

<<黑客免杀攻防>>

图书基本信息

书名：<<黑客免杀攻防>>

13位ISBN编号：9787111440420

10位ISBN编号：7111440420

出版时间：2013-9-1

出版时间：机械工业出版社

作者：任晓琿

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>

<<黑客免杀攻防>>

内容概要

《黑客免杀攻防》国内首部关于黑客免杀技术的专著，旨在为反病毒工程师剖析各种恶意软件和应对各种安全威胁提供全面指导。

不仅从攻击者（黑客）的视角全方位揭示了黑客免杀技术的常用方法、常用技术和思想原理，还从防御者（反病毒工程师）的视角深入讲解了遏制免杀技术的具体方法策略。

从纯技术的角度讲，本书不仅详细讲解了免杀技术的各种细节和方法，还详细讲解了PE文件、逆向工程、C++壳的编写、免杀壳的打造、脱壳、Rootkit等安全技术的细节。

《黑客免杀攻防》共20章，分为三大部分：基础篇（第1~6章）详细介绍了黑客免杀技术的初级技巧，包括查找（修改）特征码、常见特征码绕过技巧、壳在免杀中的应用、花指令和其他免杀基础知识；高级篇（第7~16章）深入讲解了PE文件、逆向工程、C++壳的编写、免杀壳的打造、脱壳、Rootkit等常用安全技术的原理和细节，以及黑客免杀技术是如何应用它们的，为反病毒工程师应对各种恶意软件提供了原理性指导；扩展篇（第17~20章）为遏制黑客免杀技术提供了思路和具体的方案。

<<黑客免杀攻防>>

作者简介

任晓琿，资深安全技术工程师，华章“信息安全技术丛书”专家顾问，致力于免杀技术和反病毒技术的实践。

对软件安全、逆向工程、Rootkit、加壳与脱壳等技术有较深入的研究和理解，积累了丰富的经验。北京蓝森科技有限公司创始人，黑客反病毒论坛创始人，邪恶八进制团队成员，资深培训讲师，国内知名信息安全培训品牌15PB的创始人。

目前专注于计算机安全的中高端培训。

<<黑客免杀攻防>>

书籍目录

前言

基础篇 初级免杀技术

第1章 变脸

1.1 为何变脸

1.2 何为变脸

1.3 免杀的发展史

1.4 免杀技术的简单原理

1.5 免杀与其他技术的区别

1.5.1 免杀不是Rootkit技术

1.5.2 免杀不是加密解密技术

1.6 小结

第2章 免杀基础知识

2.1 如何开始免杀

2.2 反病毒软件原理与反病毒技术介绍

2.2.1 反病毒软件的工作原理

2.2.2 基于文件扫描的反病毒技术

2.2.3 基于内存扫描的反病毒技术

2.2.4 基于行为监控的反病毒技术

2.2.5 基于新兴技术的反病毒技术

2.2.6 反病毒技术前沿

2.2.7 反病毒技术展望

2.3 了解PE文件

2.3.1 什么是PE文件

2.3.2 PE文件的结构

2.4 免杀原理

2.4.1 文件免杀原理

2.4.2 内存免杀原理

2.4.3 行为免杀原理

2.5 工具脱壳技巧

2.5.1 壳的分类

2.5.2 免杀与脱壳是什么关系

2.5.3 使用专用脱壳工具脱壳

2.5.4 使用通用脱壳工具脱壳

2.6 小结

第3章 免杀与特征码

3.1 特征码免杀技术

3.1.1 理想状态下的免杀

3.1.2 由脚本木马免杀理解特征码

3.2 特征码定位原理

3.2.1 特征码逐块填充定位原理

3.2.2 特征码逐块暴露定位原理

3.2.3 特征码混合定位原理

3.3 脚本木马定位特征码

3.4 MyCCL查找文件特征码

3.4.1 MyCCL的典型应用

<<黑客免杀攻防>>

- 3.4.2 针对MyCCL的一点思考
- 3.5 MyCCL查找内存特征码
- 3.6 特征码修改方法
 - 3.6.1 简单的特征码修改
 - 3.6.2 特征码修改进阶
- 3.7 小结
- 第4章 其他免杀技术
 - 4.1 修改入口点免杀
 - 4.2 使用VMProtect加密
 - 4.3 Overlay附加数据的处理及应用
 - 4.4 驱动程序免杀修改技巧
 - 4.4.1 驱动程序的常见免杀方法
 - 4.4.2 驱动程序的手工免杀思路
 - 4.5 补丁在免杀中的应用
 - 4.6 PE文件进阶介绍
 - 4.6.1 PE文件格式
 - 4.6.2 虚拟内存的简单介绍
 - 4.6.3 PE文件的内存映射
 - 4.7 网页木马的免杀
 - 4.7.1 脚本木马免杀
 - 4.7.2 网页挂马的免杀
 - 4.8 小结
- 第5章 花指令与免杀
 - 5.1 什么是花指令
 - 5.2 脚本木马的花指令应用
 - 5.3 花指令的根基-汇编语言
 - 5.3.1 认识汇编
 - 5.3.2 通过反汇编添加任意功能
 - 5.4 花指令入门
 - 5.5 花指令在免杀领域的应用
 - 5.5.1 花指令的应用技巧
 - 5.5.2 花指令的修改技巧简介
 - 5.5.3 空白区域寻找与加空白区段
 - 5.6 花指令的高级应用
 - 5.6.1 花指令的提取与快速应用
 - 5.6.2 SEH异常的应用
 - 5.7 小结
- 第6章 壳在免杀中的应用
 - 6.1 壳的基础知识
 - 6.2 壳在免杀领域的应用
 - 6.2.1 加壳的免杀原理
 - 6.2.2 FreeRes多重加壳
 - 6.3 壳的修改技巧
 - 6.3.1 壳的初级修改
 - 6.3.2 制作通用补丁
 - 6.4 小结
- 高级篇 免杀技术进阶

<<黑客免杀攻防>>

第7章 PE文件格式详解

7.1 MS-DOS头

7.1.1 重要字段

7.1.2 其他字段

7.2 PE文件头

7.2.1 Signature字段

7.2.2 IMAGE_FILE_HEADER结构

7.2.3 IMAGE_OPTIONAL_HEADER结构 (x86/x64)

7.2.4 数据目录表

7.3 区段表

7.3.1 IMAGE_SECTION_HEADER结构

7.3.2 区段名功能约定

7.3.3 区段对齐详解

7.3.4 地址转换

7.4 导出表

7.4.1 IMAGE_EXPORT_DIRECTORY结构

7.4.2 识别导出表

7.5 导入表

7.5.1 IMAGE_IMPORT_DESCRIPTOR结构

7.5.2 识别导入表

7.6 资源

7.6.1 资源结构

7.6.2 识别资源

7.7 异常

7.8 安全

7.8.1 安全目录结构

7.8.2 识别安全结构

7.9 基址重定位

7.9.1 基址重定位表结构

7.9.2 识别基址重定位表

7.10 调试

7.11 特殊结构数据 (版权)

7.12 全局指针

7.13 TLS

7.13.1 TLS的回调函数

7.13.2 TLS的结构 (x86/x64)

7.13.3 识别TLS

7.14 载入配置 (x86/x64)

7.15 绑定导入表

7.15.1 绑定导入表结构

7.15.2 识别绑定导入表

7.16 导入地址表

7.17 延迟加载表

7.17.1 延迟加载表结构

7.17.2 识别延迟加载表

7.18 COM描述符

7.19 小结

<<黑客免杀攻防>>

第8章 PE文件知识在免杀中的应用

8.1 PE文件与免杀思路

8.1.1 移动PE文件头位置免杀

8.1.2 导入表移动免杀

8.1.3 导出表移动免杀

8.2 PE文件与反启发式扫描

8.2.1 最后一个区段为代码段

8.2.2 可疑的区段头部属性

8.2.3 可疑的PE选项头的有效尺寸值

8.2.4 可疑的代码节名称

8.2.5 多个PE头部

8.2.6 导入表项存在可疑导入

8.3 一个稍显复杂的例子-隐藏导入表

8.3.1 操作原理与先决条件

8.3.2 修改PE文件

8.3.3 构造我们的反汇编代码

8.4 小结

第9章 软件逆向工程

9.1 准备工作

9.1.1 要准备的工具及基础知识

9.1.2 程序是从哪里开始运行的

9.2 一个简单的小例子

9.3 函数识别初探

9.4 if-else分支

9.4.1 以常量为判断条件的简单if-else分支

9.4.2 以变量为判断条件的简单if-else分支

9.4.3 以常量为判断条件的复杂if-else分支

9.4.4 以变量为判断条件的复杂if-else分支

9.4.5 识别三目运算符

9.5 循环分支

9.5.1 do-while循环

9.5.2 while循环

9.5.3 for循环

9.5.4 循环体的语句外提优化

9.6 switch-case分支

9.6.1 简单switch-case分支识别技巧

9.6.2 复杂分支的switch-case识别

9.6.3 switch-case分支结构与稀疏矩阵

9.6.4 switch-case分支结构与平衡二叉树

9.7 加法与减法的识别与优化原理

9.7.1 加法的识别与优化

9.7.2 减法的识别与优化

9.8 乘法与除法的识别与优化原理

9.8.1 乘法的位移优化

9.8.2 乘法的lea指令优化

9.8.3 除法与倒数相乘

9.8.4 倒数相乘与定点运算的配合

<<黑客免杀攻防>>

- 9.8.5 除法运算的识别与优化
- 9.8.6 取模运算的识别与优化
- 9.9 指针与数组
 - 9.9.1 指针与数组的渊源
 - 9.9.2 数组的不同表达方式
- 9.10 数组、结构体与对象
 - 9.10.1 数组与结构体
 - 9.10.2 结构体与类
- 9.11 变量作用域的识别
- 9.12 识别构造与析构函数
 - 9.12.1 快速识别出类
 - 9.12.2 识别构造函数
 - 9.12.3 识别析构函数
- 9.13 虚函数与纯虚函数的识别
 - 9.13.1 识别简单的虚函数
 - 9.13.2 识别较复杂的虚函数
- 9.14 正确识别类的继承关系
- 9.15 最后一役
 - 9.15.1 MFC逆向初探
 - 9.15.2 分析BypassUAC.exe
- 9.16 小结
- 第10章 源码级免杀
 - 10.1 怎样定位产生特征的源代码
 - 10.1.1 定位文件特征
 - 10.1.2 定位行为特征
 - 10.2 基于源码的特征修改
 - 10.2.1 变换编译器与编译选项
 - 10.2.2 添加垃圾代码
 - 10.2.3 语法变换
 - 10.2.4 添加汇编花指令
 - 10.3 小结
- 第11章 详解C++壳的编写
 - 11.1 了解壳的运行流程
 - 11.2 设计一个纯C++编写的壳
 - 11.2.1 用C++编写的壳应该是什么样的
 - 11.2.2 编写过程中会遇到的问题
 - 11.3 用C++写一个简单的壳
 - 11.3.1 配置工程
 - 11.3.2 编写Stub部分
 - 11.3.3 编写加壳部分
 - 11.3.4 编写界面部分
 - 11.4 设计一个由C++编写的专业壳
 - 11.4.1 为问题找到答案
 - 11.4.2 设计专业壳的框架
 - 11.4.3 如何设计Stub部分
 - 11.4.4 如何设计加壳部分
 - 11.4.5 需要注意的细节问题

<<黑客免杀攻防>>

- 11.5 怎样调试由C++编写的Stub部分
- 11.6 小结
- 第12章 黑客是怎样打造免杀壳的
 - 12.1 免杀壳与加密壳的异同
 - 12.2 导入表加密
 - 12.3 代码混淆与代码乱序
 - 12.4 附加驱动
 - 12.5 小结
- 第13章 脱壳技术
 - 13.1 寻找OEP
 - 13.1.1 利用内存断点
 - 13.1.2 利用堆栈平衡
 - 13.1.3 利用编译语言特点
 - 13.1.4 利用跨区段跳转
 - 13.2 转储内存映像
 - 13.3 重建导入表
 - 13.3.1 导入表重建原理
 - 13.3.2 使用ImportREC重建导入表
 - 13.4 小结
- 第14章 Rootkit基础
 - 14.1 构建一个Rootkit基础环境
 - 14.1.1 构建开发环境
 - 14.1.2 构建基于Visual Studio 2012的调试环境
 - 14.1.3 构建基于WinDbg的调试环境
 - 14.1.4 将Rootkit加载到系统
 - 14.1.5 创建一个简单的驱动并调试
 - 14.2 何为Ring0层
 - 14.3 关键表
 - 14.4 内存分页
 - 14.4.1 地址转译
 - 14.4.2 内存访问检查
 - 14.4.3 Windows对重要表的保护
 - 14.5 内存描述符表
 - 14.6 中断描述符表 (IDT)
 - 14.7 系统服务调度表
 - 14.8 控制寄存器
 - 14.8.1 利用CR0禁用内存保护机制
 - 14.8.2 其他控制寄存器
 - 14.9 小结
- 第15章 Rootkit在免杀中的应用
 - 15.1 用户模式Rootkit
 - 15.1.1 DLL远程注入技巧
 - 15.1.2 内联钩子
 - 15.1.3 导入地址表钩子
 - 15.1.4 一个保护文件不被删除的例子
 - 15.2 内核编程基础
 - 15.2.1 内核编程环境与用户层编程环境的异同

<<黑客免杀攻防>>

- 15.2.2 如何选择Windows驱动开发模型
- 15.2.3 驱动设备与请求处理
- 15.2.4 内核编程中的数据类型
- 15.2.5 函数调用
- 15.2.6 Windows内核编程的特点
- 15.3 内核模式Rootkit
 - 15.3.1 SYSENTER钩子
 - 15.3.2 SSDT钩子
 - 15.3.3 内联钩子
 - 15.3.4 IRP钩子
 - 15.3.5 LADDR钩子
 - 15.3.6 IDT钩子
 - 15.3.7 IOAPIC钩子
- 15.4 小结
- 第16章 免杀技术前沿
 - 16.1 免杀技术的发展趋势
 - 16.2 免杀前沿之突破主动防御
 - 16.2.1 “移花接木”之屏幕截图突破主动防御
 - 16.2.2 “暗渡陈仓”之利用可信进程突破主动防御
 - 16.2.3 “釜底抽薪”之利用系统进程突破主动防御
 - 16.2.4 “顺手牵羊”之利用逻辑漏洞突破主动防御
 - 16.2.5 “浑水摸鱼”之利用变形复制突破主动防御
 - 16.2.6 “金蝉脱壳”之利用异同逃逸虚拟机
 - 16.2.7 “借尸还魂”之利用替换文件突破主动防御
 - 16.2.8 “借刀杀人”之利用调试接口突破主动防御
 - 16.3 黑客免杀技术的展望
 - 16.4 小结
- 扩展篇 遏制免杀技术初探
- 第17章 浅谈部分免杀技巧的遏制
 - 17.1 盯紧PE文件
 - 17.2 盯紧程序行为
 - 17.3 小结
- 第18章 反特征码定位
 - 18.1 释放干扰码
 - 18.2 定位行为的判定
 - 18.3 设定“靶特征码”
 - 18.4 小结
- 第19章 遏制免杀与Anti Rootkit
 - 19.1 适当的监控
 - 19.2 基本检测逻辑
 - 19.3 Rootkit检测方法初探
 - 19.4 小结
- 第20章 浅谈反病毒产品的改进
 - 20.1 云查杀与本地查杀紧密结合
 - 20.2 注重感染型病毒木马的清除工作
 - 20.3 精进启发式扫描解决效率问题
 - 20.4 小结

附录A 80x86汇编基础知识

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>