1. Record Nr. UNINA9910466483403321

Autore	Monnappa K A
Titolo	Learning malware analysis : explore the concepts, tools, and techniques to analyze and investigate Windows malware / / Monnappa K A
Pubbl/distr/stampa	Birmingham ; ; Mumbai : , : Packt, , 2018
ISBN	1-78839-752-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (500 pages) : illustrations
Disciplina	005.84
Soggetti	Malware (Computer software) Computer security Computer software - Evaluation Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	Understand malware analysis and its practical implementation About This Book Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Who This Book Is For This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book. What You Will Learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Perform different code injection and hooking techniques Investigate and hunt malware using memory forensics In Detail Malware analysis and memory forensics are

powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. Style and approach The book takes the reader through al...