



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

*Michael Sikorski, Andrew Honig*

Download now

[Click here](#) if your download doesn't start automatically

# 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:**

#### **Sharon Gaines:**

Book is to be different for each grade. Book for children until adult are different content. As it is known to us that book is very important for all of us. The book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software had been making you to know about other expertise and of course you can take more information. It is extremely advantages for you. The reserve Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software is not only giving you a lot more new information but also being your friend when you sense bored. You can spend your personal spend time to read your publication. Try to make relationship with the book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. You never experience lose out for everything in case you read some books.

#### **Lacey Clements:**

The book with title Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software includes a lot of information that you can study it. You can get a lot of profit after read this book. This book exist new know-how the information that exist in this e-book represented the condition of the world currently. That is important to yo7u to know how the improvement of the world. This kind of book will bring you inside new era of the syndication. You can read the e-book on the smart phone, so you can read the item anywhere you want.

#### **Alejandro Koenig:**

A lot of people always spent their particular free time to vacation as well as go to the outside with them friends and family or their friend. Do you know? Many a lot of people spent they will free time just watching TV, as well as playing video games all day long. If you need to try to find a new activity here is look different you can read a new book. It is really fun for you personally. If you enjoy the book that you read you can spent 24 hours a day to reading a publication. The book Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software it is very good to read. There are a lot of individuals who recommended this book. These people were enjoying reading this book. When you did not have enough space to create this book you can buy the particular e-book. You can m0ore very easily to read this book from a smart phone. The price is not too expensive but this book features high quality.

#### **Gary Williams:**

People live in this new day of lifestyle always make an effort to and must have the time or they will get lots of stress from both daily life and work. So , whenever we ask do people have extra time, we will say absolutely sure. People is human not just a robot. Then we inquire again, what kind of activity do you possess when the spare time coming to an individual of course your answer will certainly unlimited right. Then do you ever try this one, reading ebooks. It can be your alternative in spending your spare time, typically the book you have read is actually Practical Malware Analysis: The Hands-On Guide to Dissecting

Malicious Software.

**Download and Read Online Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Michael Sikorski, Andrew Honig #I3Q5L4HNMUT**

## **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**