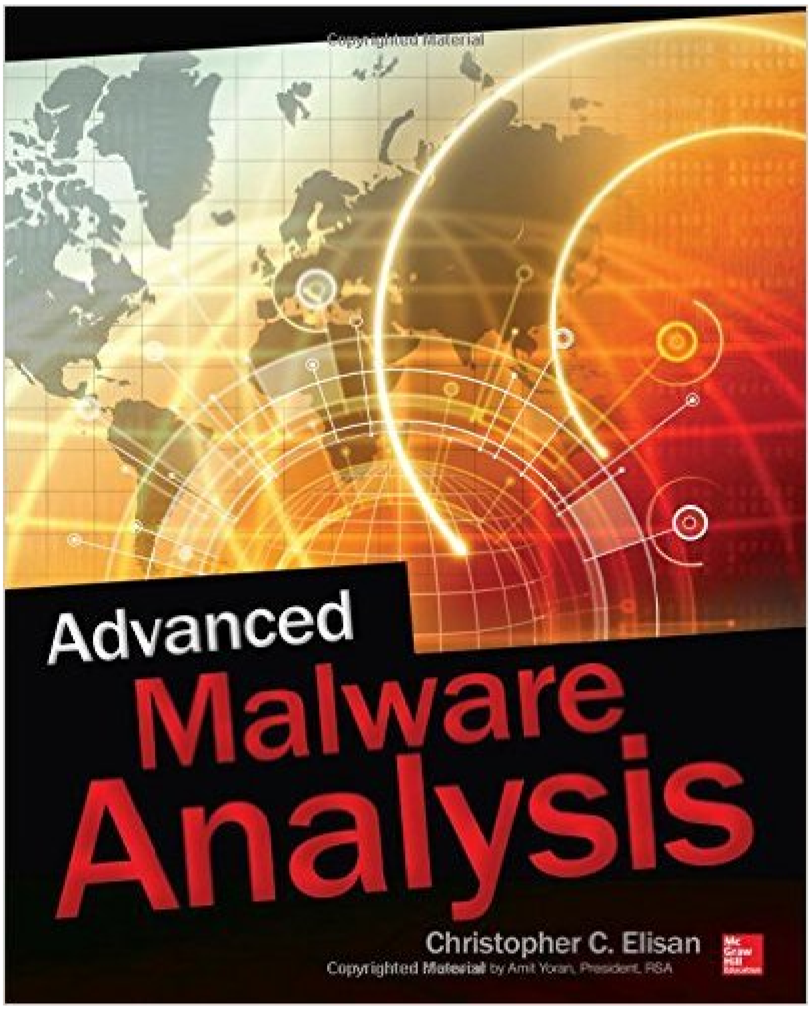
Advanced Malware Analysis



Synopsis

A one-of-a-kind guide to setting up a malware research lab, using cutting-edge analysis tools, and reporting the findings Advanced Malware Analysis is a critical resource for every information security professional’s anti-malware arsenal. The proven troubleshooting techniques will give an edge to information security professionals whose job involves detecting, decoding, and reporting on malware. After explaining malware architecture and how it operates, the book describes how to create and configure a state-of-the-art malware research lab and gather samples for analysis. Then, youâ ™ll learn how to use dozens of malware analysis tools, organize data, and create metrics-rich reports. A crucial tool for combatting malwareâ •which currently hits each second globally Filled with undocumented methods for customizing dozens of analysis software tools for very specific uses Leads you through a malware blueprint first, then lab setup, and finally analysis and reporting activities Every tool explained in this book is available in every country around the world

Book Information

Paperback: 544 pages

Publisher: McGraw-Hill Education; 1 edition (August 13, 2015)

Language: English

ISBN-10: 0071819746

ISBN-13: 978-0071819749

Product Dimensions: 7.3 x 1.1 x 9 inches

Shipping Weight: 1.7 pounds (View shipping rates and policies)

Average Customer Review: 1.6 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)

Best Sellers Rank: #1,268,318 in Books (See Top 100 in Books) #85 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Disaster & Recovery #188 inÂ Books > Computers & Technology > Security & Encryption > Viruses #650 inÂ Books > Computers & Technology > Databases & Big Data > Data Mining

Customer Reviews

Under a different title, I feel this book may have been okay (thus the two stars), but as it stands it is highly misleading. The most advanced concept covered in this book is arguably an in-depth copy/paste of the information contained within a PE file, which can easily be found online for free. In another section, the author walks you through the generation of an MD5 and SHA1 hash using Python without explaining fully what they’re useful for. On the next page, he suggests downloading a piece of software and "[making] sure that the one you are downloading is legitimate and not carrying any malicious software." This would be a wonderful time to mention using the hashes HE JUST INTRODUCED in a practical manner, but instead he keeps right on trucking into another "lab". These "labs" that the book so lovingly totes are little more than an excuse to use the Courier font and tend to span fewer than 15-20 lines. Most merely follow the pattern of "Install tool, run tool, compare output to this!". The book reads as though it was written with what the author could think up off the top of his head and arranged into semi-topical groups rather than a natural flow of important information.Overall, I would NOT recommend this book to anyone with any sort of background in malware analysis. Those just starting out or looking for a quick refresher may find some useful tidbits here and there, but there are certainly better books available for the price. Furthermore, this book only focuses on Windows malware. This isn't necessarily a bad thing, just something that may be good to know ahead of time.

This book is in no regard about "Advanced" malware analysis like the title suggests. It is not even an introductory malware analysis book. All the book covers is how to install various tools that you would need to start with malware analysis 101. The books doesn't show disassembly of malware, it doesn't discuss any Windows API calls or any other Windows internals. The book doesn't even teach you what malware really is.The first chapter (page 6) contains the following gem: "Static analysis is the easiest [...] malware analysis process. [...] It is as easy as clicking some buttons or using a command line". This sums up the book pretty well: according to the author, malware analysis is mostly about installing tools and clicking some buttons. That might be part of it, but I don't consider that "Advanced Malware Analysis" or even "Malware Analysis".What does the book tackle then? The book is mostly filled with screenshots and very detailled tutorials how to install tools.You got screenshots of the Windows update settings, the Windows 7 security settings, the user account settings, the word option setting. You even got a full page dedicated to a screenshot of xcopy.exe copying some files.An then you have tutorials. There are 25 pages dedicated how to install and use gpg to encrypt malware for moving it from source to analysis machine. Or tutorials how to install InstallRite. Of course accompanied by four screenshots of the install wizard with the options to click Next or Cancel.Chapter 11, "Inspecting Static Malware", is finally dedicated to analysing malware.

Download to continue reading...