第一图书网, tushu007.com

<<计算机病毒分析与防范大全>>

图书基本信息

书名：<<计算机病毒分析与防范大全>>

13位ISBN编号：9787121074431

10位ISBN编号：7121074435

出版时间：2008-11

出版时间：电子工业出版社

作者：韩筱卿　等编著

页数：511

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

前言

计算机病毒是一个社会性的问题，仅靠信息安全厂商研发的安全产品而没有全社会的配合，是无法有效地建立信息安全体系的。
因此，面向全社会普及计算机病毒的基础知识，增强大家的病毒防范意识，“全民皆兵”并配合适当的反病毒工具，才能真正地做到防患于未然。
我们很高兴地看到战斗在反病毒领域第一线的专业人士，将自己多年的反病毒经验加以总结，与大家共享，帮助普通的计算机使用者揭开计算机病毒的神秘面纱，这无疑是一件有利于促进信息化发展的好事情。
这本书实用性比较强，较为全面地介绍了计算机病毒的基本知识，分析了典型病毒的特征。

内容概要

本书是作者在信息安全领域多年经验的总结和提炼。
本书从计算机病毒的定义及特征开始，将目前发现的所有计算机病毒加以分类，总结出每一类病毒的共性和特征，提出具有针对性的防范建议，以便普通读者揭开病毒的神秘面纱，构建自己的防范体系。
本书适合计算机安全领域的从业者及爱好者阅读，对计算机普通用户更深入地了解计算机病毒也有莫大的帮助。

作者简介

韩筱卿，1971年生，现任北京瑞星公司副总裁。
从1995年开始涉足计算机反病毒技术研究领域；1997年，参与开发的瑞星杀毒软件第一代产品获中国国家科委(现科技部)国家科技成果奖；参与了CIH病毒、BO黑客、红色代码、尼姆达、HappyTime等多种典型流行病毒的解决处理过程。
2000年组织筹备成立了瑞星数据修复中心，经过多年的发展，使之成为计算机用户数据灾难恢复的首选之地。
先后在清华大学、北京大学、北京理工大学、北京航空航天大学、上海同济大学、四川科技大学等多所高校做关于计算机反病毒技术的专题报告。
王建锋，1971年生，现任北京瑞星公司客户服务总经理。
多年来一直从事反病毒技术研究及技术支持工作。
2000年以来，主要负责重大恶性计算机病毒的应急处理工作，组织并参与创建瑞星客户服务中心呼叫中心系统及计算机病毒应急处理平台，在新型病毒预警、分析以及反病毒策略研究等领域具有丰富的经验。
钟玮，1976年生，现任北京瑞星公司客户服务副总经理兼数据安全部经理，全面负责信息安全增值服务的管理与拓展工作。
2002年以来，参与国务院新闻办、港澳办、中组部、华远集团等国内20余家政府部门及大型企业信息安全整体解决方案及安全外包方案的制订与实施；为中粮集团、中央电视台、微软公司、国务院中直管理局、联合国驻京机构等30余家重点单位长期提供数据安全、数据恢复咨询及数据安全管理项目实施；多次组织并参与信息产业部电子教育中心、清华大学、中科院计算所等国内权威机构信息安全培训项目的实施，具有丰富的信息安全项目实践经验。

书籍目录

第一篇 认识计算机病毒　第1章 什么是计算机病毒　第2章 计算机病毒发展史　第3章 计算机病毒的危害　第二篇 计算机病毒分析　第4章 追根溯源——传统计算机病毒概述　第5章 互联网时代的瘟疫——蠕虫病毒　第6章 隐藏的危机——木马病毒分析　第7章 网页冲浪的暗流——网页脚本病毒分析　第8章 不要和陌生人说话——即时通信病毒分析　第9章 无孔不入——操作系统漏洞攻击病毒分析　第10章 病毒发展的新阶段——移动通信病毒分析　第11章 防人之心不可无——网络钓鱼概述　第12章 强买强卖——恶意软件概述　第13章 其他操作系统病毒　第三篇 反病毒技术　第14章 反病毒技术发展趋势　第15章 基础知识——常见文件格式　第16章 搭建病毒分析实验室　第17章 计算机病毒惯用技术解密　第18章 捕捉计算机病毒　第19章 病毒代码分析　第20章 反病毒技术剖析　第四篇 反病毒产品及解决方案　第21章 中国反病毒产业发展概述　第22章 主流反病毒产品特点介绍　第23章 反病毒安全体系的建立　附录A 计算机安全法规　附录B 新病毒处理流程

章节摘录

插图：第1章　什么是计算机病毒1.1　计算机病毒的定义我们知道，生物界的“病毒”（Virus）是一种没有细胞结构、只有由蛋白质的外壳和被包裹着的一小段遗传物质两部分组成的比细菌还要小的病原体生物。
如H5N1、O一157大肠杆菌、HIV（艾滋病毒）、口蹄疫病毒、狂犬病毒、天花病毒、肺结核病毒、禽流感病毒、埃博拉病毒等。
绝大多数病毒只有在电子显微镜下才能看得到，而且不能独立生存，必须寄生在其他生物的活细胞里才能生存。
由于病毒利用寄主细胞的营养生长和繁殖后代，因此给寄主生物造成极大的危害。
在人类或动物的传染性疾病中，有许多是由病毒感染引起的，如人类所患的病毒性肝炎、流行性感冒、艾滋病、脊髓灰质炎、SARS等疾病，动物中的猪瘟、鸡瘟、牛瘟等瘟疫。
我们通常所说的“计算机病毒”（Computer Virus），实际上应该被称做“为达到特殊目的而制作和传播的计算机代码或程序”，或者被称为“恶意代码”。
这些程序之所以被称做病毒，主要是由于它们与生物医学上的病毒有着很多的相同点（如图1-1所示）。
例如，它们都具有寄生性、传染性和破坏性，有些恶意代码会像生物病毒隐藏和寄生在其他生物细胞中一样寄生在计算机用户的正常文件中，而且会伺机发作，并大量地复制病毒体，感染本机的其他文件和网络中的计算机。
而且绝大多数的恶意代码都会对人类社会生活造成不利的影响，造成的经济损失数以亿计。
由此可见，“计算机病毒”这一名词是由生物医学上的病毒概念引申而来的。
与生物病毒不同的是，计算机病毒并不是天然存在的，它们是别有用心的人利用计算机软、硬件所固有的安全上的缺陷有目的地编制而成的。
从广义上讲，凡是人为编制的，干扰计算机正常运行并造成计算机软硬件故障甚至破坏计算机数据的可自我复制的计算机程序或指令集合都是计算机病毒。
依据此定义，诸如逻辑炸弹、蠕虫、木马程序等均可称为计算机病毒。
按照目前信息安全领域的普遍观点，我们可以总结出计算机病毒的十大特征。

编辑推荐

《计算机病毒分析与防范大全(第2版)》适合计算机安全领域的从业者及爱好者阅读，对计算机普通用户更深入地了解计算机病毒也有莫大的帮助。
将目前发现的所有计算机病毒加以分类，总结出每类的共性和特征，提出具有针对性的防范建议。
以专业的视角介绍反病毒行业病毒分析的流程，帮助读者构建自己的病毒分析实验室。
为初学者设计了非常实用的小实验，并录制了实验内容和实验步骤。
光盘附赠丰富的病毒查杀工具。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com