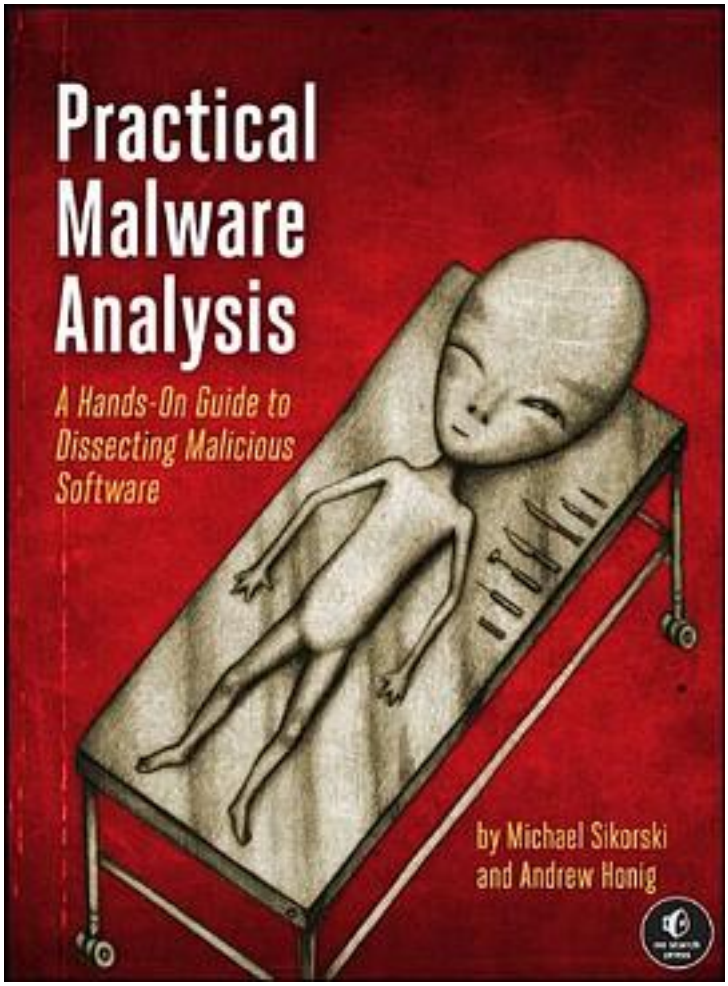
Practical Malware Analysis



Practical Malware Analysis_下载链接1_

著者:Michael Sikorski

出版者:No Starch Press

出版时间:2012-2

装帧:

isbn:9781593272906

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections

and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: * Set up a safe virtual environment to analyze malware * Quickly extract network signatures and host-based indicators * Use key analysis tools like IDA Pro, OllyDbg, and WinDbg * Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques * Use your newfound knowledge of Windows internals for malware analysis * Develop a methodology for unpacking malware and get practical experience with five of the most popular packers * Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

作者介绍:

Michael Sikorski is a malware analyst, researcher, and security consultant at Mandiant. His previous employers include the National Security Agency and MIT Lincoln Laboratory. Mike frequently teaches malware analysis to a variety of audiences including the FBI and Black Hat.

Andrew Honig is an Information Assurance Expert for the Department of Defense. He teaches courses on software analysis, reverse engineering, and Windows system programming. Andy is publicly credited with several zero-day exploits in VMware's virtualization products.

目录: Introduction
Chapter 0: Malware Analysis Primer
Part 1: Basic Analysis
Chapter 1: Basic Static Techniques
Chapter 2: Malware Analysis in Virtual Machines
Chapter 3: Basic Dynamic Analysis
Part 2: Advanced Static Analysis
Chapter 4: A Crash Course in x86 Disassembly
Chapter 5: IDA Pro
Chapter 6: Recognizing C Code Constructs in Assembly
Chapter 7: Analyzing Malicious Windows Programs
Part 3: Advanced Dynamic Analysis
Chapter 8: Debugging
Chapter 9: OllyDbg
Chapter 10: Kernel Debugging with WinDbg
Part 4: Malware Functionality
Chapter 11: Malware Behavior
Chapter 12: Covert Malware Launching
Chapter 13: Data Encoding
Chapter 14: Malware-Focused Network Signatures

Part 5: Anti-Reverse-Engineering
Chapter 15: Anti-Disassembly
Chapter 16: Anti-Debugging
Chapter 17: Anti-Virtual Machine Techniques
Chapter 18: Packers and Unpacking
Part 6: Special Topics
Chapter 19: Shellcode Analysis
Chapter 20: C++ Analysis
Chapter 21: 64-Bit Malware
Appendix A: Important Windows Functions
Appendix B: Tools for Malware Analysis
Appendix C: Solutions to Labs
・・・・・・(收起)

Practical Malware Analysis_下载链接1_

标签

计算机安全

安全

逆向

计算机

病毒

windows内核的

malware

信息安全

评论

了解病毒分析的一本好书

帮助入门吧

Practical Malware Analysis_下载链接1_

书评

随便在哪家网上书城进行搜索可以知道，在计算机安全类，特别是恶意代码分析领域的书籍可谓是凤毛麟角。如果哪位读者对于恶意代码分析有浓厚的兴趣，要么是去一些大型的安全类论坛看他人的分析报告，要么是在众多的安全类书籍中，东找一点西凑一点地进行学习。这也就说明了市面...

第15章习题 Lab15.3中通过SEH来执行恶意代码，其还原存在一个问题 mov eax,large fs:0 // 获取Esp mov eax,[eax] // 获取ExceptionList mov eax,[eax] // 获取Next mov large fs:0 eax; // 还原fs:0
如下代码，其不仅将恶意代码从链表中摘除，也会摘除正常的第一个_EXCEPTION_R...

Practical Malware Analysis_下载链接1_