Windows Malware Analysis Essentials

Victor Marak

Windows Malware Analysis Essentials

Victor Marak

Windows Malware Analysis Essentials Victor Marak

Master the fundamentals of malware analysis for the Windows platform and enhance your anti-malware skill set

About This Book

- Set the baseline towards performing malware analysis on the Windows platform and how to use the tools required to deal with malware
- Understand how to decipher x86 assembly code from source code inside your favourite development environment
- A step-by-step based guide that reveals malware analysis from an industry insider and demystifies the process

Who This Book Is For

This book is best for someone who has prior experience with reverse engineering Windows executables and wants to specialize in malware analysis. The book presents the malware analysis thought process using a show-and-tell approach, and the examples included will give any analyst confidence in how to approach this task on their own the next time around.

What You Will Learn

- Use the positional number system for clear conception of Boolean algebra, that applies to malware research purposes
- Get introduced to static and dynamic analysis methodologies and build your own malware lab
- Analyse destructive malware samples from the real world (ITW) from fingerprinting and static/dynamic analysis to the final debrief
- Understand different modes of linking and how to compile your own libraries from assembly code and integrate the codein your final program
- Get to know about the various emulators, debuggers and their features, and sandboxes and set them up effectively depending on the required scenario
- Deal with other malware vectors such as pdf and MS-Office based malware as well as scripts and shellcode

In Detail

Windows OS is the most used operating system in the world and hence is targeted by malware writers. There are strong ramifications if things go awry. Things will go wrong if they can, and hence we see a salvo of attacks that have continued to disrupt the normal scheme of things in our day to day lives. This book will guide you on how to use essential tools such as debuggers, disassemblers, and sandboxes to dissect malware samples. It will expose your innards and then build a report of their indicators of compromise along with detection rule sets that will enable you to help contain the outbreak when faced with such a situation.

We will start with the basics of computing fundamentals such as number systems and Boolean algebra. Further, you'll learn about x86 assembly programming and its integration with high level languages such as C++.You'll understand how to decipher disassembly code obtained from the compiled source code and map it back to its original design goals.

By delving into end to end analysis with real-world malware samples to solidify your understanding, you'll sharpen your technique of handling destructive malware binaries and vector mechanisms. You will also be encouraged to consider analysis lab safety measures so that there is no infection in the process.

Finally, we'll have a rounded tour of various emulations, sandboxing, and debugging options so that you know what is at your disposal when you need a specific kind of weapon in order to nullify the malware.

Style and approach

An easy to follow, hands-on guide with descriptions and screenshots that will help you execute effective malicious software investigations and conjure up solutions creatively and confidently.

Download and Read Free Online Windows Malware Analysis Essentials Victor Marak

---

From reader reviews:

Phyllis Callahan:

Do you really one of the book lovers? If yes, do you ever feeling doubt when you are in the book store? Aim to pick one book that you find out the inside because don't determine book by its cover may doesn't work is difficult job because you are scared that the inside maybe not because fantastic as in the outside appear likes. Maybe you answer might be Windows Malware Analysis Essentials why because the wonderful cover that make you consider in regards to the content will not disappoint you actually. The inside or content is usually fantastic as the outside or maybe cover. Your reading 6th sense will directly show you to pick up this book.

Tyler Smith:

Many people spending their time period by playing outside together with friends, fun activity having family or just watching TV all day long. You can have new activity to enjoy your whole day by reading through a book. Ugh, do you consider reading a book can definitely hard because you have to bring the book everywhere? It fine you can have the e-book, bringing everywhere you want in your Touch screen phone. Like Windows Malware Analysis Essentials which is finding the e-book version. So , try out this book? Let's view.

Kenneth Cunningham:

This Windows Malware Analysis Essentials is fresh way for you who has intense curiosity to look for some information given it relief your hunger associated with. Getting deeper you in it getting knowledge more you know or else you who still having small amount of digest in reading this Windows Malware Analysis Essentials can be the light food for you personally because the information inside that book is easy to get through anyone. These books develop itself in the form and that is reachable by anyone, sure I mean in the e-book form. People who think that in guide form make them feel tired even dizzy this reserve is the answer. So there isn't any in reading a guide especially this one. You can find actually looking for. It should be here for an individual. So , don't miss it! Just read this e-book style for your better life as well as knowledge.

Susan Arnold:

You can find this Windows Malware Analysis Essentials by look at the bookstore or Mall. Simply viewing or reviewing it can to be your solve difficulty if you get difficulties for ones knowledge. Kinds of this guide are various. Not only simply by written or printed but in addition can you enjoy this book by simply e-book. In the modern era similar to now, you just looking by your mobile phone and searching what your problem. Right now, choose your personal ways to get more information about your e-book. It is most important to arrange you to ultimately make your knowledge are still revise. Let's try to choose suitable ways for you.

Read Windows Malware Analysis Essentials by Victor Marak for online ebook

Windows Malware Analysis Essentials by Victor Marak 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 Windows Malware Analysis Essentials by Victor Marak books to read online.

Online Windows Malware Analysis Essentials by Victor Marak ebook PDF download

Windows Malware Analysis Essentials by Victor Marak Doc

Windows Malware Analysis Essentials by Victor Marak Mobipocket

Windows Malware Analysis Essentials by Victor Marak EPub