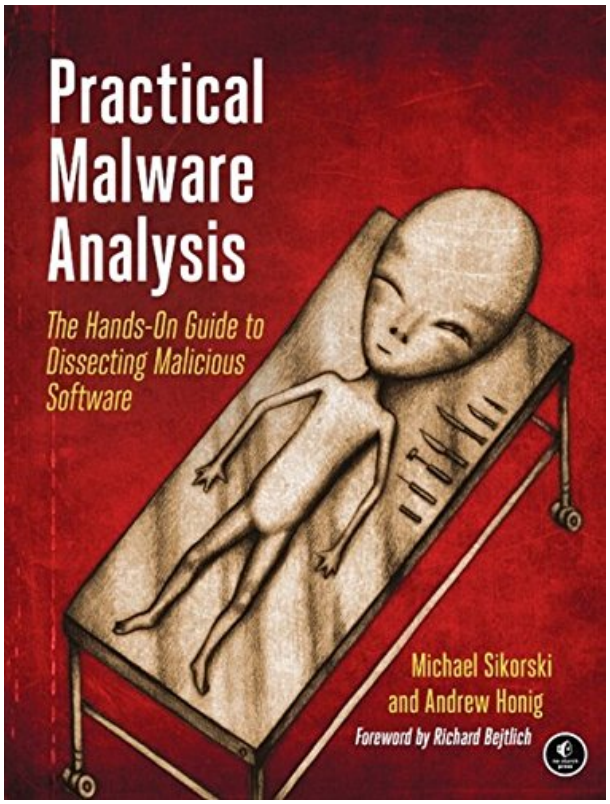
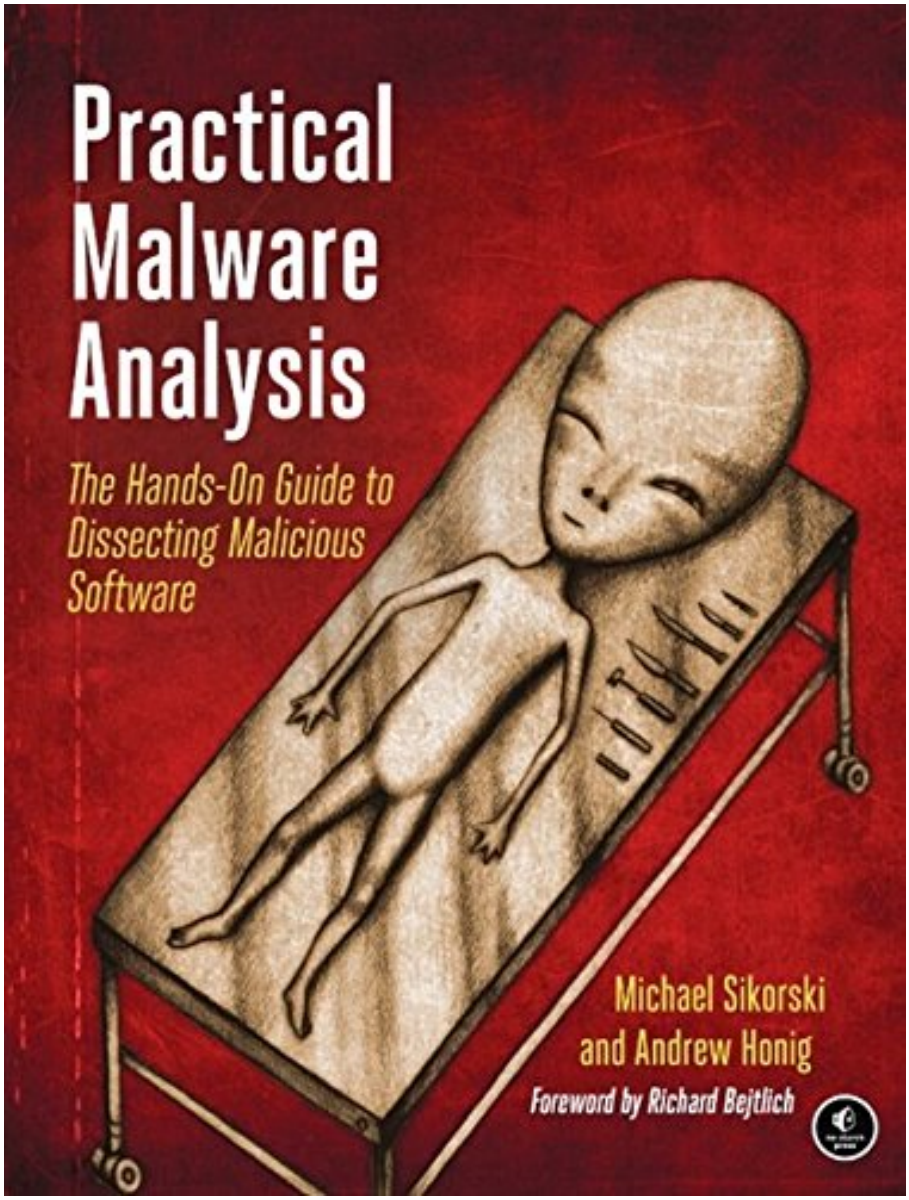
PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE BY MICHAEL SIKORSKI, ANDREW HONIG





PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE BY MICHAEL SIKORSKI, ANDREW HONIG PDF

Simply attach your gadget computer system or gizmo to the web linking. Get the contemporary innovation to make your downloading **Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig** finished. Also you don't intend to read, you can directly close guide soft documents and open Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig it later on. You could additionally easily get guide all over, since Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig it remains in your device. Or when being in the workplace, this Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig is additionally recommended to check out in your computer system gadget.

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.

PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE BY MICHAEL SIKORSKI, ANDREW HONIG PDF

Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig. Thanks for visiting the most effective site that provide hundreds type of book collections. Here, we will offer all books Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig that you need. Guides from well-known writers and authors are offered. So, you can delight in currently to obtain one at a time type of publication Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig that you will look. Well, related to guide that you want, is this Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig your choice?

Undoubtedly, to boost your life quality, every publication *Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig* will have their particular session. However, having particular awareness will make you really feel a lot more certain. When you feel something occur to your life, occasionally, checking out book Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig could aid you to make tranquility. Is that your real pastime? Sometimes of course, yet often will certainly be not exactly sure. Your choice to read Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig as one of your reading publications, could be your proper book to read now.

This is not around just how considerably this e-book Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig expenses; it is not also about exactly what type of book you truly enjoy to check out. It is regarding exactly what you can take as well as obtain from reviewing this Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig You can choose to select various other publication; yet, it doesn't matter if you try to make this publication Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig as your reading selection. You will certainly not regret it. This soft data book Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig can be your buddy regardless.

PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE BY MICHAEL SIKORSKI, ANDREW HONIG PDF

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.

- Sales Rank: #17191 in Books
- 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

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.

Most helpful customer reviews

41 of 43 people found the following review helpful.
My passport into understanding malware

By Stephen Northcutt
have been carrying this book around for three weeks and I have only made it to page 604 which is deep in the appendices, but wanted to jot down some thoughts. The book tries to be self contained, as little prior knowledge as possible is assumed. They begin by talking about static (not actually executing) and dynamic analysis followed by a malware taxonomy. By page 10 the authors show you something very useful, how to run MD5 on a Windows system. We also learn about packing which is very important in the analysis of malware and get introduced to PEiD, which unfortunately has been discontinued, version 0.95 is the last, but it still works fine. Next is PEview to look at the PE sections. All that is chapter one and my point is that anyone with a windows system and interest can use these tools and learn a lot about what goes on in a Windows system.

The next topic is virtual systems which is hugely important since you don't want to experiment with malware on your work laptop, no good can come of that. Chapter 3 requires the reader to be slightly technical, but it is all great stuff, process monitor and process explorer, and looking at strings and dependencies. I do not see how anyone that has hands on responsibility for security of Windows systems can rationalize not being familiar with these tools.

Chapter 4 is where they start the deep dive, registers and opcodes, the fundamentals of disassembly and of course we can't get anywhere without IDA Pro, so that comes right up.

Speaking of tools that have been around for a while, I was surprised that OllyDbg is still a major debugger, good on you Mr. Yuschuk. After this, the books starts to move past my technical depth. I did learn some things, I just could not follow everything, but here are a few facts I am glad I learned.

Most malware uses Berkeley style sockets, just like Unix
I really enjoyed the explanation on how to look at the Poison Ivy trojan with OllDbg
The explanation on how to use Netcat to create a reverse shell
How to use Pwdump and Pass-The-Hash
The whole concept of anti-debugging and especially using code checksums to identify a debugger is being used

Don't miss appendix B, they have taken many of the tools discussed in the text and put them in once place with a handy paragraph explanation for each one.

14 of 15 people found the following review helpful.
Navigate the Wilds of Malware
By Michael Larsen
This is a topic that has greatly interested me, but from the perspective of a tester. On one side, I think the ability to reverse engineer malware is fascinating, but more to the point what I really want to be able to do is see how the tools described can actually be used to augment security testing.

Malware has become one of those topics that we often wring our hands about because we know it's a threat, we want to better comprehend it, but do we dare open ourselves up to the potential of doing something wrong and unleashing an unintended havoc on our machines or networks? Fortunately, Michael Sikorski & Andrew Honig's book "Practical Malware Analysis" helps to de-mystify this type of operation, and also make it understandable from a variety of perspectives. If you are a programmer, this will be very handy. Even if you aren't, there is a lot of good ideas and techniques in this book that you can use.

Practical Malware Analysis is structured with regular chapters describing the concepts, and each chapter

ends with a series of labs. the answers to these labs take up nearly a third of the book. They consist of short answers for the specific questions as well as longer form answers that go into great detail to describe the steps and the methods used to test the files and provide analysis of what was found.

Part 1 starts out by explaining what Malware is and how developers and testers can get into the files and poke around using some basic and freely available tools. The first part of the book focuses on performing static analysis of files and looking inside them to understand what might be hiding in the files, along with ways o read the headers, strings and data hidden in the files. To get beyond the static analysis, the users are guided through setting up a virtual machine environment using VMWare. Dynamic Analysis is what happens when a piece of malware is actually run, and the determination is made that static analysis just won't cut it any longer. From here, we need to actually start poking at the malware and see what it will do in real time (yep, in that safe VM, using what's referred to as a "Malware Sandbox" consisting of a variety of free tools).

Part 2 of the book goes into greater detail regarding performing more advanced Static Analysis techniques, including dis-assembly, specifically dis-assembly on x86 Architecture processors, reverse engineering using tools such as IDA Pro (it gets its own chapter and shows up in the future labs), examining how to get a high level view of the code using code constructs, and how to use the tools to recognize when we are seeing those code constructs in assembly language. since Windows is the target of choice for most malware, Chapter 7 goes into specifics about how to recognize and work with the Windows API and use the registry editor to analyze registry code. Processes, threads, and network functionality are also primary considerations.

Part 3 brings us into the realm of more advanced Dynamic Analysis. Starting with debugging at both language and assembler levels, we see how to step through programs a piece at a time so we can see what is happening or change the way the code executes. Dedicated chapters to OllyDbg (a user level debugger) and WinDbg (a kernel level debugger) show how to do these steps with these specific tools.

Part 4 focuses on the way that malware behaves and what sets a program apart as being malware. It examines a variety of back doors in the system and ways the program can steal credentials, and how it covers its tracks so as to not be easily detected. Chapter 12 focuses on how Malware starts itself, and the variety of methods it uses, including process replacement and DLL manipulation so that it looks like any other innocuous running process. Chapter 13 goes into a variety of methods of encoding and decryption, while Chapter 14 covers ways in which the network is utilized to to take advantage of exploits.

Part 5 is Anti-Reverse-Engineering, and goes into the steps that malware developers go to to prevent their programs from being found or being cracked, Obscuring flow control, confusing dis-assemblers, prevent debugging, performing steps to use virtual machine detection and change the behavior or not run at all, and using methods to compress or encrypt files so that they are packed away until a given time or condition are all part of the toolkit of the malware developer to throw the malware examiner/tester off their tracks. we have to realize that while we are trying to outsmart the malware developers, they are trying to outsmart us as well.

Part 6 is a grab back of special topics including shell code analysis, special considerations for C++ code and how it differs from C, and some of the special challenges that the 64 bit processors and code base face and will face in the future.

The book rounds out with there appendices; describing important windows functions, a grab bag of tools that can be used fr malware analysis, and the biggest single section of the book, which is the answers and analysis to all of the labs provided.

This is a big book, and it covers a lot of ground. It is of course geared towards software developers, but

there's a tremendous wealth of information for the software tester, too. While we may not spend as much time de-compiling or reverse engineering the code, having the ability to see the techniques that malware developers use, and the techniques that we can use to ferret out and stop them is enlightening. This book focuses on Windows and Windows exploits, and it's meant to be an introductory primer. It's not the be all and end off of malware analysis, but for many of us who are not specifically trying to be security experts, it's a heck of an introduction.

More than being a good introduction, this is a "get your hands dirty and do so without putting your self or your neighbors in peril" book. This is a dicey topic, and its one where, in the wrong hands, or handled carelessly, you can do a lot of damage to your self and to others, so take the time to set up, wall off, and sand box as much as you can. Proceed with caution, but if you do proceed, you couldn't ask for a better tour guide.

12 of 13 people found the following review helpful.
The Best Book on Reverse Engineering Malware
By Danny
Before getting into reviewing Practical Malware Analysis, I hope you will indulge me in a rant about other books on the reverse engineering topic: They are not pretty. If you've taken one of my classes I recommend a few books for learning reversing, but climbing the steep mountain of pre-requisite material before you can attempt to be somewhat proficient is daunting. Specifically the books I recommended were based off of each individual author's own personal style of reverse engineering with the tools that were available at the time. The field has gotten much more accessible thanks to the awesome tools that are out there from companies like Hex-Rays and Zynamics.

Practical Malware Analysis does a good job of tying together the methods of modern malware analysis. While most of the previous texts have done a good job of presenting the state of the art at their time, PMA overviews many of the tools that are in use in the modern day. Part 1 starts off with the basic static techniques, how to set up a virtual environment, and dynamic analysis. These initial steps are the basis for any good reversing environment. What is nice is that these topics aren't dwelled on for an entire book.

Part 2 goes over the relationships of the Intel architecture, IDA Pro, modern compilers, and the Windows operating system to reverse engineering. Having an understanding of this as it applies to the reversing process is extremely important. Outside implementing a compiler, learning the fundamentals of the architecture is the most important skill a reverser can have for understanding the field. The difference between an adequate reverser and a great reverser lies in the understanding of how the system interactions work.

The rest of the book is focused on the advanced topics of dynamic analysis. Part 5 deals with all the ways that malware authors can make your life miserable, from anti-disassembly to packers. Part 6, "Special Topics," talks about shellcode analysis, C++ specifics, and the ever-looming threat of 64-bit malware. I suspect that there will be a second edition once 64-bit malware comes in vogue.

Overall the book is excellent for those that are new to this field. Experts love to curmudgeonly talk about how nothing is new anymore, everything sucks, and pine for the good old days of reverse engineering with some wire-wrap, a lead pencil, a 9-volt Duracell, and a single LED. If you consider yourself one of these people, reading this book is going to feel a lot like wearing someone else's underwear. If, on the other hand, you read it and put aside your natural skepticism of all things new, you might learn something.

I really do like this book.

See all 65 customer reviews...

PRACTICAL MALWARE ANALYSIS: THE HANDS-ON GUIDE TO DISSECTING MALICIOUS SOFTWARE BY MICHAEL SIKORSKI, ANDREW HONIG PDF

By downloading this soft data publication **Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig** in the on-line web link download, you remain in the 1st step right to do. This website really offers you ease of ways to obtain the very best publication, from ideal seller to the new released e-book. You can find a lot more books in this site by checking out every link that we offer. Among the collections, Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig is one of the most effective collections to market. So, the first you obtain it, the very first you will certainly obtain all favorable for this publication Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software By Michael Sikorski, Andrew Honig

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.