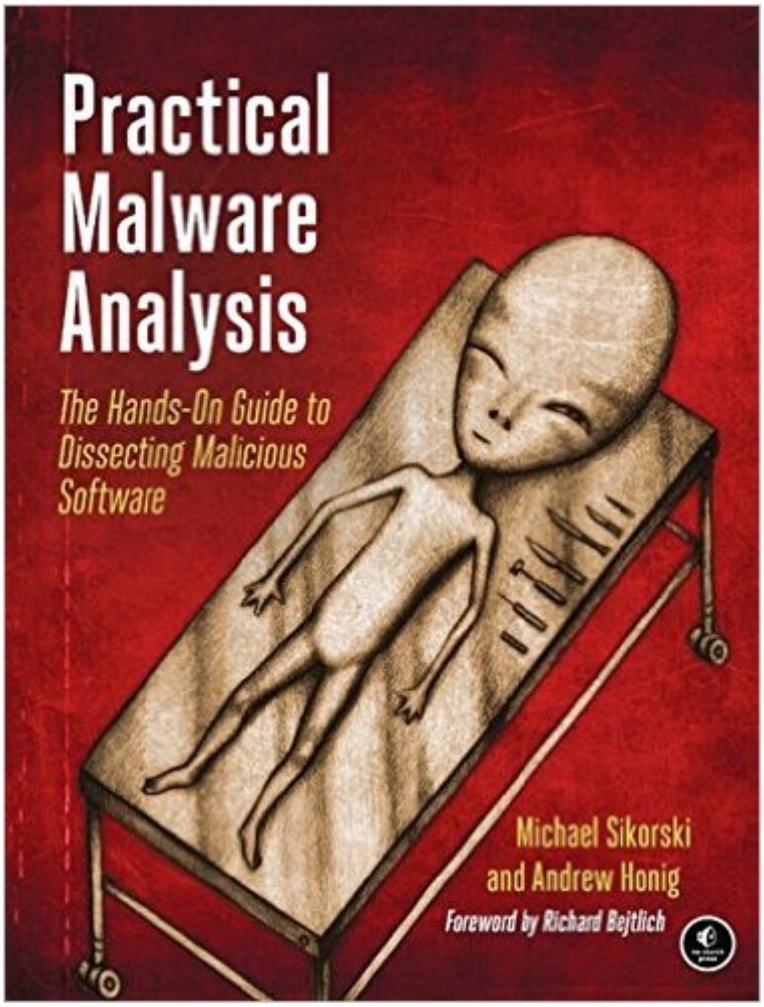
Practical Malware Analysis: The Hands-On Guide To Dissecting Malicious Software



Synopsis

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 malwareQuickly extract network signatures and host-based indicatorsUse key analysis tools like IDA Pro, OllyDbg, and WinDbgOvercome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniquesUse your newfound knowledge of Windows internals for malware analysisDevelop a methodology for unpacking malware and get practical experience with five of the most popular packersAnalyze 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.

Book Information

Paperback: 800 pages
Publisher: No Starch Press; 1 edition (March 3, 2012)
Language: English
ISBN-10: 1593272901
ISBN-13: 978-1593272906
Product Dimensions: 7 x 1.5 x 9.2 inches
Shipping Weight: 2.7 pounds (View shipping rates and policies)
Average Customer Review: 4.6 out of 5 starsÂ Â See all reviewsÂ (65 customer reviews)
Best Sellers Rank: #54,272 in Books (See Top 100 in Books) #23 inÂ Books > Computers & Technology > Security & Encryption > Viruses #36 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #110 inÂ Books > Computers & Technology >

Networking & Cloud Computing > Internet, Groupware, & Telecommunications

Customer Reviews

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.

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.

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.

Beginner’s Guide to Hacking (Programming, Penetration Testing, Network Security) (Cyber Hacking with Virus, Malware and Trojan Testing) Hacking: Viruses and Malware, Hacking an Email Address and Facebook page, and more! Cyber Security Playground Guide Malware, Rootkits & Botnets A Beginner’s Guide The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition Virus and Malware Removal Made Easy (2015) Accelerated Linux Core Dump Analysis: Training Course Transcript with GDB Practice Exercises (Pattern-Oriented Software Diagnostics, Forensics, Prognostics, Root Cause Analysis, Debugging Courses) Swift: Programming, Master’s Handbook: A TRUE Beginner’s Guide! Problem Solving, Code, Data Science, Data Structures & Algorithms (Code like a PRO in ... mining, software, software engineering,) How to Write a Software Patent Application: Your Guide to Quickly Writing Your US Software Patent Application Python: Learn Python in One Day and Learn It Well. Python for Beginners with Hands-on Project. (Learn Coding Fast with Hands-On Project Book 1) After Effects 5.0/5.5 Hands-On Training (Lynda Weinman’s Hands-On Training) CSS (with HTML5): Learn CSS in One Day and Learn It Well. CSS for Beginners with Hands-on Project. Includes HTML5. (Learn Coding Fast with Hands-On Project Book 2) C#: Learn C# in One Day and Learn It Well. C# for Beginners with Hands-on Project. (Learn Coding Fast with Hands-On Project Book 3) Code/Space: Software and Everyday Life (Software Studies)