

<<计算机病毒防范艺术>>

图书基本信息

书名：<<计算机病毒防范艺术>>

13位ISBN编号：9787111205562

10位ISBN编号：7111205561

出版时间：2007-1

出版时间：机械工业出版社

作者：斯泽

页数：444

译者：段新海

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>

## <<计算机病毒防范艺术>>

### 内容概要

本书作者是赛门铁克（Symantec）公司安全响应中心首席安全架构师，他根据自己设计和改进Norton AntiVirus系统产品及培训病毒分析人员的过程中遇到的问题精心总结编写了本书。本书最大的特色是大胆深入地探讨了病毒知识的技术细节，从病毒的感染策略上深入分析病毒的复杂性，从文件、内存和网络等多个角度讨论病毒的感染技术，对过去20年来黑客们开发的各种病毒技巧进行了分类和讲解，并介绍了代码变形和其他新兴病毒感染技术，展示了当前计算机病毒和防毒软件最新技术，向读者传授计算机病毒分析和防护的方法学。

本书可作为IT和安全专业人士的权威指南，同时也适合作为大学计算机安全专业本科、研究生的参考教材。

## <<计算机病毒防范艺术>>

### 作者简介

Peter Szor是一位举世闻名的计算机病毒和安全研究人员，他积极从事计算机病毒研究已经15年以上。

1991年，他的毕业论文主题就是计算机病毒和病毒防护。

这些年来，Peter很幸运地参与了一些最负盛名的反病毒产品的研发，如AVP、F-PROT和Symantec Norton AntiVirus。

最初（1990~1995年），他曾在匈牙利开发自己的反病毒程序—Pasteur（巴斯德）。

除了对反病毒软件开发有兴趣外，Peter还有多年的容错和安全金融交易系统的开发经验。

Peter于1997年受邀加入了计算机反病毒研究者组织（Computer Antivirus Researchers Organization, CARO）。

他是《Virus Bulletin》（病毒公告）杂志的顾问委员会成员，也是反病毒应急讨论网络（AntiVirus Emergency Discussion（AVED）network）的创办人之一。

他在加利福尼亚Santa Monica的Symantec公司担任首席研究员已5年以上。

Peter为《Virus Bulletin》、《Chip》、《Source》、《Windows NT Magazine》和《Information Security Bulletin》等杂志写过70多篇有关计算机病毒和安全方面的文章和论文。

他经常在Virus Bulletin、EICAR（欧洲计算机防毒研究所）、ICSA（国际计算机安全协会）和RSA等会议上发表演讲，而且曾在USENIX Security Symposium（USENIX安全专题讨论会）这样的安全会议上作过特邀演讲。

Peter热心于分享自己的研究成果和向别人传授计算机病毒与安全方面的知识。

译者简介：段海新，工学博士、副教授、国际信息系统安全认证专家(CISSP)。

现任清华大学信息网络工程研究中心网络与信息安全研究室主任，中国教育和科研计算机网紧急响应组(CCERT)负责人，互联网协会安全工作委员会委员，国际信息系统安全认证联盟(ISC)2亚太区顾问。

主要从事计算机网络安全方面的科研、运行管理和教学工作。

## &lt;&lt;计算机病毒防范艺术&gt;&gt;

## 书籍目录

第一部分 攻击者的策略第1章 引言：自然的游戏1.1 自我复制结构的早期模型1.2 计算机病毒的起源1.3 自动复制代码：计算机病毒的原理和定义参考文献第2章 恶意代码分析的魅力2.1 计算机病毒研究的通用模式2.2 反病毒防护技术的发展2.3 恶意程序的相关术语2.4 其他类别2.5 计算机恶意软件的命名规则2.6 公认的平台名称清单参考文献第3章 恶意代码环境3.1 计算机体系结构依赖性3.2 CPU依赖性3.3 操作系统依赖性3.4 操作系统版本依赖性3.5 文件系统依赖性3.6 文件格式依赖性3.7 解释环境依赖性3.8 系统漏洞依赖性3.9 日期和时间依赖性3.10 JIT依赖性：Microsoft .NET病毒3.11 档案文件格式依赖性3.12 基于扩展名的文件格式依赖性3.13 网络协议依赖性3.14 源代码依赖关系3.15 在Mac和Palm平台上的资源依赖性3.16 宿主大小依赖性3.17 调试器依赖性3.18 编译器和连接器依赖性3.19 设备翻译层依赖性3.20 嵌入式对象插入依赖性3.21 自包含环境的依赖性3.22 复合病毒3.23 结论参考文献第4章 感染策略的分类4.1 引导区病毒4.2 文件感染技术4.3 深入分析Win32病毒4.4 结论参考文献第5章 内存驻留技术5.1 直接感染型病毒5.2 内存驻留病毒5.3 临时内存驻留病毒5.4 交换型病毒5.5 进程病毒（用户模式）5.6 内核模式中的病毒（Windows 9x /Me）5.7 内核模式中的病毒（Windows NT/2000/XP）5.8 通过网络传播的内存注入病毒参考文献第6章 基本的自保护策略6.1 隧道病毒6.2 装甲病毒6.3 攻击性的反制病毒参考文献第7章 高级代码演化技术和病毒生成工具7.1 引言7.2 代码演化7.3 加密病毒7.4 寡形病毒7.5 多态病毒7.6 变形病毒7.7 病毒机参考文献第8章 基于病毒载荷的分类方法8.1 没有载荷8.2 偶然破坏型载荷8.3 非破坏型载荷8.4 低破坏型载荷8.5 强破坏型载荷8.6 DoS攻击8.7 窃取数据：用病毒牟利8.8 结论参考文献第9章 计算机蠕虫的策略9.1 引言9.2 计算机蠕虫的通用结构9.3 目标定位9.4 感染传播9.5 常见的蠕虫代码传送和执行技术9.6 计算机蠕虫的更新策略9.7 用信令进行远程控制9.8 有意无意的交互9.9 无线移动蠕虫参考文献第10章 漏洞利用、漏洞和缓冲区溢出攻击10.1 引言10.2 背景10.3 漏洞的类型10.4 攻击实例10.5 小结参考文献第二部分 防御者的策略第11章 病毒防御技术11.1 第一代扫描器11.2 第二代扫描器11.3 算法扫描方法11.4 代码仿真11.5 变形病毒检测实例11.6 32位Windows病毒的启发式分析11.7 基于神经网络的启发式分析11.8 常规及通用清除法11.9 接种11.10 访问控制系统11.11 完整性检查11.12 行为阻断11.13 沙箱法11.14 结论参考文献第12章 内存扫描与杀毒12.1 引言12.2 Windows NT虚拟内存系统12.3 虚拟地址空间12.4 用户模式的内存扫描12.5 内存扫描和页面调度12.6 内存杀毒12.7 内核模式的内存扫描12.8 可能的内存扫描攻击12.9 结论和下一步工作参考文献第13章 蠕虫拦截技术和基于主机的入侵防御13.1 引言13.2 缓冲区溢出攻击的对策13.3 蠕虫拦截技术13.4 未来可能出现的蠕虫攻击13.5 结论参考文献第14章 网络级防御策略14.1 引言14.2 使用路由器访问列表14.3 防火墙保护14.4 网络入侵检测系统14.5 蜜罐系统14.6 反击14.7 早期预警系统14.8 蠕虫的网络行为模式14.9 结论参考文献第15章 恶意代码分析技术15.1 个人的病毒分析实验室15.2 信息、信息、信息15.3 VMware上的专用病毒分析系统15.4 计算机病毒分析过程15.5 维护恶意代码库15.6 自动分析：数字免疫系统参考文献第16章 结论进一步阅读资料安全和早期预警方面的信息安全更新计算机蠕虫爆发统计数据计算机病毒研究论文反病毒厂商联系方式反病毒产品测试机构及相关网站

## <<计算机病毒防范艺术>>

### 编辑推荐

《计算机病毒防范艺术》可作为IT和安全专业人士的权威指南，同时也适合作为大学计算机安全专业本科、研究生的参考教材。

<<计算机病毒防范艺术>>

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>