Rather than enjoying a good book considering a mug of coffee in the afternoon, on the other hand they juggled later some harmful virus inside their computer. malware detection using assembly and api call sequences is easily reached in our digital library an online permission to it is set as public so you can download it instantly. Our digital library saves in combination countries, allowing you to acquire the most less latency period to download any of our books once this one. Merely said, the malware detection using assembly and api call sequences is universally compatible considering any devices to read.

Malware Detection-Mihai Christodorescu 2007-03-06 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, plus the data they manage.

The Huawei and Snowden Questions-Olav Lynse 2018-02-19 This open book access answers two central questions: firstly, is it at all possible to verify electronic equipment procured from untrusted vendors? Secondly, can I build trust into my products in such a way that I support verification by untrusting customers? In separate chapters the book takes readers through the state of the art in fields of computer science that can shed light on these questions. In a concluding chapter it discusses realistic ways forward. In discussions on cyber security, there is a tacit assumption that the manufacturer of equipment will collaborate with the user of the equipment to stop third-party wrongdoers. The Snowden files have revealed that equipment in the critical infrastructures of western countries has changed this. The discourse in both cases revolves around what malevolent manufacturers can do to harm their own customers, and the importance of the matter is on par with questions of national security. This book is of great interest to ICT and security professionals who need a clear understanding of the two questions posed in the subtitle, and to decision-makers in industry, national bodies and nation states.

Android Malware Detection using Machine Learning-ElMouatez Billah Karbab 2021-07-10 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.

Malware Analysis Using Artificial Intelligence and Deep Learning-Mark Stamp 2020-12-20 This book is focused 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 Analysis and Detection Engineering-Abhijit Mohanta 2020-11-05 Discover how the internals of malware work and how you can analyze and detect it. You will learn not only how to analyze and reverse malware, but also how to classify and categorize it, giving you insight into the intent of the malware. Malware Analysis and Detection Engineering is a one-stop guide to malware analysis that simplifies the topic by teaching you undocumented tricks used by analysts in the industry. You will be able to extend your expertise to analyze and reverse the challenges that malicious software throws at you. The book starts with an introduction to malware analysis and reverse engineering to provide insight on the different types of malware and also the terminology used in the anti-malware industry. You will know how to set up an isolated lab environment to safely execute and analyze malware. You will learn about malware packing, code injection, and process hollowing plus how to analyze, reverse, classify, and categorize malware using static and dynamic tools. You will be able to automate your malware analysis process by exploring detection tools to modify and trace malware programs, including sandboxes, IDS/IPS, anti-virus, and Windows binary instrumentation. The book provides comprehensive content in combination with hands-on exercises to help you dig into the details of malware dissection, giving you the confidence to tackle malware that enters your environment. What Will You Learn Analyze, dissect, reverse...
engineer, and classify malware Effectively handle malware with custom packers and compilers Unpack complex malware to locate vital malware components and decipher their intent. Use various static and dynamic malware analysis tools. Overwrite the internals of various detection engineering tools to improve your workflow. Write Snort rules and learn to use them with Suricata IDS. This book is for Security professionals, malware analysts, SOC analysts, incident responders, detection engineers, reverse engineers, and network security engineers. "This book is a must-have. If you're looking to master the ever-widening field of malware analysis, look no further. This is the definitive guide for you." - Pedram Amini, CTO, Inquest; Founder OpenRCE.org and ZeroDayInitiative

Encyclopedia of Cryptography and Security-Henk C.A. van Tilborg 2014-07-08 Explored into two volumes, the second edition of Springer's Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic. Definitive information on cryptography and information security from highly regarded researchers. Effective tool for professionals in many fields and researchers of all levels. Extensive resource with more than 700 contributions in Second Edition 1943 references, more than twice the number of references that appear in the first edition. With 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the first edition's base of 464 entries, the information in the encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The second edition's editorial board now includes 34 scholars, which was expanded from 18 members in the first edition. Representing the work of researchers from over 30 countries, the encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text's practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, references to related literature. Extensive cross-references within the encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the encyclopedia of cryptography and security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Applied Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

Malware Data Science-Joshua Saxe 2018 This title shows you how to apply machine learning, statistics and data visualization as you build your own detection and intelligence system. Following an overview of basic reverse engineering concepts like static and dynamic analysis, you'll learn to measure code similarities in malware samples and use machine learning frameworks like scikit-learn and Keras to build and train your own detectors.

Learning Malware Analysis-Monnappa K A 2018-06-29 Understand malware analysis and its practical implementation Key Features 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 Book Description 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 identify 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. What will you 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 real-world malware samples, infected memory images, and cross-references, in addition to significant research. This book is for incident responders, security professionals, system administrators, malware analysts, forensic practitioners, students, 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.

Detection of Intrusions and Malware, and Vulnerability Assessment-Ulrich Fiege 2013-03-15 This book constitutes the refereed post-proceedings of the 9th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2012, held in Heraklion, Crete, Greece, in July 2012. The revised full papers presented together with 4 short papers were carefully reviewed and selected from 44 submissions. The papers are organized in topical sections on malware, mobile security, secure design, and intrusion detection systems (IDS).

Data Mining Tools for Malware Detection-Mehedy Masud 2016-04-19 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. This book offers a great collection of data mining tools for malware detection and provides insights into the design and implementation of these tools. The book begins with an introduction to data mining, its applications, and how it can be used to detect malware. It then delves into advanced techniques for malware detection, including feature extraction, data pre-processing, and classification methods. The book covers a range of data mining tools, including decision trees, neural networks, and support vector machines. It includes practical examples and case studies to illustrate how these tools can be applied in real-world scenarios. Overall, Data Mining Tools for Malware Detection is a valuable resource for anyone looking to develop or improve 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.

**Intelligent Systems Design and Applications** - Ajith Abraham 2019-04-11 This book highlights recent research on Intelligent Systems and Nature Inspired Computing. It presents 212 selected papers from the 18th International Conference on Intelligent Systems Design and Applications (ISDA 2018) and the 10th World Congress on Nature and Biologically Inspired Computing (NaBIC), which was held at VIT University, India. ISDA-NaBIC 2018 was a premier conference in the field of Computational Intelligence and brought together researchers, engineers and practitioners whose work involved intelligent systems and their applications in industry and the “real world.” Including contributions by authors from over 40 countries, the book offers a valuable reference guide for all researchers, students and practitioners in the fields of Computer Science and Engineering.

**Mastering Malware Analysis** - Alexey Kleymenov 2019-06-06 Malware analysis is a powerful investigation technique widely used in various security areas including digital forensics and incident response processes. Working through practical examples, you’ll be able to analyze any type of malware you may encounter within the modern world.

**Autonomous Cyber Deception** - Elah Al-Shaer 2019-01-02 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 book 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.

**Detection of Intrusions and Malware, and Vulnerability Assessment** - Leyla Bilge 2021-07-09 This book constitutes the proceedings of the 18th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2021, held virtually in July 2021. The 18 full papers and 1 short paper presented in this volume were carefully reviewed and selected from 65 submissions. DIMVA serves as a premier forum for advancing the state of the art in intrusion detection, malware detection, and vulnerability assessment. Each year, DIMVA brings together international experts from academia, industry, and government to present and discuss novel research in these areas. Chapter “SPECULARIZER: Detecting Speculative Execution Attacks via Performance Tracking” is available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

**Proceedings of International Conference on Computational Intelligence and Data Engineering** - Nabendu Chaki 2020-12-20 This book is a collection of high-quality research work on cutting-edge technologies and the most-happening areas of computational intelligence and data engineering. It includes selected papers from the International Conference on Computational Intelligence and Data Engineering (ICCIDE 2020). It covers various topics, including collective intelligence, intelligent transportation systems, fuzzy systems, Bayesian network, ant colony optimization, data privacy and security, data mining, data warehousing, big data analytics, cloud computing, natural language processing, swarm intelligence and speech processing.

**Computational Network Application Tools for Performance Management** - Millie Pant 2019-12-24 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 computing 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.

**Android Malware** - Xuxian Jiang 2013-06-13 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.

**Sustainable Communication Networks and Application** - P. Karrupusamy 2019-11-07 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.

**Information and Operational Technology Security Systems** - Apostolos P. Fournaris 2019-03-23 This book constitutes the refereed proceedings of the First International Workshop, IOSec 2018, sponsored by CIPSEC, held in Heraklion, Crete, Greece, in September 2018. The 12 full papers presented were carefully reviewed and selected from 22 submissions. They were organized in topical sections named: Critical Infrastructure Cybersecurity Issues; CyberSecurity Threats, Assessment and Privacy; and Vulnerability and Malware Detection.
The Art of Computer Virus Research and Defense - Peter Szor 2005-02-03 Symantec’s chief antivirus researcher has written the definitive guide to contemporary virus threats, defense techniques, and analysis tools. Unlike most books on computer viruses, The Art of Computer Virus Research and Defense is a reference written strictly for white hats: IT and security professionals responsible for protecting their organizations against malware. Peter Szor systematically covers everything you need to know, including virus behavior and classification, protection strategies, antivirus and worm-blocking techniques, and much more. Szor presents the state-of-the-art in both analysis and protection, providing specific, implementation-based strategies to handle increasingly complex attacks. Along the way, he provides extensive information on code metamorphism and other emerging techniques, so you can anticipate and prepare for future threats. Szor also offers the most thorough and practical primer on virus analysis ever published—addressing everything from creating your own personal laboratory to automating the analysis process. This book’s coverage includes Discovering how malicious code attacks on a variety of platforms Classifying malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more Identifying and responding to code obfuscation threats: encrypted, polymorphic, and metamorphic Mastering empirical methods for analyzing malicious code—and what to do with what you learn Reverse-engineering malicious code with disassemblers, debuggers, emulators, and virtual machines Implementing technical defenses: scanning, code emulation, disinfection, inoculation, integrity checking, sandboxing, honeypots, behavior blocking, and much more Using worm blocking, host-based intrusion prevention, and network-level defense strategies

Security and Privacy Management, Techniques, and Protocols - Maleh, Yassine 2018-04-06 The security of information and communication technology is a high priority for any organization. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy Management, Techniques, and Protocols is a critical scholarly resource that examines emerging protocols and methods for effective management of information security at organizations. Featuring coverage on a broad range of topics such as cryptography, secure routing protocols, and wireless security, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on security and privacy management.

Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health - Haansheng Ning 2020-02-02 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.

Logging and Log Management - Anton Chuvakin 2012-12-31 Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; log analysis and protocallaggregation; analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolkits for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards, logging, and log analysis. This book is written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers. Comprehensive coverage of log management including analysis, visualization, reporting and more Includes information on different uses for logs - from system operations to regulatory compliance Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

Preventing Ransomware - Abhijit Mohanta 2018-03-23 Your one-stop guide to know digital extortion and it's prevention. Key Features A complete guide to how ransomware works Builds a security mechanism to prevent digital extortion. A practical approach to knowing about, and responding to, ransomware. Book Description Ransomware has been one of the full-code class attacks and it has affected numerous organizations in the recent past. The current need is to have a defensive mechanism in place for workstations and servers under one organization. This book starts by explaining the basics of malware, specifically ransomware. The book provides some quick tips on malware analysis and how you can identify different kinds of malware. We will also take a look at different types of ransomware, and how it reaches your system, spreads in your organization, and hijacks your computer. We will then move on to how the ransom is paid and the negative effects of doing so. We will learn how to respond quickly to ransomware attacks and how to protect yourself. The book gives a brief overview of the internals of security software and Windows features that can be helpful in ransomware prevention for administrators. You will also look at practical use cases in each stage of the ransomware phenomenon. The book talks in detail about the latest ransomware attacks involving WannaCry, Petya, and BadRabbit. By the end of this book, you will have end-to-end knowledge of the trending malware in the tech industry at present. What will you learn Understand malware types and malware techniques with examples Obtain a quick malware analysis Understand ransomware techniques, their distribution, and their payment mechanism Case studies of famous ransomware attacks Discover detection technologies for complex malware and ransomware Configure security software to protect against ransomware Handle ransomware infections Who this book is for This book is targeted towards security administrator, security analysts, or any stakeholders in the security sector who want to learn about the most trending malware in the current market: ransomware.

Innovative Security Solutions for Information Technology and Communications - Jean-Louis Lanet 2019-02-05 This book constitutes the thoroughly refereed proceedings of the 11th International Conference on Security for Information Technology and Communications, SecITC 2018, held in Bucharest, Romania, in November 2019. The 35 revised full papers presented together with 14 short papers were carefully reviewed and selected from 70 submissions. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.

Information Computing and Applications - Chunfeng Liu 2011-12-18 The two-volume set, CCIS 243 and CCIS 244, constitutes the refereed proceedings of the Second International Conference on Information Computing and Applications, ICICA 2010, held in Qinhuangdao, China, in October 2011. The 191 papers presented in both volumes were carefully reviewed and selected from numerous submissions. They are organized in topical sections on computational statistics, social networking and computing, evolutionary computing and applications, information education and application, internet and web computing, scientific and engineering computing, system simulation computing, bio-inspired and DNA computing, internet and Web computing, multimedia networking and computing, parallel and distributed computing.

Recent Advances in Intrusion Detection - Engin Kirda 2009-09-11 On behalf of the Program Committee, it is our pleasure to present the proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID 2009), held in Saint-Malo, France, during September 23-25. As in the past, the symposium brought together leading researchers and practitioners from academia, government, and industry to discuss intrusion detection research and practice. There were six main sessions: preemergent full research papers on anomaly and speciation; authentication-based approaches, malware detection and prevention, network intrusion detection and prevention, intrusion detection for mobile devices, and high-performance intrusion detection. Furthermore, there was a poster session on emerging research areas and case studies. The RAID 2009 Proceedings also contain 34 revised full paper submissions from all over the world. All submissions were carefully reviewed by independent viewers on the basis of space, topic, technical assessment, and overall balance. The 34 selected papers cover detection and prevention, analysis and visualization, and evaluation of secure systems and algorithms.
the symposium accepted submissions for poster presentations which have been published as - tended abstracts, reporting early-stage research, demonstration of applications, or case studies. Thirty posters were submitted for a numerical review by an independent, three-person sub-committee of the Program Committee based on novelty, description, and evaluation. The sub-committee recommended the - ceptance of 16 of these posters for presentation and publication. The success of RAID 2009 depended on the joint e?ort of many people.

Assembly Code Clone Detection for Malware Binaries-Mohammad Reza Farhadi 2013

Malware-Ed Skoudis 2004 Describes various types of malware, including viruses, worms, user-level RootKits, and kernel-level manipulation, their characteristics and attack method, and how to defend against an attack.

Cyber Threat Intelligence-Ali Dehghantanha 2018-04-27 This book provides readers with up-to-date research of emerging cyber threats and defensive mechanisms, which are timely and essential. It covers cyber threat intelligence concepts against a range of threat actors and threat tools (i.e. ransomware) in cutting-edge technologies, i.e., Internet of Things (IoT), Cloud computing and mobile devices. This book also provides the technical information on cyber-threat detection methods required for the researcher and digital forensics experts, in order to build intelligent automated systems to fight against advanced cybercrimes. The ever increasing number of cyber-attacks requires the cyber security and forensic specialists to detect, analyze and defend against the cyber threats in almost real-time, and with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions - this in essence defines cyber threat intelligence notion. However, such intelligence would not be possible without the aid of artificial intelligence, machine learning and advanced data mining techniques to collect, analyze, and interpret cyber-attack campaigns which is covered in this book. This book will focus on cutting-edge research from both academia and industry, with a particular emphasis on providing wider knowledge of the field, novelty of approaches, combination of tools and so forth to perceive reason, learn and act on a wide range of data collected from different cyber security and forensics solutions. This book introduces the notion of cyber threat intelligence and analytics and presents different attempts in utilizing machine learning and data mining techniques to create threat feeds for a range of consumers. Moreover, this book sheds light on existing and emerging trends in the field which could pave the way for future works. The inter-disciplinary nature of this book, makes it suitable for a wide range of audiences with backgrounds in artificial intelligence, cyber security, forensics, big data and data mining, distributed systems and computer networks. This would include industry professionals, advanced-level students and researchers that work within these related fields.

Rising Threats in Expert Applications and Solutions-Vijay Singh Rathore 2020 This book presents high-quality, peer-reviewed papers from the FICR International Conference on Rising Threats in Expert Applications and Solutions 2020, held at IIS University Jaipur, Rajasthan, India, on January 17-19, 2020. Featuring innovative ideas from a wide range of experts and practitioners in the field, this book covers a variety of topics, including expert applications and artificial intelligence/machine learning; advanced web technologies, like IoT, big data, and cloud computing in expert applications; information and cybersecurity threats and solutions; multimedia applications in forensics, security and intelligence; advances in app development; management practices for expert applications; and social and ethical aspects of expert applications in applied sciences.

Cuckoo Malware Analysis-Digit Oktavianito 2013-10-16 This is a step-by-step, practical tutorial for analyzing and detecting malware and performing digital investigations. This book features clear and concise guidance in an easily accessible format.Cuckoo Malware Analysis is great for anyone who wants to analyze malware through programming, networking, disassembling, forensics, and virtualization. Whether you are new to malware analysis or have some experience, this book will help you get started with Cuckoo Sandbox so you can start analyzing malware effectively and efficiently.

Cyber Deception-Sushil Jajodia 2016-07-15 This edited volume features a wide spectrum of the latest computer science research relating to cyber deception. Specifically, it features work from the areas of artificial intelligence, game theory, programming languages, graph theory, and more. The work presented in this book highlights the complex and multi-facted aspects of cyber deception and presents novel approaches to these problems. This book can be used as a text for a graduate-level seminar/course on cutting-edge computer science research relating to cyber-security, or as a supplemental text for a regular graduate-level course on cyber-security.

Windows Malware Analysis Essentials-Victor Marak 2015-09-01 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 Analyze 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.