1. Record Nr.	UNINA9910299281403321
Titolo	Cyber Threat Intelligence / / edited by Ali Dehghantanha, Mauro Conti, Tooska Dargahi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-73951-4
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (334 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 70
Disciplina	005.8
Soggetti	Data protection Artificial intelligence Computer networks Data and Information Security Artificial Intelligence Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1 Introduction -- 2 Machine Learning Aided Static Malware Analysis -- 3 Application of Machine Learning Techniques to Detecting Anomalies in Communication Networks: Datasets and Feature Selection -- 4 Application of Machine Learning Techniques to Detecting Anomalies in Communication Networks: Classification Algorithms -- 5 Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection -- 6 Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware -- 7 BoTShark - A Deep Learning Approach for Botnet Traffic Detection -- 8 A Practical Analysis of The Rise in Mobile Phishing -- 9 PDF-Malware Detection: A Survey and Taxonomy of Current Techniques -- 10 Adaptive Traffic Fingerprinting for Darknet Threat Intelligence -- 11 A Model for Android and iOS Applications Risk Calculations: CVSS Analysis and Enhancement Using Case-Control Studies -- 12 A Honeypot Proxy Framework for Deceiving Attackers with Fabricated Content -- 13 Investigating the Possibility of Data Leakage in Time of Live VM Migration -- 14 Forensics Investigation of OpenFlow-Based SDN

Sommario/riassunto

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 backgroundsin 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.