

<<恶意代码防范>>

图书基本信息

书名：<<恶意代码防范>>

13位ISBN编号：9787040290554

10位ISBN编号：7040290553

出版时间：2010-7

出版时间：高等教育

作者：刘功申//张月国//孟魁

页数：364

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>

## &lt;&lt;恶意代码防范&gt;&gt;

## 前言

信息安全是一个复杂的系统工程。

在这个系统工程中，不能仅仅依靠技术或管理的任何一方来解决问题，而应该从技术和管理两方面进行统筹考虑。

一套好的管理制度和策略应该是以单位实际情况为主要依据，能及时反映单位实际情况变化，具有良好的可操作性，由科学的管理条款组成。

随着信息技术的发展，信息资源管理将被作为国家战略来推进，企业竞争焦点也将落在对信息资源的开发利用上。

“三分技术、七分管理、十二分数据”的说法成为现代企业信息化管理的标志性注释。

信息资源已经成为继土地和资本之后最重要的财富来源。

对于恶意代码及其防范来说，曾经有一些简单的认识：计算机不可能因为仅仅读了一封电子邮件而感染恶意代码；恶意代码不可能损害计算机硬件设备；计算机不可能因为浏览一个图形文件而染毒；杀毒软件是防范恶意代码的一切；数据备份和恢复对防范恶意代码无关紧要；恶意代码防范策略是虚无缥缈的内容等等。

但是，在恶意代码迅速发展的今天，这些说法都已经过时，我们必须更新关于恶意代码及其防范工作的知识。

本书是在作者多年教学经验和信息安全社会培训工作的基础上编写而成的，力求反映作者近年来的最新科研成果。

全书共分为13章，在简单介绍恶意代码的基本概念和类别的基础上，重点探讨了恶意代码防范的思路、技术、方法和策略，并给出了恶意代码的防治方案。

本书各章内容简介如下。

第1章恶意代码概述。

本章分析了引入恶意代码概念的原因，介绍了恶意代码的种类和特征，并在此基础上探讨了恶意代码的关键历史转折点、传播途径、感染症状、命名规则及未来发展趋势等相关问题。

第2章典型恶意代码。

在总结现有恶意代码类别的基础上，介绍了几款典型的恶意代码：普通计算机病毒、蠕虫、特洛伊木马、恶意脚本、流氓软件、逻辑炸弹、僵尸网络、网络钓鱼、R00tkit、智能移动终端恶意代码、垃圾信息、其他新型恶意代码等。

第3章恶意代码防范原理。

恶意代码防范技术分为6个层次：检测、清除、预防、免疫、策略、数据备份及恢复。

在此详细介绍了恶意代码的检测原理和方法、恶意代码清除的原理和方法、恶意代码的防范、恶意代码的免疫。

第4章数据备份与数据恢复。

随着恶意代码清除难度的加大，数据备份和数据恢复技术走向前台。

数据备份及恢复技术不仅是灾准备份和灾难恢复的核心技术，也是恶意代码领域的核心内容。

第5章商业安全软件的常用技术。

本章主要介绍了商业软件采用的特殊防范技术，例如内存检测技术、广谱杀毒技术、虚拟机技术、驱动程序技术、云查杀技术等。

## <<恶意代码防范>>

### 内容概要

《恶意代码防范》是在作者多年教学经验和信息安全社会培训工作的基础上编写而成的，力求反映作者近年来的最新科研成果。

全书共分为13章，在简单介绍恶意代码的基本概念和类别的基础上，重点探讨了恶意代码防范的思路、技术、方法和策略，并给出了恶意代码的防治方案。

《恶意代码防范》内容深入浅出，用通俗的语言和实例向读者展示恶意代码防范的知识。教材配套资源丰富，易学易教，包括PPT电子版课件、多种题型的题库、实验用软件和源代码等。

《恶意代码防范》适合作为普通高等学校信息安全及相关专业本科生的教材，也可作为相关领域的工程技术人员的参考书。

## &lt;&lt;恶意代码防范&gt;&gt;

## 书籍目录

第1章 恶意代码概述1.1 恶意代码概念的产生1.2 恶意代码的概念1.3 恶意代码的发展历史1.4 恶意代码的种类1.5 恶意代码的传播途径1.6 感染恶意代码的症状1.6.1 恶意代码的表现现象1.6.2 与恶意代码现象类似的硬件故障1.6.3 与恶意代码现象类似的软件故障1.7 恶意代码的命名规则1.8 恶意代码的最新发展趋势1.9 习题第2章 典型恶意代码2.1 传统计算机病毒2.2 蠕虫2.3 特洛伊木马2.4 恶意脚本2.5 流氓软件2.6 逻辑炸弹2.7 后门2.8 僵尸网络2.9 网络钓鱼2.10 Rootkit工具2.11 智能移动终端恶意代码2.12 垃圾信息2.13 其他恶意代码2.14 习题第3章 恶意代码防范原理3.1 恶意代码防范技术的发展3.2 恶意代码防范技术的发展3.3 恶意代码防范理论模型3.4 恶意代码防范思路3.5 恶意代码的检测3.5.1 恶意代码的检测原理3.5.2 恶意代码的检测方法3.5.3 自动检测的源码分析3.6 恶意代码的清除3.6.1 恶意代码的清除原理3.6.2 恶意代码的清除方法3.7 恶意代码的防范3.7.1 系统监控技术3.7.2 源监控技术3.7.3 个人防火墙技术3.7.4 系统加固技术3.8 恶意代码的免疫3.8.1 恶意代码的免疫原理3.8.2 免疫的方法及其特点3.8.3 数字免疫系统3.9 恶意代码处理流程3.10 章节实验3.11 习题第4章 数据备份与数据恢复4.1 数据备份与数据恢复的意义4.2 数据备份4.2.1 个人PC备份策略4.2.2 系统级备份策略4.3 数据恢复4.4 数据恢复工具箱4.5 数据备份及恢复常用工具4.5.1 Easy Recovery工具使用4.5.2 注册表备份工具4.5.3 Foxmail通信簿备份及恢复4.6 章节实验4.7 习题第5章 商业安全软件的常用技术5.1 恶意代码防治技术的进展5.2 商业软件采用的防治技术5.2.1 内存检测技术5.2.2 广谱特征码5.2.3 虚拟机技术5.2.4 驱动程序技术5.2.5 云查杀技术5.2.6 无缝连接技术5.2.7 检查压缩文件5.2.8 沙盘技术5.2.9 启发式扫描技术5.2.1 OPE病毒的启发式特征5.2.1 1网络恶意代码立体防御技术5.3 现有防治技术的缺陷5.4 习题第6章 QAV软件分析与使用6.1 项目组成6.2 Scanner Daemon基本框架6.2.1 main-ehass分析6.2.2 扫描配置模块6.2.3 病毒特征码模块6.2.4 扫描引擎模块6.2.5 文件系统支持模块6.3 测试示例6.4 Scanner Daemon使用实验6.4.1 Scanner Daemon配置说明6.4.2 Scanner Daemon使用说明6.5 Virus Hammer分析与使用6.5.1 Vims Hammer运行环境6.5.2 Linux环境下的启动6.5.3 Windows环境下的启动6.5.4 Virus Hammer使用6.6 Pattern Finder分析与使用6.6.1 Pattern Finder工作原理6.6.2 Pattern Finder运行环境6.6.3 Pattern Finder启动6.6.4 Pattern Finder使用6.7 章节实验6.8 习题第7章 ClamAV软件分析与使用7.1 ClamAV总体结构7.2 ClamAV使用说明7.3 ClamAV安装与配置7.4 源代码分析7.4.1 ClamAV配置7.4.2 病毒特征代码库7.4.3 clamd初始化7.4.4 elamdscarl模块7.4.5 clamd响应模块7.4.6 elamd扫描模块7.5 章节实验7.6 习题第8章 恶意代码检测用匹配算法8.1 模式匹配算法概述8.2 经典单模式匹配算法8.3 多模式匹配算法8.3.1 经典多模式匹配DFSA算法8.3.2 基于有序二叉树的多模式匹配算法8.4 HASH算法8.4.1 算法条件8.4.2 词典构造8.4.3 查找过程8.4.4 改进思路8.5 章节实验8.6 习题第9章 常用杀毒软件及解决方案9.1 恶意代码防范产业发展9.2 国内外反病毒软件评测机构9.2.1 WildList——恶意代码清单资料库9.2.2 德国AV-Test评测机构9.2.3 英国VirusBulletin评测机构9.2.4 奥地利AV-Comparatives评测机构9.2.5 Veilzon公司的ICSA评测机构9.2.6 westCoastLabs——西海岸实验室9.2.7 中国的反病毒软件评测机构9.3 国内外著名杀毒软件比较9.3.1 杀毒软件必备功能9.3.2 流行杀毒产品比较9.3.3 恶意代码防范产品的地缘性9.4 企业级恶意代码防治方案9.4.1 企业恶意代码防范需求9.4.2 企业网络的典型结构9.4.3 企业网络的典型应用9.4.4 恶意代码在网络上传播的过程9.4.5 企业网络恶意代码防范方案9.5 习题第10章 Linux系统杀毒工具10.1 avast ! 杀毒软件IO.1.1 avast ! 的主要功能10.1.2 avast ! 安装10.1.3 avast ! 使用与配置10.2 ClamTk杀毒软件10.2.1 ClamTk安装与更新10.2.2 ClamTk使用与配置10.3 AntiVir杀毒软件10.3.1 AntiVir安装与更新10.3.2 AntiVir配置与使用10.3.3 YkAntiVir安装与使用10.4 其他工具10.4.1 rkhunter具10.4.2 chkrootkit工具10.5 章节实验10.6 习题第11章 windows系统防范工具11.1 瑞星杀毒软件11.1.1 瑞星杀毒软件的功能11.1.2 瑞星杀毒软件的使用11.1.3 瑞星杀毒软件的配置11.2 木马克星11.2.1 木马克星概述11.2.2 木马克星的安装11.2.3 木马克星的使用11.3 个人防火墙工具11.3.1 windows防火墙11.3.2 常规功能11.3.3 例外功能11.3.4 高级功能11.4 其他防范恶意代码工具11.4.1 Regmon工具\_11.4.2 FileMon工具11.4.3 ProcessExplorer工具11.5 章节实验11.6 习题第12章 智能手机安全防范工具12.1 手机安全防范工具概述12.1.1 国外智能手机恶意代码防范产品12.1.2 国内智能手机恶意代码防范产品12.2

<<恶意代码防范>>

Kaspersky手机版杀毒软件12.2.1 KAVMobile安装12.2.2 KAVMobile使用12.3 智能手机版任务管理器12.4 章节实验12.5 习题第13章 恶意代码防治策略13.1 恶意代码防治策略的基本准则13.2 国家层面上的防治策略13.3 单机用户防治策略13.3.1 一般技术措施13.3.2 个人用户上网基本策略13.4 建立安全的单机系统13.4.1 打牢基础13.4.2 选好工具13.4.3 注意方法13.4.4 应急措施13.4.5 自我提高13.5 企业用户防治策略13.5.1 建立防御计划13.5.2 执行计划13.5.3 恶意代码扫描引擎相关问题13.5.4 额外的防御工具13.6 未来的防范措施13.7 恶意代码犯罪相关法律法规基础13.8 习题附录 恶意代码相关网上资源参考文献

## <<恶意代码防范>>

### 章节摘录

插图：2.专业化发展2003年，媒体报道发现了第一例感染手机的恶意代码，也有人认为这不是一个真正的恶意代码。

手机恶意代码、PDA恶意代码的出现标志着恶意代码开始向专业化方向发展。

由于这些设备都采用嵌入式操作系统并且软件接口较少，以往很少有恶意代码制造者涉足这个领域。随着时间的推移、技术细节的公开，已经有人开始转向这个领域。

3.简单化发展与传统计算机病毒不同的是，许多恶意代码是利用当前最新的编程语言与编程技术来实现的，它们易于修改以产生新的变种，从而避开安全防范软件的搜索。

例如，“爱虫”是用VBScript语言编写的，只要通过Windows自带的编辑软件修改恶意代码中的一部分，就能轻而易举地制造出新变种，以躲避安全防范软件的追击。

4.多样化发展新恶意代码可以是可执行程序、脚本文件、HTML网页等多种形式，并正向电子邮件、网上贺卡、卡通图片、ICQ、OICQ等发展。

更为棘手的是，新恶意代码的手段更加阴狠，破坏性更强。

据计算机经济研究中心的报告显示，在2000年5月，爱虫、蠕虫大流行的前5天，就造成了67亿美元的损失。

## <<恶意代码防范>>

### 编辑推荐

《恶意代码防范》是在作者多年教学经验和信息安全社会培训工作的基础上编写而成，力求反映作者近年来的最新科研成果。

《恶意代码防范》内容深入浅出。

用通俗的语言和实例向读者展示恶意代码防范的知识。

在简单介绍恶意代码基本概念和类别的基础上，本教材重点探讨了恶意代码防范的思路、技术、方法和策略。

《恶意代码防范》配套资源丰富，易学易教，包括PPT电子课件、多种题型的题库、实验用软件和源代码等。

#### 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>