

<<计算机病毒分析与防治简明教程>>

图书基本信息

书名：<<计算机病毒分析与防治简明教程>>

13位ISBN编号：9787302163770

10位ISBN编号：7302163774

出版时间：2007-11

出版时间：清华大学

作者：赵树升

页数：275

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>

<<计算机病毒分析与防治简明教程>>

内容概要

《计算机病毒分析与防治简明教程》全面翔实地介绍了各种病毒的原理，以操作系统的发展为主线，结合病毒的发展过程来综合分析病毒。

在分析工具上，较多地利用了脚本语言、c++和汇编语言，注重理论与实践相结合，每介绍一种类型的病毒，均以实例阐述。

在深入分析和全面阐述之后，《计算机病毒分析与防治简明教程》想向读者揭示，病毒只不过是利用了系统或应用软件提供的某些功能，利用漏洞来进行破坏的一段代码而已。

基于此，病毒并不可怕，病毒是可以清除的，同时和病毒的斗争也将是长期的。

《计算机病毒分析与防治简明教程》结构清晰、内容翔实，既可作为工科院校相关专业的教材，也可作为从事工程设计工作的专业技术人员的参考书。

<<计算机病毒分析与防治简明教程>>

书籍目录

第1章 计算机病毒概述 11.1 计算机病毒的定义 11.2 计算机病毒的特性 11.3 计算机病毒的分类 21.4 计算机病毒的产生与历史 51.4.1 病毒的起源 51.4.2 病毒产生的原因 61.4.3 病毒的发展过程 61.4.4 病毒的发展趋势 81.5 计算机病毒的命名 91.6 计算机病毒的本质 91.6.1 病毒的隐藏位置 91.6.2 病毒对系统功能的利用 101.6.3 病毒对系统漏洞的利用 101.6.4 病毒的一般结构 111.6.5 感染病毒后的常见症状 111.7 病毒的工作机制 111.7.1 病毒的触发机制 121.7.2 病毒的传播机制 121.7.3 病毒的破坏机制 131.8 反病毒技术 131.8.1 反病毒技术发展过程 141.8.2 常见反病毒技术介绍 141.8.3 反病毒技术发展趋势 171.9 本章小结 181.10 习题 18

第2章 引导型病毒分析 192.1 预备知识 192.1.1 磁盘数据结构 192.1.2 系统引导过程与引导扇区分析 222.1.3 读写扇区方式 282.1.4 程序常驻内存 292.2 引导型病毒 302.2.1 引导型病毒工作原理 302.2.2 一个引导型病毒分析 312.3 实验1：引导程序设计 362.4 实验2：接管中断程序设计 412.5 清除病毒程序设计 452.6 本章小结 472.7 习题 47

第3章 DOS文件型病毒分析 493.1 预备知识 493.1.1 COM文件分析 493.1.2 EXE文件分析 493.2 DOS文件病毒 513.2.1 DOS文件病毒原理 513.2.2 病毒对int 21h的利用 513.2.3 一个DOS文件型病毒分析 523.3 实验：用Debug修改COM文件 593.3.1 增加代码原理 613.3.2 增加程序代码 623.4 清除DOS文件病毒 643.5 本章小结 773.6 习题 77

第4章 PE文件病毒 784.1 预备知识：PE文件结构 784.1.1 PE文件结构分析 784.1.2 编程分析PE文件结构 834.2 PE病毒常用技术 854.2.1 API与API的调用 854.2.2 病毒使用API 874.2.3 病毒使用变量 944.3 添加节方式修改PE 954.4 加长最后一节修改PE 1144.5 插入节方式修改PE 1204.6 设计自己的病毒专杀工具 1264.6.1 清除病毒原理 1264.6.2 程序设计实现 1284.7 用重构PE文件结构法防病毒 1294.7.1 自我防病毒原理 1294.7.2 自免疫保护实现 1314.7.3 自免疫演示 1774.8 本章小结 1784.9 习题 178

第5章 网络蠕虫病毒 1795.1 预备知识 1795.1.1 VBScript 脚本 1795.1.2 JavaScript脚本 1805.1.3 组件与脚本对组件的调用 1805.2 网络蠕虫的综述 1825.2.1 网络蠕虫的起源与发展 1825.2.2 网络蠕虫的特点 1845.2.3 蠕虫病毒的传播方式 1845.3 举例：利用Unicode漏洞 1875.3.1 Unicode漏洞的利用 1875.3.2 扫描Unicode漏洞 1885.4 蠕虫与溢出 1915.4.1 溢出解析 1915.4.2 栈溢出举例 1945.4.3 缓冲区溢出漏洞的避免方法 1975.5 典型蠕虫病毒分析 1985.5.1 “美丽莎”病毒分析 1985.5.2 “求职信”病毒介绍 2025.5.3 “冲击波”病毒分析 2045.5.4 “欢乐时光”病毒介绍 2085.6 防范网络蠕虫病毒 2095.7 本章小结 2105.8 习题 210

第6章 木马与远程控制技术 2116.1 预备知识 2116.1.1 套接字与网络编程 2116.1.2 木马分类介绍 2126.2 远程控制通信的实现 2146.2.1 TCP阻塞方式 2146.2.2 TCP非阻塞方式 2156.2.3 UDP方式 2176.2.4 ICMP方式 2186.3 远程控制的控制技术 2216.3.1 屏幕的截取 2226.3.2 虚拟鼠标的操作 2236.3.3 虚拟键盘的操作 2246.3.4 进程管理 2256.4 木马技术揭露 2296.4.1 木马程序的安装 2296.4.2 木马的启动 2306.4.3 木马的隐藏技术分析 2336.5 一个完整的远程控制程序 2366.6 木马的清除方法 2396.6.1 监视端口 2396.6.2 进程内模块监视 2406.6.3 监视文件 2426.6.4 监视注册表 2436.7 试验：清除“广外女生”木马 2446.8 本章小结 2456.9 习题 245

第7章 病毒常用技术分析 2467.1 病毒的加密技术 2467.1.1 脚本代码的加密 2467.1.2 PE文件的加密 2477.1.3 花指令方法 2517.2 病毒的变种、多态与变形 2547.2.1 多态与变形病毒的来历与分类 2557.2.2 多态原理浅析 2567.2.3 变形引擎浅析 2607.3 病毒的一些常用保护方法 2627.3.1 自我删除 2627.3.2 自我复制 2637.3.3 搜索资源（Email地址和共享目录） 2657.4 病毒对系统的破坏 2717.5 本章小结 2747.6 习题 275

参考文献 276

<<计算机病毒分析与防治简明教程>>

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>