 6 章：以几个流行电脑病毒为例，对如何清除电脑病毒做进一步阐述。
- 第 7 章：介绍木马病毒的检测和清除技术。
- 第 8 章：介绍黑客的基本知识和一些基本的防范手段。

读者对象

本书主要适合以下 4 类读者阅读。

- 普通家庭用户。电脑的普及使普通家庭用户日益增多，而家庭用户的电脑使用水平普遍偏低，本书完善有效的防范措施，简明实用的病毒处理办法能较有效地帮助他们。
- 掌握一定电脑知识的办公人员或学生。相当一部分办公人员对电脑安全和电脑病毒的认识非常缺乏，处理电脑中毒的方法非常有限，甚至存在不良的电脑操作习惯，一些学生也是如此，希望本书能够帮助他们。
- 中小型公司的网络管理和安全维护人员。中小企业由于受资源所限，往往只是购置一些单机版或带少量客户端的服务器版套件来自己设置。本书在这方面能

够给予维护人员一定的帮助。

- 接受安全和电脑病毒知识培训的人员。本书对实用性和启发性的强调，能较快地帮助他们进行实际操作，可作为电脑安全知识和电脑病毒防治的培训教材和自学用书，建议课时设置时着重考虑上机操作。

本书也能为那些对电脑安全及电脑病毒防治技术有浓厚兴趣的读者，提供一些帮助。

配套光盘的内容简介

为了方便读者学习，本书在所附光盘中录制了一些重要操作的动画演示文件，供读者学习参考。

- 第 3 章：包含操作系统的更新操作过程和两款个人网络防火墙的安装和配置。
- 第 4 章：四款反病毒软件的安装和配置过程。
- 第 5 章：在线查毒、杀毒以及实用工具的使用。
- 第 6 章：下载和安装系统补丁。
- 第 7 章：在线检测木马和反木马软件的使用。
- 第 8 章：安全扫描和实用软件的使用

在配套光盘中有“光盘使用说明.doc”文件，读者可以根据该自述文件的提示使用该光盘。

本书由华中科技大学赵亮、李卫华合作编写。在编写过程中得到了向先波老师、汪金福先生的大力帮助，在此对他们深表谢意。

感谢您选择了本书，也请您把对本书的意见和建议告诉我们。

老虎工作室网站 http://www.laohu.net，电子函件 postmaster@laohu.net。

老虎工作室

2005 年 8 月

目　录

第1章　了解电脑病毒

使用电脑的人都应该听说过电脑病毒，知道电脑病毒会影响电脑正常运行，是电脑使用者最大的敌人。当电脑出现不正常状况的时候，人们的第一反应是感染了电脑病毒。那么电脑病毒到底是什么，他们又是如何运作的呢？在 1994 年 2 月 18 日我国正式颁布实施的《中华人民共和国计算机信息系统安全保护条例》第二十八条中明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”

简单地说，电脑病毒就是一种程序，它能侵入安全系统，对电脑系统进行各种破坏，妨碍操作人员的正常工作，给用户带来损失。同时电脑病毒具有自我复制传播能力，能传播给其他用户，造成大范围的破坏。

本章主要内容：

- 电脑病毒发展现状
- 电脑病毒的由来
- 电脑病毒的特征
- 电脑病毒分类
- 常见病毒类型
- 反病毒技术
- 反病毒动态
- 黑客相关

1.1　电脑病毒发展现状

现今电脑病毒层出不穷，平均每天出现的新病毒约为 30 种，其中一半以上是蠕虫病毒。电脑病毒的传播危害巨大，对人们正常的生产、生活产生了严重影响。图 1-1 显示了近年来全球信息安全损失金额。

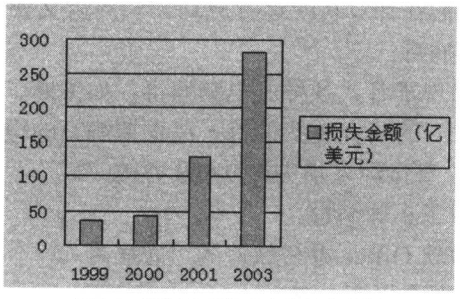

图1-1　近年全球信息安全损失金额

2000 年的时候，针对 DOS 操作系统的病毒还占据了电脑病毒的绝大部分，而随着微软 Windows 操作系统的普及，Windows 操作系统作为主流操作系统成为了电脑病毒的主要攻击目标。利用 Windows 操作系统漏洞的蠕虫病毒泛滥，具体表现如下。

- 2003 年年初爆发的“2003 蠕虫王”病毒，数小时内就使全球主干网陷入瘫痪。
- 2003 年 8 月爆发的全球规模的“冲击波”病毒，疫情超过了“2003 蠕虫王”病毒，它给整个互联网带来了严重冲击，并造成几十亿美元的直接经济损失，感染电脑数目超过了 800 万台。
- 2004 年五一期间爆发的“震荡波”病毒，和“冲击波”病毒一样，是利用系统漏洞，通过网络冲击未安装补丁的电脑，给全球造成了近 5 亿美元的损失。

据中国公安部 2004 年全国信息网络安全状况暨计算机病毒疫情调查结果显示，中国电脑用户电脑病毒的感染率为 87.9%，3 次以上感染电脑病毒的用户数量占全部感染用户数量的 57.1%，感染率最高的电脑病毒是网络蠕虫病毒和针对浏览器的病毒或者恶意代码，其中因未修补、防范软件漏洞等原因造成的安全事件占总数的 66%。

电脑病毒呈现出网络化、多样化和集成黑客技术等趋势。电脑病毒的传播和技术发展越来越依赖于网络，通过网络传播的邮件病毒、蠕虫病毒已经成为主要的病毒类型。部分病毒不仅可以通过电子邮件，也可以利用其他移动介质传播，不仅可以堵塞网络，也可以破坏用户电脑的文件。利用密码表探测弱口令密码、给系统留下后门、发动分布式拒绝服务攻击（DDoS 攻击）等方式已经成为电脑病毒传播破坏的常见手段。

可以预料，电脑病毒作为电脑技术发展的副产品将会长期存在。我们还将在很长一段时间内与电脑病毒共存。如何防止电脑病毒入侵自己的电脑，如何清除隐藏在电脑中的电脑病毒，是每一个电脑用户必须学会的知识。

1.2　电脑病毒的由来

20 世纪 60 年代的时候，Bell 实验室的 3 名年轻程序员编制了一组名为“核心大战”（Core War）的游戏，这是第一个有着破坏、复制和修复功能的程序。

1977 年夏天，美国科普小说家托马斯·捷·瑞安的科幻小说《P-1 的春天》（The Adolescence of P-1）中描写了一种可以在电脑中互相传染的病毒，病毒最后控制了 7000 台电脑，造成了一场灾难。

1983 年 11 月 3 日，计算机安全专家弗雷德·科恩研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼将它命名为计算机病毒（Computer Viruses），并在计算机安全讨论会上正式提出，专家们在计算机上运行成功，一周后又获准进行 5 个实验的演示，从而诞生了世界上第一个电脑病毒。

1987 年，在世界各地出现了各式各样的电脑病毒，如大麻、黑色星期五等。

1988 年 11 月 2 日，23 岁的研究生罗伯特·莫里斯编写的电脑病毒发作范围扩展到了 5 个计算机中心和 12 个地区，直接经济损失达 9 600 万美元。

1988 年底，在我国发现了小球病毒。

1996 年，出现了针对微软 Office 办公软件的“宏病毒”。

电脑病毒的产生原因主要有以下几种。

(1) 为了某种商业、政治目的，或者为了满足个人破坏欲望，以破坏用户电脑系统、产生大范围破坏为目标，恶意编制电脑病毒。这类病毒一般破坏性大，传播范围比较广。大部分病毒都属于这种，如流行的 Mydoom、震荡波等。

(2) 一些电脑爱好者出于兴趣，也可能只是为了满足自己的表现欲望，编写出一些玩笑性的、非恶意的电脑病毒。这类病毒一般破坏性不大。

(3) 软件厂商为了防止产品被非法复制和使用，编制一些程序对产品进行加密，当产品被非法使用时，该程序将自动激活产生破坏作用。如江民逻辑炸弹，就能够改写盗版用户电脑的分区表使软硬盘皆不能启动电脑。

(4) 产生于实验室，作为娱乐程序如“核心大战”，或者设计的有用程序，被不小心传播开来。

1.3 电脑病毒的特征

电脑病毒也是程序，不过和正常的程序相比，它有独特的地方。具体来说，它有如下 4 个特征。

- 传染性

  电脑病毒对文件或者操作系统进行非法操作后，使文件或者操作系统成为新的传播源。特别是通过网络传播的电脑病毒，甚至可以呈几何级数向外扩散。电脑病毒的传染性大大增加了病毒的破坏性和影响力。

- 破坏性

  文件型病毒往往通过修改文件和程序对系统进行破坏，引导型病毒往往通过修改软盘或者硬盘的引导扇区进行破坏，宏病毒通过感染文档文件进行破坏。破坏力的大小由病毒制作者的意愿决定。

- 隐蔽性

  一般说来电脑病毒为了达到它大肆传染的目的，会通过各种方法隐藏自身。对于数据、文件和操作系统的破坏往往不容易被外人察觉。很多病毒文件也将自身设定为隐藏或者系统文件而达到隐蔽的目的。

- 触发性

  部分病毒的发作有具体的条件，这个条件可能是时间、日期或者特定程序的运行。例如大名鼎鼎的 CIH 病毒 1.2 版本就是在每年的 4 月 26 日发作，而 1.4 版本将发作时间改为每月的 26 日，诺维格病毒设定在 2004 年 2 月 1 日~2004 年 2 月 12 日对 www.sco.com 网站实施拒绝服务（DoS）攻击。

电脑病毒破坏性非常明显，不仅每个病毒有其特定的破坏症状，而且同一类病毒通常表现出相似的特征，如邮件病毒利用 Outlook 软件发送群体信件、蠕虫病毒不停发送数据包、恶意网页代码锁定浏览器主页等，这些是非常明显的病毒手法，但即使是未感染病毒的系统，由于硬件和软件的故障，也可能表现出类似于电脑病毒的症状。要区分这两种情况，需要累积一定的经验，避免遇到系统不正常就误以为是感染了电脑病毒。

1.4 电脑病毒分类

据杀毒软件厂商赛门铁克公司的调查，到目前为止，世界上的病毒约有 6 万余种，并且

以每天 30 余种的速度增加。本节我们分别按病毒攻击的操作系统、病毒的破坏状况、感染的内容对电脑病毒进行分类，并且介绍影响较广的蠕虫病毒、邮件病毒、恶意网页代码和木马，最后给出防范意见。

1.4.1　按病毒攻击的操作系统分类

根据病毒所攻击的操作系统，可将电脑病毒分为以下几类。

(1)　攻击 DOS 操作系统的病毒

这类病毒出现得最早、最多，但随着 DOS 操作系统被 Windows 操作系统所取代，这类病毒已经很少影响到目前的电脑。

(2)　攻击 Windows 操作系统的病毒

因为微软公司的 Windows 操作系统已经成为主流操作系统，所以病毒制造者将攻击目标转移到 Windows 操作系统上来。最新出现的病毒绝大部分都是针对 Windows 操作系统的，本书所介绍的电脑病毒就是指这类病毒。

(3)　攻击 UNIX 操作系统的病毒

UNIX 操作系统应用非常广泛，特别是应用在中型和大型机上。UNIX 病毒将对网络服务造成较大冲击。

(4)　攻击 Linux 操作系统的病毒

Linux 是许多电脑爱好者的第二操作系统，许多中型、大型计算机上也安装了 Linux 操作系统。随着 Linux 的流行，针对 Linux 的病毒有增多的趋势。

(5)　攻击 MAC 操作系统的病毒

攻击 MAC 操作系统的病毒已经出现。

(6)　其他操作系统

攻击某种机型的手机蠕虫病毒已经出现。虽然到目前为止只出现了概念性的手机蠕虫病毒“卡波儿”和甚至无法称之为病毒的具有破坏性的短信，但是随着即时通信的发展，手机可能成为病毒的另一个舞台。

1.4.2　按病毒的破坏状况分类

根据病毒对系统的破坏程度，将电脑病毒分为以下几类。

(1)　良性电脑病毒

良性电脑病毒类似于恶作剧，只是不断复制自身进行传播，在用户电脑中弹出图片、声响等，不会破坏用户电脑的数据。这类病毒虽然称为良性病毒，但是仍然会对电脑的性能产生一定影响。每年的愚人节都会出现这样恶作剧般的良性电脑病毒。

良性电脑病毒的危害程序示意图如图 1-2 所示。

(2)　恶性电脑病毒

恶性电脑病毒对电脑的性能造成严重影响，破坏用户文件，导致系统运行缓慢甚至死机，严重影响电脑正常运行。大多数的病毒都是属于恶性电脑病毒。恶性电脑病毒危害程序示意图如图 1-3 所示。

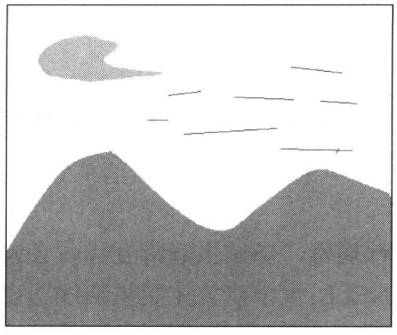

图1-2　良性电脑病毒如轻风吹过，不造成较大影响

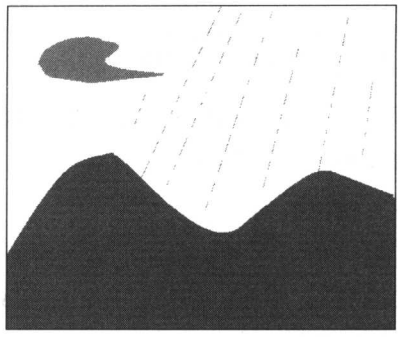

图1-3　恶性电脑病毒如风雨交加，让人苦恼不已

(3)　极恶性电脑病毒

极恶性电脑病毒是电脑的严重威胁，它能删除文件、破坏操作系统，甚至于格式化硬盘、修改 BIOS，破坏计算机硬件。如大名鼎鼎的 CIH 病毒就能破坏硬盘上的所有数据并清除主板上的 BIOS 信息。极恶性电脑病毒危害程度示意图如图 1-4 所示。

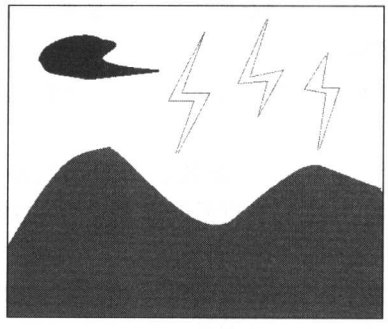

图1-4　极恶性电脑病毒如电闪雷鸣，使人躲之不及

1.4.3　按感染的内容分类

根据病毒感染内容的不同，将电脑病毒分为以下几类：

(1)　引导型病毒

感染软盘的引导扇区，或者硬盘的引导扇区和主引导记录，一般通过软盘传播。在使用被感染的软盘或者硬盘启动电脑的时候病毒会首先取得系统控制权驻留内存并伺机传播到其他的硬盘或者软盘的引导扇区。引导型病毒并不通过网络传播，所以感染此类病毒的机会已经很少。

(2)　程序型病毒

将病毒附加到可执行文件上。当运行被感染的文件时，将会首先运行病毒代码，病毒代码运行完后才继续运行正常的文件。通常接触到的病毒都属于这一类。

(3)　宏病毒

随着微软 Office 办公软件的通用化，出现了一类针对 Office 办公软件的电脑病毒。与其他病毒不同，宏病毒并不感染程序文件，只感染文档文件。宏病毒通过修改 Word 定义的宏（覆盖或者重新定义 Word 中的宏定义），达到破坏的目的。

1.5 常见病毒类型

下面介绍常见的电脑病毒类型，这些电脑病毒命名的依据是人们对于病毒的通称，是用户接触最多的病毒类型。

一、蠕虫病毒

蠕虫病毒又称 Worm，是通过网络传播的一种恶性病毒，当蠕虫病毒发作时会向网络中发送大量数据，甚至于堵塞网络。1988 年美国 CORNELL 大学研究生莫里斯编写出世界上第一个蠕虫病毒。

蠕虫病毒大致可分为以下两类。

一类是利用系统漏洞传播并主动进行攻击的蠕虫病毒，如上述造成较大影响的冲击波、震荡波都是属于这类。这类蠕虫的攻击性非常明显，针对未修补漏洞的系统进行攻击，能对网络进行大面积的破坏，但是对已经修复漏洞的系统不起作用，清除这类病毒通常也很简单。

另一类传播方式比较复杂多样，如邮件病毒，就是通过发送大量病毒邮件来达到传播自身的目的，这类病毒相对较难清除。

蠕虫病毒虽然危险，但如果注意以下几点，小心防范，还是能避免大多数的蠕虫病毒侵扰。

(1) 定时到微软网站进行更新，及时安装最新的系统补丁。大部分蠕虫病毒都是利用系统漏洞传播，打上补丁能有效防范部分蠕虫病毒。
(2) 关闭不需要的系统服务。
(3) 使用防火墙和反病毒软件，反病毒软件应该及时更新病毒库。
(4) 对于邮件群发蠕虫病毒，要及时查杀。

下面给出部分蠕虫病毒对应的系统漏洞：

- 冲击波病毒（Blaster）
  利用 DCOM RPC 漏洞（参见Microsoft 安全公告 MS03-026）。
- 冲击波杀手病毒（Welchia）
  利用 DCOM RPC 漏洞（参见Microsoft 安全公告 MS03-026）。
  利用 WebDav 漏洞（参见Microsoft 安全公告 MS03-007）。
- 冲击波杀手变种病毒（Welchia.B）
  利用 DCOM RPC 漏洞（参见Microsoft 安全公告 MS03-026）。该蠕虫利用此漏洞专门攻击 Windows XP 系统。
  利用 WebDav 漏洞（参见Microsoft 安全公告 MS03-007）。该蠕虫利用此漏洞专门攻击运行 Microsoft IIS 5.0 的计算机。该蠕虫利用这些漏洞，将会影响 Windows 2000 系统，并可能影响 Windows NT/XP 系统。
  利用 Workstation 服务缓冲区溢出漏洞（参见Microsoft 安全公告 MS03-049）。
  利用 Locator 服务漏洞（参见Microsoft 安全公告 MS03-001）。该蠕虫利用此漏洞专门攻击 Windows 2000 系统。
- 震荡波病毒（Sasser）
  利用微软 SSL 安全漏洞（参见Microsoft 安全公告 MS04-011）。