1. Record Nr. UNINA9910983358003321

Autore	Gritzalis Dimitris
Titolo	Malware : Handbook of Prevention and Detection / / edited by Dimitris Gritzalis, Kim-Kwang Raymond Choo, Constantinos Patsakis
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	9783031662454 3031662458
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (0 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 91
Altri autori (Persone)	ChooKim-Kwang Raymond PatsakisConstantinos
Disciplina	005.8 323.448
Soggetti	Data protection - Law and legislation Artificial intelligence Computer networks - Security measures Privacy Artificial Intelligence Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I Theoretical foundation and modeling -- Chapter 1 Classifying Malware using Tensor Decomposition -- Chapter 2 Radial Spike and Slab Bayesian Neural Networks for Sparse Data in Ransomware Attacks -- Chapter 3 Mathematical models for malware propagation: state of art and perspectives -- Chapter 4 Botnet Defense System: A System to Fight Botnets with Botnets -- Part II Machine learning for malware classification -- Chapter 5 Machine Learning-Based Malware Detection in a Production Setting -- Chapter 6 Machine Learning for Windows Malware Detection and Classification: Methods, Challenges and Ongoing Research -- Chapter 7 Conventional Machine Learning-based Android Malware Detectors -- Chapter 8 Conventional Machine Learning-based Android Malware Detectors -- Chapter 9 Method to automate the classification of PE32 malware using Word2vec and LSTM -- Part III Social and legal -- Chapter 10 The South African and Senegalese legislative response to malware facilitated cybercrime --

Chapter 11Malware as a Geopolitical Tool.-Part IV Malware analysis in practice and evasions -- Chapter 12 Advancements in Malware Evasion: Analysis Detection and the Future Role of AI.-Chapter 13 Unpacking malware in the real world: a step by step guide -- Chapter 14 Forensic Analysis of CapraRAT Android Malware -- Chapter 15 Hidden Realms: Exploring Steganography Methods in Games for Covert Malware Delivery -- Part V Malware ecosystem -- Chapter 16 The Malware as a Service ecosystem -- Chapter 17Preventing and detecting malware in smart environments. The smart home case.

Sommario/riassunto

This book provides a holistic overview of current state of the art and practice in malware research as well as the challenges of malware research from multiple angles. It also provides step-by-step guides in various practical problems, such as unpacking real-world malware and dissecting it to collect and perform a forensic analysis. Similarly, it includes a guide on how to apply state-of-the-art Machine Learning methods to classify malware. Acknowledging that the latter is a serious trend in malware, one part of the book is devoted to providing the reader with the state-of-the-art in Machine Learning methods in malware classification, highlighting the different approaches that are used for, e.g., mobile malware samples and introducing the reader to the challenges that are faced when shifting from a lab to production environment. Modern malware is fueling a worldwide underground economy. The research for this book is backed by theoretical models that simulate how malware propagates and how the spread could be mitigated. The necessary mathematical foundations and probabilistic theoretical models are introduced, and practical results are demonstrated to showcase the efficacy of such models in detecting and countering malware. It presents an outline of the methods that malware authors use to evade detection. This book also provides a thorough overview of the ecosystem, its dynamics and the geopolitical implications are introduced. The latter are complemented by a legal perspective from the African legislative efforts, to allow the reader to understand the human and social impact of malware. This book is designed mainly for researchers and advanced-level computer science students trying to understand the current landscape in malware, as well as applying artificial intelligence and machine learning in malware detection and classification. Professionals who are searching for a perspective to streamline the challenges that arise, when bringing lab solutions into a production environment, and how to timely identify ransomware signals at scale will also want to purchase this book. Beyond data protection experts, who would like to understand how malware siphons private information, experts from law enforcement authorities and the judiciary system, who want to keep up with the recent developments will find this book valuable as well.