Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software

Michael Sikorski, Andrew Honig

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software

Michael Sikorski, Andrew Honig

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig

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*.

[Download](#) Practical Malware Analysis: The Hands-On Guide to ...pdf

[Read Online](#) Practical Malware Analysis: The Hands-On Guide t ...pdf

Download and Read Free Online Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig

---

From reader reviews:

Shad Broussard:

Book is to be different for every grade. Book for children until finally adult are different content. As you may know that book is very important for people. The book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software seemed to be making you to know about other knowledge and of course you can take more information. It is quite advantages for you. The publication Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software is not only giving you far more new information but also for being your friend when you experience bored. You can spend your own spend time to read your e-book. Try to make relationship while using book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. You never really feel lose out for everything should you read some books.

Loren Parker:

Is it anyone who having spare time then spend it whole day by watching television programs or just lying on the bed? Do you need something totally new? This Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software can be the reply, oh how comes? A book you know. You are and so out of date, spending your spare time by reading in this fresh era is common not a geek activity. So what these ebooks have than the others?

Charles Stubblefield:

Don't be worry for anyone who is afraid that this book will probably filled the space in your house, you can have it in e-book means, more simple and reachable. That Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software can give you a lot of buddies because by you investigating this one book you have point that they don't and make a person more like an interesting person. This specific book can be one of one step for you to get success. This e-book offer you information that might be your friend doesn't recognize, by knowing more than additional make you to be great persons. So , why hesitate? Let's have Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.

Laura McCallum:

A lot of e-book has printed but it differs. You can get it by net on social media. You can choose the top book for you, science, comic, novel, or whatever through searching from it. It is identified as of book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. You can contribute your knowledge by it. Without leaving behind the printed book, it can add your knowledge and make anyone happier to read. It is most essential that, you must aware about e-book. It can bring you from one destination for a other place.

Download and Read Online Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig #VQTHG43ODEN

Read Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig for online ebook

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig books to read online.

Online Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig ebook PDF download

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig Doc

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig Mobipocket

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig EPub