<<计算机病毒防治实用教程>>

图书基本信息

书名：<<计算机病毒防治实用教程>>

13位ISBN编号：9787111312017

10位ISBN编号：7111312015

出版时间：2010-9

出版时间：李治国 机械工业出版社 (2010-09出版)

作者：李治国 编

页数：214

前言

计算机病毒在今天已经成为影响信息系统安全最严重的因素之一。
因此，社会对计算机病毒防治方面专业人才的需求也在快速增长。
全国各大本科高校和高职院校相继开设了计算机病毒防治的相关课程以满足社会对这方面人才的需求。
在全国高职院校中重庆电子工程职业学院较早开设了信息安全专业，并在信息安全行业专家和知名信息安全企业的协助下，编写了信息安全专业的系列教材，本书即为该系列教材中的核心教材之一。
本书首先全面介绍了计算机病毒的基础知识；再以病毒行为分析、病毒源码分析、病毒清除和病毒防治为主线，对多种类型的典型病毒进行了深入剖析；最后系统地阐述了反病毒程序设计和病毒防治策略。
本书共6章，每章的主要内容如下所述：第1章阐述了计算机病毒的基本原理和基本概念。
内容涉及计算机病毒的定义、特点、分类、技术特征和计算机病毒的命名方法等，同时还介绍了计算机病毒的发展过程，并列举了病毒史上公认的十大病毒产生的危害。
第2章介绍了如何搭建计算机病毒分析平台，这是进行病毒行为分析的基础。
第3章对大量典型病毒案例进行了深入剖析。
主要内容包括注册表的原理和作用，网页脚本病毒、宏病毒、蠕虫病毒和木马病毒的行为分析、源码分析和清除原理。
第4章介绍了计算机病毒的主要防范措施、计算机病毒的免疫技术和查毒技术，并对多种病毒的查毒方法进行了详细对比，分析了不同查毒方法的自身特点。
第5章介绍了反病毒软件的编制技术。
主要内容包括杀毒技术的发展情况、最新的杀毒技术、反病毒软件的体系结构和杀毒软件案例剖析。
最后列举了简单杀毒程序实例，指导读者进行反病毒程序的编写训练。
第6章介绍了计算机病毒防治的总体策略和目前市场上的主流病毒防治产品的情况。
作者在编写过程中，得到了龚小勇教授和武春岭老师的帮助和指导，以及趋势科技公司的鼎力支持，在此一并表示衷心的感谢！
笔者分析病毒已有多年，从事这方面的教学工作也已多年，但受水平所限，书中内容难免有不足之处，恳请读者和专家赐教。

<<计算机病毒防治实用教程>>

内容概要

本课程是高职高专信息安全专业的必修课程。

《计算机病毒防治实用教程》从计算机病毒的概念及其发展趋势开始，分类介绍了网页脚本病毒、宏病毒、蠕虫病毒及木马病毒等典型病毒，每类病毒都结合实例，从病毒防治的技术原理、病毒行为分析及防治措施等方面讲解了几个具有代表性的防治技术，最后还介绍了防病毒软件技术的发展方向和有代表性厂家产品的发展情况。

《计算机病毒防治实用教程》可作为高职高专院校信息安全专业、网络技术专业等的教学用书。也可作为防病毒软件设计者的参考书。

<<计算机病毒防治实用教程>>

书籍目录

章节摘录

插图：1996年，计算机病毒的破坏能力又有了进一步提高，为了躲避反病毒软件的监视，新的变形病毒应运而生。
以前那种采用特征代码串来标识计算机病毒的技术又开始失效。
最先传人中国的是“幽灵”，随后是“猴子”等两栖（同时感染系统和文件）变形病毒，这些病毒先后在一定范围内流行，不过由于反病毒软件的及时跟进，以及国人已经习惯于综合使用各种反病毒软件，因此这些病毒都没有能掀起太大的风浪。
令人担忧的是，随着国际互连网络的普及，计算机病毒编写者开始通过互联网络来交流编程技术和心得体会。
网上也出现了专门的变形病毒引擎，利用这些引擎，任何人都可以编写出带无穷变形功能的计算机病毒。
1997年，在沉寂了一小段时间以后，病毒又找到了新的突破点，部分计算机用户利用了功能强大的宏语言，编制了各色各样的宏病毒。
随后是各种各样的好奇者，简单地利用宏编辑器改造了自己的产品。
据一些反病毒软件站点报告，全世界一个星期就有近千只新病毒出现，而其中绝大部分是宏病毒。
1997年下半年，一个叫做SPY的可以攻击NE（16位Windows格式可执行文件）格式程序的病毒，曾经在南方流行一时，敲响了向Windows进攻的警钟。
到了1998年的年中，CIH病毒终于攻破了Windows 95平台。
这个病毒创造了几个第一，即第一个流行的攻击PE格式32位保护模式程序的病毒；第一个可以破坏计算机硬件的病毒。
以前的病毒最多只能破坏软件系统，而CIH病毒不但直接利用IOS指令摧毁硬盘数据（即使主板具有防病毒功能，也无能为力），而且通过清洗存储在Flash EPROM中的BIOS指令，导致系统主板无法工作，彻底破坏机器。
CIH病毒利用虚拟设备驱动程序（VXD）技术逃过了当时所有反病毒软件的监测，并且令目前所有宣称可以防病毒的主板大失颜面。
据网上的一封道歉信报道，CIH病毒是中国台湾的一名学生编写的。
通过反编译发现，这个病毒系利用SIDT指令来获取系统的核心级执行权限，进而截获系统核心功能的调用。
这实际上可以说是Windows 95系统（Windows 98同样有这个问题）的一个漏洞。
所幸的是，Windows NT已经封锁了这一条指令，因此CIH病毒无法在Windows NT下兴风作浪。

编辑推荐

《计算机病毒防治实用教程》由重庆电子工程职业学院国家示范院校重点建设专业信息安全技术专业，组织具有丰富教学经验的一线教师与知名企业工程师一起开发，以面向企业应用为目标、以工程案例为中心、以任务驱动为主线组织教学内容，注重实践能力的培养。

<<计算机病毒防治实用教程>>

版权说明