1. Record Nr. UNINA9910484631603321

Titolo	Malware Analysis Using Artificial Intelligence and Deep Learning / / edited by Mark Stamp, Mamoun Alazab, Andrii Shalaginov
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-62582-6
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XX, 651 p. 253 illus., 209 illus. in color.)
Disciplina	005.84
Soggetti	Computer crimes Machine learning Computational intelligence Data protection Computer Crime Machine Learning Computational Intelligence Security Services
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	1. Optimizing Multi-class Classication of Binaries Based on Static Features -- 2.Detecting Abusive Comments Using Ensemble Deep Learning Algorithms -- 3. Deep Learning Techniques for Behavioural Malware Analysis in Cloud IaaS -- 4. Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges -- 5. A Selective Survey of Deep Learning Techniques and Their Application to Malware Analysis -- 6. A Comparison of Word2Vec, HMM2Vec, and PCA2Vec for Malware Classication -- 7. Word Embedding Techniques for Malware Evolution Detection -- 8. Reanimating Historic Malware Samples -- 9. DURLD: Malicious URL detection using Deep learning based Character-level representations -- 10. Sentiment Analysis for Troll Detection on Weibo -- 11. Beyond Labeling: Using Clustering to Build Network Behavioral Proles of Malware Families -- 12. Review of the Malware Categorization in the Era of Changing Cybethreats Landscape: Common Approaches,

Challenges and Future Needs -- 13. An Empirical Analysis of Image-Based Learning Techniques for Malware Classication -- 14. A Survey of Intelligent Techniques for Android Malware Detection -- 15. Malware Detection with Sequence-Based Machine Learning and Deep Learning -- 16. A Novel Study on Multinomial Classication of x86/x64 Linux ELF Malware Types and Families through Deep Neural Networks -- 17. Cluster Analysis of Malware Family Relationships -- 18. Log-Based Malicious Activity Detection using Machine and Deep Learning -- 19. Deep Learning in Malware Identication and Classication -- 20. Image Spam Classication with Deep Neural Networks -- 21. Fast and Straightforward Feature Selection Method -- 22. On Ensemble Learning -- 23. A Comparative Study of Adversarial Attacks to Malware Detectors Based on Deep Learning -- 24. Review of Articial Intelligence Cyber Threat Assessment Techniques for Increased System Survivability -- 25. Universal Adversarial Perturbations and Image Spam Classiers.

Sommario/riassunto

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.