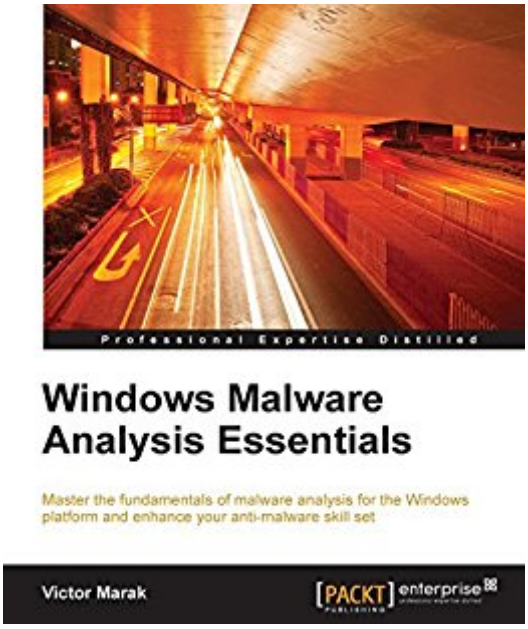
# Windows Malware Analysis Essentials



## Synopsis

Master the fundamentals of malware analysis for the Windows platform and enhance your anti-malware skill setAbout This BookSet the baseline towards performing malware analysis on the Windows platform and how to use the tools required to deal with malwareUnderstand how to decipher x86 assembly code from source code inside your favourite development environmentA step-by-step based guide that reveals malware analysis from an industry insider and demystifies the processWho This Book Is ForThis 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 LearnUse the positional number system for clear conception of Boolean algebra, that applies to malware research purposesGet introduced to static and dynamic analysis methodologies and build your own malware labAnalyse destructive malware samples from the real world (ITW) from fingerprinting and static/dynamic analysis to the final debriefUnderstand different modes of linking and how to compile your own libraries from assembly code and integrate the codein your final programGet to know about the various emulators, debuggers and their features, and sandboxes and set them up effectively depending on the required scenarioDeal with other malware vectors such as pdf and MS-Office based malware as well as scripts and shellcodeIn DetailWindows 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 approachAn 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.

## Book Information

File Size: 49294 KB

Print Length: 330 pages

Publisher: Packt Publishing; 1 edition (September 1, 2015)

Publication Date: September 1, 2015

Sold by:Â  Digital Services LLC

Language: English

ASIN: B014HFNB36

Text-to-Speech:  Enabled

X-Ray:  Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting:  Enabled

Best Sellers Rank: #791,323 Paid in Kindle Store (See Top 100 Paid in Kindle Store)  #196 inÂ Books > Computers & Technology > Security & Encryption > Viruses  #308 inÂ Books > Computers & Technology > Computer Science > Computer Simulation  #410 inÂ Books > Computers & Technology > Business Technology > Windows Server

## Customer Reviews

I have read through the chapters of this book several times, and it is helpful from start to finish. It starts out with well written introductory chapters to catch people back up on the knowledge they need in order to properly grasp later concepts, and it does it well! Concepts such as a basic understanding of bits and x86 assembly that are not otherwise easily grasped. This book also contains a plethora of information on malware structure, basic tooling used to understand malware, and is often written in a playful and enjoyable manner that assists in making the content a pleasure to read. I know it says "Windows" in the title, but many of the topics covered and tooling carries over to other platforms as well.

Very thorough book, I enjoyed reading it !The technical subject is quite high level but thanks to a wonderful and precise introduction about the basics of reverse engineering and disassembling, you

can attain your goals of understanding malicious codes.I recommend tremendously !

Wonderful published book. Great vendor!!



WINDOWS 10: WINDOWS 10 COMPANION: THE COMPLETE GUIDE FOR DOING ANYTHING WITH WINDOWS 10 (WINDOWS 10, WINDOWS 10 FOR DUMMIES, WINDOWS 10 MANUAL, WINDOWS ... WINDOWS 10 GUIDE) (MICROSOFT OFFICE) Windows Malware Analysis Essentials Windows 10: The Ultimate User Guide To Microsoft's New Operating System - 33 Amazing Tips You Need To Know To Master Windows 10! (Windows, Windows 10 Guide,General Guide) Windows 10 For Beginners: Simple Step-by-Step Manual On How To Customize Windows 10 For Your Needs.: (Windows 10 For Beginners - Pictured Guide) ... 10 books, Ultimate user guide to Windows 10) Group Policy: Management, Troubleshooting, and Security: For Windows Vista, Windows 2003, Windows XP, and Windows 2000 Windows Command-Line for Windows 8.1, Windows Server 2012, Windows Server 2012 R2 (Textbook Edition) (The Personal Trainer for Technology) How to Stop E-Mail Spam, Spyware, Malware, Computer Viruses and Hackers from Ruining Your Computer or Network: The Complete Guide for Your Home and Work How to Set Up a Home Network: Share Internet, Files and Printers between Windows 7, Windows Vista, and Windows XP Windows 10: 2016 User Guide and Manual: Microsoft Windows 10 for Windows Users Windows 10: The Practical Step-by-Step Guide to Use Microsoft Windows 10 (Windows for Beginners and Beyond) Windows 10: A Beginner's User Guide to Windows 10 (The Ultimate Manual to operate Windows 10) Windows 10: User Guide and Manual 2016 - Everything You Need To Know About Microsoft's Best Operating System! (Windows 10 Programming, Windows 10 Software, Operating System) Windows 10: A Beginner To Expert Guide - Learn How To Start Using And Mastering Windows 10 (Tips And Tricks, User Guide, Windows For Beginners) Windows Group Policy: The Personal Trainer for Windows Server 2012 and Windows Server 2012 R2 Analytics: Data Science, Data Analysis and Predictive Analytics for Business (Algorithms, Business Intelligence, Statistical Analysis, Decision Analysis, Business Analytics, Data Mining, Big Data) Save America's Windows: Caring for older and historic wood windows. Windows Programming Made Easy: Using Object Technology, COM, and the Windows Eiffel Library Windows 10 for Seniors: Get Started with Windows 10 (Computer Books for Seniors series) Linux for Windows Addicts: A Twelve Step Program for Habitual Windows Users. Windows to Linux Migration Toolkit: Your Windows to Linux Extreme Makeover