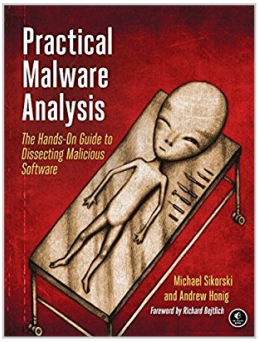

Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software

By Michael Sikorski, Andrew Honig

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

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

By Michael Sikorski, Andrew Honig

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

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

- Sales Rank: #29754 in Books
- Brand: No Starch Press
- Published on: 2012-03-03
- Original language: English
- Number of items: 1

- Dimensions: 9.25" h x 1.53" w x 7.00" l, 2.72 pounds
- Binding: Paperback
- 800 pages

Editorial Review

Amazon.com Review

Praise for *Practical Malware Analysis*

“The book every malware analyst should keep handy.”
--Richard Bejtlich, CSO, Mandiant & Founder of TaoSecurity

“An excellent crash course in malware analysis.”
--Dino Dai Zovi, Independent Security Consultant

“. . . the most comprehensive guide to analysis of malware, offering detailed coverage of all the essential skills required to understand the specific challenges presented by modern malware.”
--Chris Eagle, Senior Lecturer of Computer Science at the Naval Postgraduate School

“A hands-on introduction to malware analysis. I'd recommend it to anyone who wants to dissect Windows malware.”
--Ilfak Guilfanov, Creator of IDA Pro

“. . . a great introduction to malware analysis. All chapters contain detailed technical explanations and hands-on lab exercises to get you immediate exposure to real malware.”
--Sebastian Porst, Google Software Engineer

“. . . brings reverse engineering to readers of all skill levels. Technically rich and accessible, the labs will lead you to a deeper understanding of the art and science of reverse engineering. I strongly recommend this book for beginners and experts alike.”
--Danny Quist, PhD, Founder of Offensive Computing

“If you only read one malware book or are looking to break into the world of malware analysis, this is the book to get.”
--Patrick Engbretson, IA Professor at Dakota State University and Author of *The Basics of Hacking and Pen Testing*

“. . . an excellent addition to the course materials for an advanced graduate level course on Software Security or Intrusion Detection Systems. The labs are especially useful to students in teaching the methods to reverse engineer, analyze and understand malicious software.”
--Sal Stolfo, Professor, Columbia University

About the Author

Michael Sikorski is a Principal Consultant at Mandiant. He provides specialized research and development security solutions to the company's federal client base, reverse engineers malicious software discovered by incident responders, and has helped create a series of courses in malware analysis (from Beginner to Advanced). He has taught these courses to a variety of audiences including the FBI, the National Security

Agency (NSA), and BlackHat. A former member of MIT's Lincoln Laboratory and the NSA, he holds a Top Secret security clearance.

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.

Users Review

From reader reviews:

Robert Heck:

Reading a guide can be one of a lot of pastime that everyone in the world likes. Do you like reading book thus. There are a lot of reasons why people fantastic. First reading a e-book will give you a lot of new information. When you read a book you will get new information simply because book is one of numerous ways to share the information or maybe their idea. Second, studying a book will make anyone more imaginative. When you reading a book especially fictional book the author will bring you to imagine the story how the personas do it anything. Third, you are able to share your knowledge to others. When you read this Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, you could tells your family, friends and also soon about yours guide. Your knowledge can inspire average, make them reading a guide.

Elaine Roberts:

The publication untitled Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software is the reserve that recommended to you you just read. You can see the quality of the reserve content that will be shown to you actually. The language that author use to explained their way of doing something is easily to understand. The article author was did a lot of investigation when write the book, so the information that they share to you personally is absolutely accurate. You also could possibly get the e-book of Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software from the publisher to make you much more enjoy free time.

Chris Barrentine:

Beside this Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software in your phone, it could give you a way to get nearer to the new knowledge or data. The information and the knowledge you can got here is fresh through the oven so don't become worry if you feel like an aged people live in narrow small town. It is good thing to have Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software because this book offers for your requirements readable information. Do you sometimes have book but you rarely get what it's exactly about. Oh come on, that would not happen if you have this with your hand. The Enjoyable option here cannot be questionable, just like treasuring beautiful island. Techniques you still want to miss the item? Find this book and read it from right now!

Victor Green:

Many people said that they feel uninterested when they reading a book. They are directly felt this when they get a half parts of the book. You can choose the particular book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software to make your personal reading is interesting. Your personal skill of reading talent is developing when you such as reading. Try to choose very simple book to make you enjoy you just read it and mingle the feeling about book and reading through especially. It is to be 1st opinion for you to like to open a book and learn it. Beside that the guide Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software can to be your new friend when you're feel alone and confuse in doing what must you're doing of that time.

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