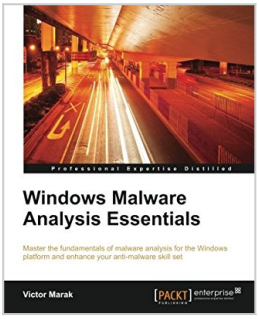

Windows Malware Analysis Essentials

By Victor Marak

Windows Malware Analysis Essentials By 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.

Windows Malware Analysis Essentials

By Victor Marak

Windows Malware Analysis Essentials By 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.

Windows Malware Analysis Essentials By Victor Marak Bibliography

- Rank: #1384510 in Books
- Published on: 2015-09-01
- Released on: 2015-09-01
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .75" w x 7.50" l, 1.25 pounds
- Binding: Paperback
- 330 pages

Editorial Review

About the Author

Victor Marak

Victor Marak is a security researcher, an electronic musician, and a world backpacker. He is a college dropout and an autodidact, and he loves working on interesting subjects such as medieval music composition, demonology, DSP electronics, and psychology. He has worked for start-ups, mid-tier, and fortune 500 companies with 5 years of experience in anti-virus technologies and malware research. He was into music production prior to joining the anti-malware industry, and his solo projects are on the world's largest electronic dance music market? Beatport, as well as other major retailers like iTunes, Amazon and Traxxsource. He is in perpetual backpacking mode, set to globe-trotting, especially to his favorite countries in Europe and Russia. He can be found hanging around in the wrong social networks - LinkedIn and Quora. This is his first book.

Users Review

From reader reviews:

Emily Meredith:

A lot of people always spent their particular free time to vacation or maybe go to the outside with them loved ones or their friend. Do you know? Many a lot of people spent these people free time just watching TV, or perhaps playing video games all day long. If you want to try to find a new activity here is look different you can read a book. It is really fun for you personally. If you enjoy the book that you simply read you can spent the entire day to reading a reserve. The book Windows Malware Analysis Essentials it is very good to read. There are a lot of individuals who recommended this book. These people were enjoying reading this book. In case you did not have enough space to create this book you can buy the e-book. You can m0ore quickly to read this book from the smart phone. The price is not very costly but this book has high quality.

Myrtle Galloway:

Do you have something that you want such as book? The publication lovers usually prefer to pick book like comic, short story and the biggest the first is novel. Now, why not hoping Windows Malware Analysis Essentials that give your enjoyment preference will be satisfied through reading this book. Reading routine all over the world can be said as the method for people to know world a great deal better then how they react to the world. It can't be mentioned constantly that reading practice only for the geeky individual but for all of you who wants to always be success person. So , for all of you who want to start reading as your good habit, you can pick Windows Malware Analysis Essentials become your own starter.

Sunday Richey:

In this particular era which is the greater man or woman or who has ability to do something more are more valuable than other. Do you want to become considered one of it? It is just simple strategy to have that. What

you should do is just spending your time little but quite enough to get a look at some books. One of the books in the top checklist in your reading list is usually Windows Malware Analysis Essentials. This book that is qualified as The Hungry Slopes can get you closer in becoming precious person. By looking way up and review this e-book you can get many advantages.

Keith Lugo:

As we know that book is significant thing to add our know-how for everything. By a publication we can know everything we would like. A book is a range of written, printed, illustrated or maybe blank sheet. Every year ended up being exactly added. This book Windows Malware Analysis Essentials was filled about science. Spend your extra time to add your knowledge about your science competence. Some people has several feel when they reading a book. If you know how big advantage of a book, you can sense enjoy to read a e-book. In the modern era like now, many ways to get book that you wanted.

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