

<<决战恶意代码>>

图书基本信息

书名：<<决战恶意代码>>

13位ISBN编号：9787121009921

10位ISBN编号：7121009927

出版时间：2005-4

出版时间：电子工业出版社

作者：（美）斯考迪斯 兹勒特尔

页数：478

字数：650000

译者：陈贵敏 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>

<<决战恶意代码>>

内容概要

本书旨在用预防、检测和处理攻击计算机系统和网络的恶意代码所需的工具和技术来武装你。书中讨论了如何预先保证系统安全，以防止这样的攻击；如何发现渗透进你的防御系统的恶意代码；如何分析随时都有可能遇到的 MALWARE 样本等。

本书突出强调实用性，书中详细介绍了保证系统不受恶意代码攻击所能采取的措施，这些措施已经过时间考验并且切实可行。

按照书中的技巧，你完全可以构建一个顶尖的防御工具包，用来对付随处发现的恶意代码。

系统管理员、网络工作者、家用计算机用户，特别是安全从业者，都需要利用此书，以此为自己的网络抵御那些随时都在变得更加凶狠的攻击。

<<决战恶意代码>>

作者简介

Ed Skoudis , 是有名的信息安全预测专家、克林顿安全办公室的高级顾问以及网络安全研究会 “ The Hack-Counter Hack Training Course ” 的创始人, 是多年来一直从事计算机安全工作。

Ed Skoudis 的另外一部畅销书—— “ Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses ” (中文版译名为《反击黑客》), 详细介绍防御各种黑客攻击的技术与方法。

而这本书所讲述的 Malware 要比黑客攻击工具具有更为广泛的内容。

<<决战恶意代码>>

书籍目录

第1章 介绍 1.1 定义问题 1.2 为什么恶意代码如此普遍 1.3 恶意代码的类型 1.4 恶意代码的历史 1.5 为什么写这本书 1.6 有哪些期望 1.7 参考文献 第2章 病毒 2.1 计算机病毒的早期历史 2.2 感染机制和目标 2.3 病毒的传播机制 2.4 防御病毒 2.5 malware 的自我保护技术 2.6 结论 2.7 总结 2.8 参考文献 第3章 蠕虫 3.1 为什么使用蠕虫？ 3.2 蠕虫简史 3.3 蠕虫的组成 3.4 蠕虫传播的障碍 3.5 即将到来的超级蠕虫 3.6 大的并非总是好的：非超级蠕虫 3.7 防御蠕虫 3.8 结论 3.9 总结 3.10 参考文献 第4章 恶意移动代码 4.1 浏览器脚本 4.2 ActiveX 控件 4.3 Java Applets 4.4 E-mail 客户程序中的移动代码 4.5 分布式应用软件和移动代码 4.6 防御恶意移动代码的其他方法 4.7 结论 4.8 总结 4.9 参考文献 第5章 后门 5.1 不同类型的后门通路 5.2 安装后门 5.3 自动启动后门 5.4 通用的网络连接工具：NetCat 5.5 GUI 越过网络大量使用虚拟网络计算 5.6 无端口后门 5.7 结论 5.8 总结 5.9 参考文献 第6章 特洛伊木马 6.1 名字中有什么 6.2 包装明星 6.3 特洛伊软件发行站点 6.4 给代码“下毒” 6.5 “指定”一个浏览器：Setiri 6.6 将数据隐藏在可执行文件中：隐藏和多态 6.7 结论 6.8 总结 6.9 参考书目 第7章 用户模式 RootKit 7.1 UNIX 用户模式 RootKit 7.2 Windows 用户模式 RootKit 7.3 结论 7.4 总结 7.5 参考文献 第8章 内核模式 RootKits 8.1 内核是什么？ 8.2 内核控制的影响 8.3 Linux 内核 8.4 Windows 内核 8.5 结论 8.6 总结 8.7 参考文献 第9章 进一步深入 9.1 设置舞台：malware 的不同层次 9.2 更深层次：BIOS 的可能性和 malware 微代码 9.3 组合 malware 9.4 结论 9.5 总结 9.6 参考文献 第10章 情节 10.1 情节 1：白璧微瑕 10.2 情节 2：内核偷盗者的入侵 10.3 情节 3：沉默的蠕虫 10.4 结论 10.5 总结 第11章 恶意代码分析 11.1 建立一个恶意代码分析实验室 11.2 恶意代码分析过程 11.3 结论 11.4 总结 11.5 参考文献 第12章 结论 12.1 跟上技术发展的有用站点 12.2 临别思考

<<决战恶意代码>>

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>