

恶意传播代码



[恶意传播代码_下载链接1](#)

著者:(美)Roger A.Grimes著;张

出版者:机械工业出版社

出版时间:2004-6

装帧:

isbn:9787111124832

本书为系统管理员和用户提供了大量信息，帮助他们来理解Windows系统下的恶意代码问题。通过对不同的恶意传播代码分章探讨，作者对各种类型的恶意代码都进行了详细的讨论，包括：

- 病毒
- 木马和蠕虫
- ActiveX和Java恶意攻击代码

- DOS病毒
- 宏病毒
- 基于浏览器的恶意攻击代码
- Email攻击
- 即时消息攻击 (Instant messaging attack)

本书对于每一种攻击方式均进行了详尽的介绍。除了描述这些攻击方式的原理之外，还提供了一些技术细节，以帮助你理解为什么这些攻击能够实现。每一章对于相应的攻击方式都介绍了应当采取的具体保护措施。

尽管你已经竭尽全力，但仍然可能受到恶意代码的攻击。有时这种攻击的结果非常明显；而有时除非造成巨大破坏，结果难以察觉。本书介绍了如何寻找和识别遭受各种不同攻击的迹象。每一章都介绍了如何删除这些恶意代码并恢复你的系统。在每一章结尾，作者对该章相应的攻击类型的危险程度作了评价。

Roger A.

Grimes从1987开始就与恶意传播代码进行着各种形式的对抗。作为一个获得了MCSE、CNE和A+等Microsoft认证和Novell网络认证的工程师，他在恶意代码这一领域积累了丰富的专业经验。他将自己的经验与深入浅出的写作风格相融合，使得这本书成为Windows系统管理员和使用者不可多得的参考书。

作者介绍:

目录: 前言

第一章 介绍

追查

什么是恶意传播代码

恶意代码和法律

编写恶意代码的亚文化

恶意传播代码术语

小结

第二章 DOS病毒

背景介绍

DOS技术

DOS病毒技术

DOS病毒类型

病毒防御原理

DOS病毒的例子

如何发现DOS病毒

清除DOS病毒

保护你的系统不受病毒攻击

危险评估 —— 低

小结

第三章 Windows技术

Windows技术

Windows的新版本

小结

第四章 Windows病毒

Windows平台下的DOS病毒
Windows平台下的Windows病毒
Windows NT病毒感染的特征和症状
Windows病毒的例子
发现Windows病毒
清除病毒
清除文件感染病毒
Windows下的病毒防御
未来
危险评估 —— 中
小结
第五章 宏病毒
什么是宏病毒
微软 Word和Excel宏
使用宏
Office 2000安全
宏病毒技术
宏病毒例子
发现宏病毒
清除宏病毒并且恢复系统
防御宏病毒
危险评估 —— 高
小结
第六章 木马和蠕虫
威胁
什么是木马和蠕虫
特征和症状
木马的类型
木马技术
熟悉你的计算机
木马和蠕虫的例子
发现并且清除木马和蠕虫
预防木马和蠕虫
危险评估 —— 高
小结
第七章 即时消息攻击
即时消息介绍
即时消息类型
IRC
攻击即时消息
IRC攻击的例子
发现恶意IM
清除恶意IM
保护你自己不受IM攻击
危险评估 —— 中
小结
第八章 Internet浏览器技术
介绍
浏览器技术
网页语言
其他浏览器技术
何时应该注意浏览器中的内容
小结
第九章 通过Internet浏览器攻击

基于浏览器的攻击行为
攻击和入侵示例
检测Internet浏览器攻击
删除和修复被破坏的文件
预防Internet浏览器攻击
危险评估 —— 中
小结
第十章 恶意的Java applet
Java
Java安全
Java的恶意利用
Java 恶意利用的例子
检测恶意的Java applet
删除恶意的Java代码
保护自己免受恶意的Java代码攻击
危险评估 —— 低
小结
第十一章 恶意ActiveX控件
ActiveX
ActiveX安全
ActiveX安全性评述
恶意ActiveX的例子
检测恶意ActiveX控件
删除并预防恶意ActiveX控件
危险评估 —— 中
小结
第十二章 邮件攻击
介绍
邮件程序
邮件漏洞
检测邮件攻击
删除被感染的邮件
阻止邮件攻击
危险评估 —— 高
小结
第十三章 欺骗性病毒
计算机病毒之母
欺骗性病毒消息的种类
检测
删除并阻止欺骗性病毒
危险评估 —— 低
小结
第十四章 防御
防御策略
恶意传播代码防御计划
使用良好的反病毒扫描程序
反病毒扫描位置
使得任何一台Windows PC变得安全的最好步骤
额外的防御工具
反病毒产品综述
前景
小结
第十五章 恶意传播代码的未来
计算机技术的未来

恶意传播代码的发展
 真正的防范措施
 小结
 词汇表
 ([收起](#))

[恶意传播代码_下载链接1](#)

标签

计算机

安全

美国

编程

评论

病毒原代码

[恶意传播代码_下载链接1](#)

书评

[恶意传播代码_下载链接1](#)