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:

Dustin Singh:

Why don't make it to be your habit? Right now, try to prepare your time to do the important work, like looking for your favorite book and reading a e-book. Beside you can solve your long lasting problem; you can add your knowledge by the guide entitled Windows Malware Analysis Essentials. Try to make the book Windows Malware Analysis Essentials as your buddy. It means that it can being your friend when you really feel alone and beside that of course make you smarter than previously. Yeah, it is very fortuned in your case. The book makes you considerably more confidence because you can know every thing by the book. So , we should make new experience and knowledge with this book.

Derek McCaleb:

Reading a book tends to be new life style in this era globalization. With reading you can get a lot of information which will give you benefit in your life. Together with book everyone in this world can certainly share their idea. Ebooks can also inspire a lot of people. Plenty of author can inspire their reader with their story or perhaps their experience. Not only the storyplot that share in the publications. But also they write about advantage about something that you need illustration. How to get the good score toefl, or how to teach your kids, there are many kinds of book which exist now. The authors on this planet always try to improve their talent in writing, they also doing some research before they write to their book. One of them is this Windows Malware Analysis Essentials.

Ronald Stauffer:

Don't be worry when you are afraid that this book will certainly filled the space in your house, you may have it in e-book method, more simple and reachable. This specific Windows Malware Analysis Essentials can give you a lot of good friends because by you considering this one book you have point that they don't and make anyone more like an interesting person. This particular book can be one of one step for you to get success. This reserve offer you information that maybe your friend doesn't realize, by knowing more than some other make you to be great persons. So , why hesitate? We need to have Windows Malware Analysis Essentials.

Helen Richards:

A lot of publication has printed but it is different. You can get it by internet on social media. You can choose the most beneficial book for you, science, comic, novel, or whatever by searching from it. It is identified as of book Windows Malware Analysis Essentials. You can include your knowledge by it. Without causing the printed book, it might add your knowledge and make you actually happier to read. It is most essential that, you must aware about reserve. It can bring you from one spot to other place.

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