

<<计算机病毒原理与防范技术>>

图书基本信息

书名：<<计算机病毒原理与防范技术>>

13位ISBN编号：9787030344328

10位ISBN编号：7030344324

出版时间：2012-6

出版时间：科学出版社

作者：秦志光、张凤荔、刘峤

页数：251

字数：454750

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>

<<计算机病毒原理与防范技术>>

内容概要

计算机病毒原理及防范技术主要内容包括计算机病毒概述、计算机病毒的工作机制、计算机病毒的表现、新型计算机病毒的发展趋势、计算机病毒检测技术、典型病毒的防范技术、网络安全、即时通信病毒和移动通信病毒分析、操作系统漏洞攻击和网络钓鱼概述、常用反病毒软件等。

计算机病毒原理及防范技术内容丰富，具有先进性和实用性，既是一本计算机病毒与技术的专著，也是一本计算机病毒与防范技术的教材。

计算机病毒原理及防范技术可作为信息安全、计算机，以及各类信息技术、管理学等专业的大学本科生和硕士研究生的教材或参考书，也可作为从事计算机病毒研究和应用工程开发的科技、管理、工程人员的参考书。

<<计算机病毒原理与防范技术>>

书籍目录

丛书序前言第1章 计算机病毒概述1.1 计算机病毒的产生与发展1.1.1 计算机病毒的起源1.1.2 计算机病毒的发展背景1.1.3 计算机病毒的发展历史1.2 计算机病毒的基本概念1.2.1 计算机病毒的一般特征1.2.2 计算机病毒在网络环境下表现的特征1.2.3 计算机病毒的生命周期1.2.4 计算机病毒的传播途径1.2.5 计算机感染上病毒的一般症状1.3 计算机病毒的分类1.3.1 按照病毒的破坏情况分类1.3.2 按照病毒攻击的系统分类1.3.3 按照病毒的寄生部位或传染对象分类1.3.4 按照病毒攻击的对象分类1.3.5 按照病毒的连接方式分类1.3.6 按照病毒的寄生方式分类1.3.7 按照病毒特有的算法分类1.3.8 按照病毒存在的媒体分类1.3.9 按照病毒的“作案”方式分类1.3.10 Linux平台下的病毒分类1.3.11 网络病毒习题第2章 计算机病毒的工作机制2.1 计算机病毒的工作过程2.1.1 计算机病毒的引导模块2.1.2 计算机病毒的感染模块2.1.3 计算机病毒的表现模块2.2 计算机病毒的引导机制2.2.1 计算机病毒的寄生对象2.2.2 计算机病毒的寄生方式2.2.3 计算机病毒的引导过程2.3 计算机病毒的传染机制2.3.1 计算机病毒的传染方式2.3.2 计算机病毒的传染过程2.3.3 系统型计算机病毒传染机理2.3.4 文件型计算机病毒传染机理2.4 计算机病毒的触发机制2.5 计算机病毒的破坏机制2.6 计算机病毒的传播机制习题第3章 计算机病毒的表现3.1 计算机病毒发作前的表现3.1.1 计算机经常无缘无故死机3.1.2 操作系统无法正常启动3.1.3 运行速度异常3.1.4 内存不足的错误3.1.5 打印、通信及主机接口发生异常3.1.6 无意中要求对软盘进行写操作3.1.7 以前能正常运行的应用程序经常死机或者出现非法错误3.1.8 系统文件的时间、日期和大小发生变化3.1.9 宏病毒的表现现象3.1.10 磁盘空间迅速减少3.1.11 网络驱动器卷或共享目录无法调用3.1.12 陌生人发来的电子邮件3.1.13 自动链接到一些陌生的网站3.2 计算机病毒发作时的表现3.2.1 显示器屏幕异常3.2.2 声音异常3.2.3 硬盘灯不断闪烁3.2.4 进行游戏算法3.2.5 Windows桌面图标发生变化3.2.6 计算机突然死机或重启3.2.7 自动发送电子邮件3.2.8 鼠标、键盘失控3.2.9 被感染系统的服务端口被打开3.2.10 反计算机病毒软件无法正常工作3.3 计算机病毒发作后的表现3.3.1 硬盘无法启动,数据丢失3.3.2 文件、文件目录丢失或被破坏3.3.3 数据密级异常3.3.4 使部分可软件升级的主板的BIOS程序混乱3.3.5 网络瘫痪3.3.6 其他异常现象习题第4章 新型计算机病毒的发展趋势4.1 计算机病毒的发展趋势4.1.1 网络化4.1.2 人性化4.1.3 隐蔽化4.1.4 多样化4.1.5 平民化4.1.6 智能化4.2 新型计算机病毒发展的主要特点4.2.1 新型计算机病毒的主要特点4.2.2 基于Windows的计算机病毒4.2.3 新型计算机病毒的传播途径4.2.4 新型计算机病毒的危害4.2.5 电子邮件成为计算机病毒传播的主要媒介4.2.6 新型计算机病毒的最主要载体4.3 新型计算机病毒的主要技术4.3.1 ActiveX与Java4.3.2 计算机病毒驻留内存技术4.3.3 修改中断向量表技术4.3.4 计算机病毒隐藏技术4.3.5 对抗计算机病毒防范系统技术4.3.6 技术的遗传与结合习题第5章 计算机病毒检测技术5.1 计算机反病毒技术的发展历程5.2 计算机病毒检测技术原理5.2.1 计算机病毒检测技术的基本原理5.2.2 检测病毒的基本方法5.3 计算机病毒主要检测技术和特点5.3.1 外观检测法5.3.2 系统数据对比法5.3.3 病毒签名检测法5.3.4 特征代码法5.3.5 检查常规内存数5.3.6 校验和法5.3.7 行为监测法(主动防御)5.3.8 软件模拟法5.3.9 启发式代码扫描技术5.3.10 主动内核技术5.3.11 病毒分析法5.3.12 感染实验法5.3.13 算法扫描法5.3.14 语义分析法5.3.15 虚拟机分析法习题第6章 典型病毒的防范技术6.1 计算机病毒防范和清除的基本原则和技术6.1.1 计算机病毒防范的概念和原则6.1.2 计算机病毒预防基本技术6.1.3 清除计算机病毒的一般性原则6.1.4 清除计算机病毒的一般过程6.1.5 计算机病毒预防技术6.1.6 计算机病毒免疫技术6.1.7 漏洞扫描技术6.1.8 实时反病毒技术6.1.9 防范计算机病毒的特殊方法6.2 引导型计算机病毒6.2.1 原理6.2.2 预防6.2.3 检测6.2.4 清除6.3 文件型病毒6.3.1 原理6.3.2 预防6.3.3 检测6.3.4 清除6.4 CIH病毒6.5 脚本病毒6.5.1 原理6.5.2 检测6.5.3 清除6.6 宏病毒6.6.1 原理6.6.2 预防6.6.3 检测6.6.4 清除6.7 特洛伊木马病毒6.7.1 原理6.7.2 预防6.7.3 检测6.7.4 清除6.8 蠕虫病毒6.8.1 原理6.8.2 预防6.8.3 清除6.9 黑客型病毒6.9.1 黑客病毒种类6.9.2 攻击方式6.10 后门病毒6.10.1 原理6.10.2 IRC后门计算机病毒6.11 安全建议习题第7章 网络安全7.1 网络安全概述7.1.1 计算机网络面临的威胁7.1.2 网络安全防范的内容7.2 Internet服务的安全隐患7.2.1 电子邮件7.2.2 文件传输(FTP)7.2.3 远程登录(Telnet)7.2.4 黑客7.2.5 计算机病毒7.2.6 用户终端的安全问题7.2.7 用户自身的安全问题7.3 垃圾邮件7.3.1 垃圾邮件的定义7.3.2 垃圾邮件的危害7.3.3 追踪垃圾邮件7.3.4 邮件防毒技术7.4 系统安全7.4.1 网络安全体系7.4.2 加密技术7.4.3 黑客防范7.4.4 安全漏洞库及补丁程序7.5 恶意代码的处理7.5.1 恶意代码的种类7.5.2 恶意代码的传播手法7.5.3 恶意代码的发展趋势7.5.4 恶意代码的危害及其解决方案7.5.5 IE恶性修改7.5.6 IE防范措施7.6 网络安全的防范技巧7.7 用户对计算机病毒的认

<<计算机病毒原理与防范技术>>

识误区习题第8章 即时通信病毒和移动通信病毒分析8.1 即时通信病毒背景介绍8.1.1 什么是即时通信8.1.2 主流即时通信软件简介8.1.3 即时通信软件的基本工作原理8.2 即时通信病毒的特点及危害8.3 即时通信病毒发作现象及处理方法8.4 防范即时通信病毒的安全建议8.5 移动通信病毒背景介绍8.5.1 移动通信病毒的基本原理8.5.2 移动通信病毒的传播途径8.5.3 移动通信病毒的危害8.5.4 移动通信病毒的类型8.6 移动通信病毒的发作现象8.6.1 破坏操作系统8.6.2 破坏用户数据8.6.3 消耗系统资源8.6.4 窃取用户隐私8.6.5 恶意扣取费用8.6.6 远程控制用户手机8.6.7 其他表现方式8.7 典型移动通信病毒分析8.7.1 移动通信病毒发展过程8.7.2 典型手机病毒Cabir8.8 防范移动通信病毒的安全建议习题第9章 操作系统漏洞攻击和网络钓鱼概述9.1 操作系统漏洞9.2 Windows操作系统漏洞9.3 Linux操作系统的已知漏洞分析9.4 漏洞攻击病毒背景介绍9.5 漏洞攻击病毒分析9.5.1 “冲击波”病毒9.5.2 “振荡波”病毒9.5.3 “振荡波”与“冲击波”病毒横向对比与分析9.5.4 “红色代码”病毒9.5.5 solaris蠕虫9.5.6 “震网”病毒9.6 针对ARP协议安全漏洞的网络攻击9.6.1 同网段ARP欺骗分析9.6.2 不同网段ARP欺骗分析9.6.3 ARP欺骗的防御原则9.7 操作系统漏洞攻击病毒的安全建议9.8 “网络钓鱼”背景介绍9.9 “网络钓鱼”的手段及危害9.9.1 利用电子邮件“钓鱼”9.9.2 利用木马程序“钓鱼”9.9.3 利用虚假网址“钓鱼”9.9.4 假冒知名网站“钓鱼”9.9.5 其他“钓鱼”方式9.10 防范“网络钓鱼”的安全建议9.10.1 对金融机构应采取的网上安全防范措施建议9.10.2 对于个人用户的安全建议第10章 常用反病毒软件10.1 反病毒行业发展历史与现状10.1.1 反病毒软件行业的发展历程10.1.2 国内外反病毒软件行业所面临的严峻形势10.2 使用反病毒软件的一般性原则10.2.1 反病毒软件选用准则10.2.2 使用反病毒软件注意要点10.2.3 理想的反计算机病毒工具应具有的功能10.3 常用反计算机病毒工具10.3.1 诺顿网络安全特警10.3.2 McAfee VirusScan10.3.3 PC-cillin10.3.4 卡巴斯基安全部队10.3.5 江民杀毒软件KV201110.3.6 瑞星杀毒软件2011版10.3.7 金山毒霸201110.3.8 微点杀毒软件10.3.9 360杀毒软件10.3.10 小红伞个人免费版10.3.11 ESET NOD32杀毒软件10.3.12 BitDefender杀毒软件习题参考文献

<<计算机病毒原理与防范技术>>

章节摘录

版权页：插图：第1章 计算机病毒概述 计算机病毒与医学上的“病毒”相比不完全相同，计算机病毒不是天然存在的，而是某些人利用计算机软、硬件所固有的弱点所编制的、具有特殊功能的程序。计算机病毒是一个程序，或一段可执行代码，它像生物病毒一样具有独特的复制能力，能够很快蔓延，有很强的感染性、一定的潜伏性、特定的触发性和极大的破坏性，又常常难以被根除。

随着计算机网络的发展，计算机病毒与计算机网络技术结合，其蔓延的速度更加迅速。

计算机病毒是一个靠修改其他程序，并把自身复制品传染给其他程序的程序。

计算机病毒是一种人为的计算机程序，这种程序隐藏在计算机系统的可存取信息资源中，利用计算机系统信息资源进行生存、繁殖，影响和破坏计算机系统的运行。

在《中华人民共和国计算机信息系统安全保护条例》中对计算机病毒有明确的定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，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”。

计算机的信息需要存取、复制和传送，计算机病毒作为信息的一种形式可以随之繁殖、感染和破坏，并且，当计算机病毒取得控制权之后，它会主动寻找感染目标、广泛传播。

随着计算机技术发展得越来越快，计算机病毒技术与计算机反病毒技术的对抗也越来越激烈。

从1983年计算机病毒被首次确认以来，直到1987年才开始在世界范围受到普遍的重视，至今全世界已经发现万余种病毒，并且还在快速增加。

现在每天都要出现几十种新的计算机病毒，其中很多计算机病毒的破坏性非常大，稍有不慎，就会给计算机用户造成严重的后果。

计算机操作系统的弱点往往被计算机病毒利用，所以一方面要提高系统的安全性以预防计算机病毒；另一方面，信息保密的要求又让人在泄密和截获计算机病毒之间无法选择。

这样，计算机病毒与反计算机病毒势必成为一个长期的技术对抗过程。

计算机病毒主要由反计算机病毒软件来对付，而且反计算机病毒技术将成为一项长期的科研任务。

1.1 计算机病毒的产生与发展 1.1.1 计算机病毒的起源 计算机病毒的来源多种多样，一般来自玩笑与恶作剧、报复心理、版权保护等方面，有的是计算机工作人员或业余爱好者纯粹为了寻求开心而制造出来的，有的则是软件公司为保护自己的产品不被非法复制而制造的报复性惩罚。

还有一种情况就是蓄意破坏，它分为个人行为和政府行为两种：个人行为多为雇员对雇主的报复行为，而政府行为则是有组织的战略战术手段。

对病毒的起源有几种说法。

第一种为科学幻想起源说。

1977年，美国科普作家托马斯·丁·雷恩推出轰动一时的《P-1的青春》一书，作者构思了一种能够自我复制、利用信息通道传播的计算机程序，并称之为计算机病毒。

这是世界上第一个幻想出来的计算机病毒。

第二种为恶作剧起源说。

恶作剧者是为了显示一下自己在计算机技术方面的天赋，或是要报复一下他人或单位而编写的计算机病毒，只是和对方开个玩笑。

而出发点有些恶意成分的人所编写的病毒的破坏性很大，世界上流行的许多计算机病毒都是恶作剧者的产物。

<<计算机病毒原理与防范技术>>

编辑推荐

《普通高等教育信息安全类国家级特色专业系列规划教材:计算机病毒原理及防范技术》可作为信息安全、计算机,以及各类信息技术、管理学等专业的大学本科生和硕士研究生的教材或参考书,也可作为从事计算机病毒研究和应用工程开发的科技、管理、工程人员的参考书。

<<计算机病毒原理与防范技术>>

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>