

<<计算机病毒揭秘与对抗>>

图书基本信息

书名：<<计算机病毒揭秘与对抗>>

13位ISBN编号：9787121146053

10位ISBN编号：7121146053

出版时间：2011-10

出版时间：电子工业出版社

作者：王倍昌

页数：544

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>

<<计算机病毒揭秘与对抗>>

内容概要

随着计算机及其应用的发展，计算机病毒迅速泛滥，已极大地影响着广大的计算机用户，几乎所有的计算机用户都受到过计算机病毒的困扰。

本书将深入揭秘计算机病毒完成各种功能（如：隐藏自身、隐蔽执行、自动运行、感染正常程序、自我保护等）所使用的病毒技术原理，并且介绍相应的对抗技术，同时也介绍了当今流行的反病毒技术。

掌握这些技术后，就可以开发出自己的计算机病毒查杀工具、计算机病毒分析工具、反病毒扫描工具、系统恢复工具等实用性工具，从而帮助您成为专业的反病毒工程师。

<<计算机病毒揭秘与对抗>>

书籍目录

第1章 计算机病毒概述

- 1.1 计算机病毒基本知识
 - 1.1.1 计算机病毒概念
 - 1.1.2 计算机病毒的特点
 - 1.1.3 计算机病毒的产生与发展
 - 1.1.4 计算机病毒的分类
 - 1.1.5 计算机病毒的命名
- 1.2 计算机病毒的防治
 - 1.2.1 计算机病毒的危害
 - 1.2.2 如何防止计算机中毒
 - 1.2.3 计算机中毒后的处理

第2章 计算机病毒行为揭秘

- 2.1 Windows系统基础知识
 - 2.1.1 Windows系统的NT架构
 - 2.1.2 Windows系统相关概念
- 2.2 计算机病毒常见表现行为及目的
 - 2.2.1 病毒如何爆发
 - 2.2.2 病毒为何长期存在
 - 2.2.3 病毒因何难以察觉
 - 2.2.4 病毒为何难以查杀清除
 - 2.2.5 病毒爆发后对系统的整体影响
- 2.3 计算机病毒通用分析方法
 - 2.3.1 行为分析
 - 2.3.2 代码分析

第3章 Windows系统编程

- 3.1 字符集编码
 - 3.1.1 MBCS (多字节字符系统)
 - 3.1.2 Unicode (统一码)
 - 3.1.3 字符相关的Windows API函数
- 3.2 进程相关开发
 - 3.2.1 进程创建
 - 3.2.2 进程相关操作
 - 3.2.3 进程操作类的封装
- 3.3 线程相关开发及多线程同步控制
 - 3.3.1 线程创建
 - 3.3.2 线程执行原理
 - 3.3.3 线程相关操作
 - 3.3.4 多线程同步控制
- 3.4 注册表操作开发
 - 3.4.1 注册表键的操作
 - 3.4.2 注册表键值的操作
- 3.5 文件、目录、驱动器相关操作开发
 - 3.5.1 文件基本操作
 - 3.5.2 获取文件信息
 - 3.5.3 文件遍历操作

<<计算机病毒揭秘与对抗>>

- 3.5.4 内存映射文件
- 3.5.5 文件夹操作
- 3.5.6 驱动器操作
- 3.6 网络编程
 - 3.6.1 局域网访问控制技术
 - 3.6.2 Socket编程
- 3.7 动态链接库相关开发
 - 3.7.1 DLL程序的开发
 - 3.7.2 DLL程序的利用
- 3.8 服务开发
 - 3.8.1 服务程序的工作原理
 - 3.8.2 服务程序的安装与卸载
 - 3.8.3 一个简单服务程序的开发
 - 3.8.4 服务的遍历
- 第4章 PE文件编程
 - 4.1 PE文件格式概述
 - 4.2 PE结构查看工具
 - 4.3 PE文件解析开发
 - 4.3.1 加载PE文件
 - 4.3.2 封装PE文件操作类
 - 4.3.3 解析节表
 - 4.3.4 解析导入表
 - 4.3.5 解析导出表
 - 4.3.6 解析资源
 - 4.3.7 解析重定位表
 - 4.3.8 处理附加数据
- 第5章 计算机病毒的惯用技术实现原理及对策
 - 5.1 隐藏执行——注入技术
 - 5.1.1 DLL注入
 - 5.1.2 注入DLL应对措施
 - 5.1.3 远程代码注入
 - 5.1.4 远程代码注入杀毒方案
 - 5.2 病毒各种自启动手段揭秘
 - 5.2.1 利用系统自启动功能
 - 5.2.2 利用SPI
 - 5.2.3 DLL劫持
 - 5.2.4 BHO
 - 5.2.5 服务劫持
 - 5.3 计算机病毒感染原理及清除方法
 - 5.3.1 常见感染型病毒的感染原理
 - 5.3.2 感染型病毒的查杀
 - 5.3.3 各种感染型病毒的清除示例
 - 5.4 加壳与脱壳
 - 5.4.1 壳的种类
 - 5.4.2 壳的原理
 - 5.4.3 简易加壳软件的实现
 - 5.4.4 静态脱壳机的编写

<<计算机病毒揭秘与对抗>>

第6章 高级反病毒技术

6.1 虚拟机技术

6.1.1 虚拟机的实现

6.1.2 虚拟机在反病毒领域中的应用

6.1.3 病毒与虚拟机的对抗

6.2 云查杀技术

6.3 启发式扫描技术

6.3.1 动态启发式

6.3.2 静态启发式

6.4 主动防御技术

<<计算机病毒揭秘与对抗>>

编辑推荐

这本《计算机病毒揭秘与对抗》由王倍昌编著，共分为六章：第1章讲解了计算机病毒的基础知识。

第2章讲解反病毒相关的Windows系统知识并且概述了计算机病毒的奥秘。

第3章讲解Windows系统开发相关知识以及计算机病毒相关的Windows编程技术。

第4章讲解PE文件格式。

第5章讲解计算机病毒常用的技术原理和使用C/C++语言的实现细节，以及相关反病毒技术的实现。

第6章讲解当今比较流行、比较高级的反病毒技术。

<<计算机病毒揭秘与对抗>>

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>