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 techniques.

This book constitutes the thoroughly refereed post-proceedings of the 11th International Conference on Computer Aided Systems Theory, EUROCAST 2007. Coverage in the 144 revised full papers presented includes formal approaches, computation and simulation in modeling biological systems, intelligent information processing, heuristic problem solving, signal processing architectures, robotics and robotic soccer, cybercars and intelligent vehicles and artificial intelligence components.
Access Free Malware Detection Using Assembly
And Api Call Sequences

A comprehensive guide to teach readers how to develop and implement effective malware detection and removal strategies using assembly and API call sequences. It provides methodologies and builds your own malware lab to 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 code in your final program. Get to know about the various emulators, debuggers, 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.
Access Free Malware Detection Using Assembly
And Api Call Sequences

This book explores a range of important theoretical and practical issues in the field of computational network application tools, while also presenting the latest advances and innovations using intelligent technology approaches. The main focus is on detecting and diagnosing complex application performance problems so that an optimal and expected level of system service can be attained and maintained. The book discusses challenging issues like enhancing system efficiency, performance, and assurance management, and blends the concept of system modeling and optimization techniques with soft computing, neural network, and sensor network approaches. In addition, it presents certain metrics and measurements that can be translated into business value. These metrics and measurements can also help to establish an empirical performance baseline for various applications, which can be used to identify changes in system performance. By presenting various intelligent technologies, the book provides readers with compact but insightful information on several broad and rapidly growing areas in the computation network application domain. The book's twenty-two chapters examine and address current and future research topics in areas like neural networks, soft computing, nature-inspired computing, fuzzy logic and evolutionary computation, machine learning, smart security, and wireless networking, and cover a wide range of applications from pattern recognition and system modeling, to intelligent control problems and biomedical applications. The book was written to serve a broad readership, including engineers, computer scientists, management professionals, and mathematicians interested in studying tools and techniques for computational intelligence and applications for performance analysis. Featuring theoretical concepts and best practices in computational network applications, it will also be helpful for researchers, graduate and undergraduate students with an interest in the fields of soft computing, neural networks, machine learning, sensor networks, smart security, etc.

This textbook surveys the knowledge base in automated and resilient cyber deception. It features four major parts: cyber deception reasoning frameworks, dynamic decision-making for cyber deception, network-based deception, and malware deception. An important distinguishing characteristic of this book is its inclusion of student exercises at the end of each chapter. Exercises include technical problems, short-answer discussion questions, or hands-on lab exercises, organized at a range of difficulties from easy to advanced. This is a useful textbook for a wide range of classes and degree levels within the security arena and other related topics. It's also suitable for researchers and practitioners with a variety of cyber security backgrounds from novice to experienced.

This book includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Computer Science, Informatics, and Systems Sciences, and Engineering. It includes selected papers from the conference proceedings of the Ninth International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2013). Coverage includes topics in: Industrial Electronics, Technology & Automation, Telecommunications and Networking, Systems, Computing Sciences and Software Engineering, Engineering Education, Instructional Technology, Assessment, and E-learning. Provides the latest in a series of books growing out of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering; includes chapters in the most advanced areas of Computing, Informatics, Systems Sciences, and Engineering; accessible to a wide range of readership, including
Access Free Malware Detection Using Assembly And Api Call Sequences

This book constitutes the proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defenses, RAID 2014, held in Gothenburg, Sweden, in September 2014. The 22 full papers were carefully reviewed and selected from 113 submissions, and are presented together with 10 poster abstracts. The papers address all current topics in computer security, including network security, authentication, malware, intrusion detection, browser security, web application security, wireless security, vulnerability analysis.

Mobile devices, such as smart phones, have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. In particular, the widespread presence of information-stealing applications and other types of mobile malware raises substantial security and privacy concerns. Android Malware presents a systematic view on state-of-the-art mobile malware that targets the popular Android mobile platform. Covering key topics like the Android malware history, malware behavior and classification, as well as, possible defense techniques.

This book presents state-of-the-art theories and technologies and discusses developments in the two major fields: engineering and sustainable computing. In this modern era of information and communication technologies [ICT], there is a growing need for new sustainable and energy-efficient communication and networking technologies. The book highlights significant current and potential international research relating to theoretical and practical methods toward developing sustainable communication and networking technologies. In particular, it focuses on emerging technologies such as wireless communications, mobile networks, Internet of things [IoT], sustainability, and edge network models. The contributions cover a number of key research issues in software-defined networks, blockchain technologies, big data, edge/fog computing, computer vision, sentiment analysis, cryptography, energy-efficient systems, and cognitive platforms.

Particularly in the fields of software engineering, virtual reality, and computer science, data mining techniques play a critical role in the success of a variety of projects and endeavors. Understanding the available tools and emerging trends in this field is an important consideration for any organization. Data Mining and Analysis in the Engineering Field explores current research in data mining, including the important trends and patterns and their impact in fields such as software engineering. With a focus on modern techniques as well as past experiences, this vital reference work will be of greatest use to engineers, researchers, and practitioners in scientific-, engineering-, and business-related fields.

This two-volume set (CCIS 1137 and CCIS 1138) constitutes the proceedings of the Third International Conference on Cyberspace Data and Intelligence, Cyber DI 2019, and the International Conference on Cyber-Living, Cyber-Syndrome, and Cyber-Health, CyberLife 2019, held under the umbrella of the 2019 Cyberspace Congress, held in Beijing, China, in December 2019. The 64 full papers presented together with 18 short papers were carefully reviewed and selected from 160 submissions. The papers are grouped in the following topics: Cyber Data, Information and Knowledge; Cyber and Cyber-enabled Intelligence; Communication and Computing; Cyber Philosophy, Cyberlogic and Cyber Science; and Cyber Health and Smart Healthcare.
Access Free Malware Detection Using Assembly And Api Call Sequences

The process of software reverse engineering and malware analysis often comprise a combination of static and dynamic analyses. The successful outcome of each step is tightly coupled with the functionalities of the tools and skills of the reverse engineer. Even though automated tools are available for dynamic analysis, the static analysis process is a fastidious and time-consuming task as it requires manual work and strong expertise in assembly coding. In order to enhance and accelerate the reverse engineering process, we introduce a new dimension known as clone-based analysis. Recently, binary clone matching has been studied with a focus on detecting assembly (binary) clones. An alternative approach in clone analysis, which is studied in the present research, is concerned with assembly to source code matching. There are two major advantages in considering this extra dimension. The first advantage is to avoid dealing with low-level assembly code in situations where the corresponding high-level code is available. The other advantage is to prevent reverse engineering parts of the software that have been analyzed before. The clone-based analysis can be helpful in significantly reducing the required time and improving the accuracy of static analysis. In this research, we elaborate a framework for assembly to open-source code matching. Two types of analyses are provided by the framework, namely online and offline. The online analysis process triggers queries to online source code repositories based on extracted features from the functions at the assembly level. The result is the matched set of references to the open-source project files with similar features. Moreover, the offline analysis assigns functionality tags and provides in-depth information regarding the potential functionality of a portion of the assembly file. It reports on function stack frames, prototypes, arguments, variables, return values and low-level system calls. Besides, the offline analysis is based on a built-in dictionary of common user-level and kernel-level API functions that are used by malware to interact with the operating system. These functions are called for performing tasks such as file I/O, network communications, registry modification, and service manipulation. The offline analysis process has been expanded through an incremental learning mechanism which results in an improved detection of crypto-related functions in the disassembly. The other developed extension is a customized local code repository which performs automated source code parsing, feature extraction, and dataset generation for code matching. We apply the framework in several reverse engineering and malware analysis scenarios. Also, we show that the underlying tools and techniques are effective in providing additional insights into the functionality, inner workings, and components of the target binaries.

Every day approximately three-hundred thousand to four-hundred thousand new malware are registered, many of them being adware and variants of previously known malware. Anti-virus companies and researchers cannot deal with such a deluge of malware – to analyze and build patches. The only way to scale the efforts is to build algorithms to enable machines to analyze malware and classify and cluster them to such a level of granularity that it will enable humans (or machines) to gain critical insights about them and build solutions that are specific enough to detect and thwart existing malware and generic-enough to thwart future variants. Advances in Malware and Data-Driven Network Security comprehensively covers data-driven malware security with an emphasis on using statistical, machine learning, and AI as well as the current trends in ML/statistical approaches to detecting, clustering, and classification of cyber-threats. Providing information on advances in malware and data-driven network security as well as future research directions, it is ideal for graduate students,
Access Free Malware Detection Using Assembly
And Api Call Sequences

This book constitutes the refereed post-proceedings of the 9th International Conference on Data-Driven Network Security, held in January 2020 at IIS University Jaipur, Rajasthan, India. The book includes high-quality, peer-reviewed papers from the conference, covering a range of topics related to data-driven network security.

The authors develop a malware fingerprinting framework to cover accurate android malware detection and family attribution in this book. The authors emphasize the following: (1) the scalability over a large malware corpus; (2) the resiliency to common obfuscation techniques; (3) the portability over different platforms and architectures. First, the authors propose an approximate fingerprinting technique for android packaging that captures the underlying static structure of the android applications in the context of bulk and offline detection at the app-market level. This book proposes a malware clustering framework to perform malware clustering by building and partitioning the similarity network of malicious applications on top of this fingerprinting technique. Second, the authors propose an approximate fingerprinting technique that leverages dynamic analysis and natural language processing techniques to generate Android malware behavior reports. Based on this fingerprinting technique, the authors propose a portable malware detection framework employing machine learning classification. Third, the authors design an automatic framework to produce intelligence about the underlying malicious cyber-infrastructures of Android malware. The authors then leverage graph analysis techniques to generate relevant intelligence to identify the threat effects of malicious Internet activity associated with android malware. The authors elaborate on an effective android malware detection system, in the online detection context at the mobile device level. It is suitable for deployment on mobile devices, using machine learning classification on method call sequences. Also, it is resilient to common code obfuscation techniques and adaptive to operating systems and malware change overtime, using natural language processing and deep learning techniques.

Researchers working in mobile and network security, machine learning and pattern recognition will find this book useful as a reference. Advanced-level students studying computer science within these topic areas will purchase this book as well.
Access Free Malware Detection Using Assembly And Api Call Sequences

This textbook surveys the knowledge base in automated and resilient cyber deception. It features four major parts: cyber deception reasoning frameworks, dynamic decision-making for cyber deception, network-based deception, and malware deception. An important distinguishing characteristic of this book is its inclusion of student exercises at the end of each chapter. Exercises include technical problems, short-answer discussion questions, or hands-on lab exercises, organized at a range of difficulties from easy to advanced. This is a useful textbook for a wide range of classes and degree levels within the security arena and other related topics. It’s also suitable for researchers and practitioners with a variety of cybersecurity backgrounds from novice to experienced.

Cybersecurity has been gaining serious attention and recently has become an important topic of concern for organizations, government institutions, and largely for people interacting with digital online systems. As many individual and organizational activities continue to grow and are conducted in the digital environment, new vulnerabilities have arisen which have led to cybersecurity threats. The nature, source, reasons, and sophistication for cyberattacks are not clearly known or understood, and many times invisible cyber attackers are never traced or can never be found. Cyberattacks can only be known once the attack and the destruction have already taken place long after the attackers have left. Cybersecurity for computer systems has increasingly become important because the government, military, corporate, financial, critical infrastructure, and medical organizations rely heavily on digital network systems, which process and store large volumes of data on computer devices that are exchanged on the internet, and they are vulnerable to “continuous” cyberattacks. As cybersecurity has become a global concern, it needs to be clearly understood, and innovative solutions are required. The Handbook of Research on Advancing Cybersecurity for Digital Transformation looks deeper into issues, problems, and innovative solutions and strategies that are linked to cybersecurity. This book will provide important knowledge that can impact the improvement of cybersecurity, which can add value in terms of innovation to solving cybersecurity threats. The chapters cover cybersecurity challenges, technologies, and solutions in the context of different industries and different types of threats. This book is ideal for cybersecurity researchers, professionals, scientists, scholars, and managers, as well as practitioners, stakeholders, researchers, academicians, and students interested in the latest advancements in cybersecurity for digital transformation.

Software similarity and classification is an emerging topic with wide applications. It is applicable to the areas of malware detection, software theft detection, plagiarism detection, and software clone detection. Extracting program features, processing those features into suitable representations, and constructing distance metrics to define similarity and dissimilarity are the key methods to identify software variants, clones, derivatives, and classes of software. Software Similarity and Classification reviews the literature of those core concepts, in addition to relevant literature in each application and demonstrates that considering these applied problems as a similarity and classification problem enables techniques to be shared between areas. Additionally, the authors present in-depth case studies using the software similarity and classification techniques developed throughout the book.

Although the use of data mining for security and malware detection is quickly on the rise, most books on the subject provide high-level theoretical discussions to the near exclusion of the practical aspects. Breaking the mold, Data Mining Tools for Malware Detection provides a step-by-step breakdown of how to develop data mining tools for malware detection. Integrating theory with practical techniques and experimental results, it focuses on malware detection applications for email worms, malicious code, remote exploits, and botnets.
The authors describe the systems they have designed and developed: email worm detection using data mining, a scalable multi-level feature extraction technique to detect malicious executables, detecting remote exploits using data mining, and flow-based identification of botnet traffic by mining multiple log files. For each of these tools, they detail the system architecture, algorithms, performance results, and limitations. Discusses data mining for emerging applications, including adaptable malware detection, insider threat detection, firewall policy analysis, and real-time data mining. Includes four appendices that provide a firm foundation in data management, secure systems, and the semantic web. Describes the authors' tools for stream data mining. From algorithms to experimental results, this is one of the few books that will be equally valuable to those in industry, government, and academia. It will help technologists decide which tools to select for specific applications, managers will learn how to determine whether or not to proceed with a data mining project, and developers will find innovative alternative designs for a range of applications.

Data mining analysis techniques have undergone significant developments in recent years. This has led to improved uses throughout numerous functions and applications. Intelligent Multidimensional Data Clustering and Analysis is an authoritative reference source for the latest scholarly research on the advantages and challenges presented by the use of cluster analysis techniques. Highlighting theoretical foundations, computing paradigms, and real-world applications, this book is ideally designed for researchers, practitioners, upper-level students, and professionals interested in the latest developments in cluster analysis for large data sets.

This book presents the latest advances and research findings in the fields of computational science and communication presented at the International Conference on Smart Innovations in Communications and Computational Sciences (ICSICCS 2020). The areas covered include smart innovation; systems and technologies; embedded knowledge and intelligence; innovation and sustainability; advanced computing; networking and informatics. It also focuses on the knowledge-transfer methodologies and the innovation strategies employed to make these effective. This fascinating compilation appeals to researchers, academics and engineers around the globe.

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: – Set up a safe virtual environment to analyze malware – Quickly extract network signatures and host-based indicators – Use key analysis tools like IDA Pro, OllyDbg, and WinDbg – Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques – Use your newfound knowledge of Windows internals for malware analysis – Develop a methodology for unpacking malware and get practical experience with five of the most popular packers – Analyze special cases of malware with shellcode, C++, and 64-bit code. Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You’ll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you’re tasked with securing one network or a thousand networks, or you’re making a living as a...
Access Free Malware Detection Using Assembly
And Api Call Sequences

This book focuses on the use of deep learning (DL) and artificial intelligence (AI) as tools to advance the fields of malware detection and analysis. The individual chapters of the book deal with a wide variety of state-of-the-art AI and DL techniques, which are applied to a number of challenging malware-related problems. DL and AI based approaches to malware detection and analysis are largely data driven and hence minimal expert domain knowledge of malware is needed. This book fills a gap between the emerging fields of DL/AI and malware analysis. It covers a broad range of modern and practical DL and AI techniques, including frameworks and development tools enabling the audience to innovate with cutting-edge research advancements in a multitude of malware (and closely related) use cases.

Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a “big data” problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you’ll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Saxe introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You’ll learn how to:
- Analyze malware using static analysis
- Observe malware behavior using dynamic analysis
- Identify adversary groups through shared code analysis
- Catch 0-day vulnerabilities by building your own machine learning detector
- Measure malware detector accuracy
- Identify malware campaigns, trends, and relationships through data visualization

Whether you’re a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.
Access Free Malware Detection Using Assembly And Api Call Sequences

In recent years, there has been a growing demand for more robust and efficient methods to detect and prevent malicious code, particularly as the prevalence of cyber threats continues to rise. The combination of information and communication technologies (ICT) has led to the development of new, innovative methods for detecting and mitigating the impact of malware.

The book highlights significant current and potential international research relating to theoretical and practical methods toward developing sustainable communication and networking technologies. In particular, it focuses on emerging technologies such as wireless communications, mobile networks, Internet of things (IoT), sustainability, and edge network models. The contributions cover a number of key research issues in software-defined networks, blockchain technologies, big data, edge/fog computing, computer vision, sentiment analysis, cryptography, energy-efficient systems, and cognitive platforms.

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using.

Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, as well as the data they manage.

Copyright code: 9ee6944bcf8fe3fe305da67fd73b8bc9

Copyright: app.panelsensor.com