

《恶意软件、Rootkit和僵尸网络》

图书基本信息

书名：《恶意软件、Rootkit和僵尸网络》

13位ISBN编号：9787111436959

10位ISBN编号：7111436954

出版时间：2013-10

出版社：机械工业出版社

作者：Christopher C.Elisan

页数：251

译者：郭涛,章磊 张普含 张翀斌

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《恶意软件、Rootkit和僵尸网络》

作者简介

Christopher C. Elisan，资深逆向分析工程师和恶意软件研究专家，RSA NetWitness的首席恶意软件分析科学家。他经常为《今日美国》、《信息周刊》、《隐秘读物》（Dark Reading）等领导性出版物提供恶意软件、僵尸网络、高级持续性威胁方面的专家意见。

译者简介

郭涛，博士，中国信息安全测评中心副总工程师，软件安全实验室主任，主要研究方向为软件安全与漏洞分析技术。多次承担自然科学基金、863、核高基、电子发展基金等多项国家重大科研项目，负责多项国家标准的制定工作，获国家科技进步一等奖一次、省部级科技进步一等奖一次，出版专著、译著十余本，发表学术论文数十篇。

书籍目录

本书赞誉

译者序

序

前言

第一部分 基础知识

第1章 背景知识

1.1 一次恶意软件遭遇

1.2 目前所面临的威胁概述

1.3 对国家安全构成的威胁

1.4 开启旅程

1.5 本章小结

参考文献

第2章 恶意软件简史

2.1 计算机病毒

2.1.1 计算机病毒的分类

2.1.2 早期挑战

2.2 恶意软件

2.2.1 恶意软件分类

2.2.2 恶意软件的发展

2.3 风险软件

2.4 恶意软件开发套件

2.5 恶意软件的影响

2.6 本章小结

第3章 rootkit的隐藏

3.1 什么是rootkit

3.2 环境的结构

3.2.1 操作系统内核

3.2.2 用户态和内核态

3.2.3 ring

3.2.4 从用户态转换到内核态

3.3 rootkit的类型

3.3.1 用户态rootkit

3.3.2 内核态rootkit

3.4 rootkit技术

3.4.1 hooking

3.4.2 DLL注入

3.4.3 直接内核对象操纵

3.5 应对rootkit

3.6 本章小结

第4章 僵尸网络的兴起

4.1 什么是僵尸网络

4.1.1 主要特点

4.1.2 关键组件

4.1.3 C&C结构

4.2 僵尸网络的使用

4.2.1 分布式拒绝服务攻击

4.2.2 点击欺诈

- 4.2.3 垃圾邮件转发
- 4.2.4 单次安装付费代理
- 4.2.5 大规模信息获取
- 4.2.6 信息处理
- 4.3 僵尸网络的保护机制
 - 4.3.1 防弹主机
 - 4.3.2 动态DNS
 - 4.3.3 Fast-Fluxing技术
 - 4.3.4 域名变化地址
- 4.4 对抗僵尸网络
 - 4.4.1 技术战线
 - 4.4.2 法律战线
- 4.5 本章小结
- 4.6 参考文献

第二部分 恶劣的现状

第5章 威胁生态系统

- 5.1 威胁生态系统组成
 - 5.1.1 技术因素
 - 5.1.2 人为因素
 - 5.1.3 威胁生态系统的演进
- 5.2 高级持续性威胁
 - 5.2.1 攻击方法
 - 5.2.2 攻击的收益
- 5.3 恶意软件经济
- 5.4 本章小结

第6章 恶意软件工厂

- 6.1 逃避反病毒检测的必要性
 - 6.1.1 恶意软件事件处理过程
 - 6.1.2 恶意软件检测
 - 6.1.3 反病毒产品绕过技术
- 6.2 建立恶意软件军队的必要性
 - 6.2.1 下一代恶意软件工具套件
 - 6.2.2 独立的防护工具
 - 6.2.3 恶意软件装甲军队的作用
- 6.3 恶意软件工厂
 - 6.3.1 恶意软件流水线
 - 6.3.2 攻击者工具的获得
 - 6.3.3 恶意软件日益泛滥
- 6.4 本章小结

第7章 感染载体

- 7.1 感染载体概述
 - 7.1.1 物理媒介
 - 7.1.2 电子邮件
 - 7.1.3 即时通信和聊天软件
 - 7.1.4 社交网络
 - 7.1.5 URL链接
 - 7.1.6 文件共享
 - 7.1.7 软件漏洞
- 7.2 变成感染载体的可能性

7.3 本章小结

第8章 受感染系统

8.1 恶意软件感染过程

8.1.1 安装恶意软件文件

8.1.2 设置恶意软件的持久性

8.1.3 移除恶意软件安装证据

8.1.4 向恶意软件传递控制权

8.2 活跃的恶意软件

8.2.1 在系统中长期潜伏

8.2.2 和攻击者通信

8.2.3 执行有效载荷

8.3 本章小结

第三部分 企业的应对

第9章 组织保护

9.1 威胁事件响应者

9.2 理解系统的价值

9.2.1 系统对于组织的价值

9.2.2 系统对于攻击者的价值

9.3 理解系统的特征

9.3.1 系统类型

9.3.2 运营影响

9.3.3 主机数据的敏感度

9.3.4 系统用户

9.3.5 网络位置

9.3.6 资产的可访问性

9.3.7 资产访问权限

9.3.8 系统恢复

9.3.9 系统状态

9.4 设置系统优先级

9.5 企业安全态势

9.6 了解遭受攻击的代价

9.6.1 直接损失

9.6.2 间接损失

9.7 系统保护

9.7.1 威胁建模

9.7.2 识别合适的解决方案

9.7.3 前置式威胁检测

9.8 建立事件响应计划

9.8.1 识别不同的受害场景

9.8.2 识别解决方案模式

9.8.3 定义角色和职责

9.8.4 建立草案

9.8.5 定期演习

9.8.6 评审和改进

9.9 把一切付诸行动

9.10 保护之外

9.11 本章小结

第10章 检测威胁

10.1 建立基准

- 10.1.1 建立网络基准
- 10.1.2 建立主机基准
- 10.2 检测异常
 - 10.2.1 检测网络异常
 - 10.2.2 检测主机异常
- 10.3 隔离异常源
- 10.4 深入分析受感染资产
 - 10.4.1 精确定位恶意软件
 - 10.4.2 基于攻击意图对恶意软件进行分类
- 10.5 本章小结
- 第11章 缓解威胁
 - 11.1 威胁缓解
 - 11.2 立即式响应
 - 11.2.1 隔离
 - 11.2.2 验证
 - 11.2.3 威胁的检测和分类
 - 11.2.4 修复和恢复
 - 11.3 先应式响应
 - 11.3.1 预防措施
 - 11.3.2 定期进行安全审计
 - 11.4 内部威胁
 - 11.4.1 什么是内部威胁
 - 11.4.2 缓解内部威胁
 - 11.5 保持警惕
 - 11.6 本章小结
- 第四部分 结束语
- 第12章 永不停歇的战斗
 - 12.1 本书回顾
 - 12.2 未来展望
 - 12.2.1 恶意软件的未来
 - 12.2.2 rootkit展望
 - 12.2.3 僵尸网络的未来
 - 12.3 好人们也很忙
 - 12.4 冒险才刚刚开始
 - 12.5 本章小结
- 附录A 系统启动过程
- 附录B 有用的网络链接
- 词汇表

《恶意软件、Rootkit和僵尸网络》

精彩短评

1、感觉挺不错的。。。就是有点贵

《恶意软件、Rootkit和僵尸网络》

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:www.tushu000.com