Contents

Cyber Threat Intelligence: Challenges and Opportunities 1
Mauro Conti, Tooska Dargahi, and Ali Dehghantanha

Machine Learning Aided Static Malware Analysis: A Survey and Tutorial 7
Andrii Shalaginov, Sergii Banin, Ali Dehghantanha, and Katrin Franke

Application of Machine Learning Techniques to Detecting Anomalies in Communication Networks: Datasets and Feature Selection Algorithms 47
Qingye Ding, Zhida Li, Soroush Haeri, and Ljiljana Trajković

Application of Machine Learning Techniques to Detecting Anomalies in Communication Networks: Classification Algorithms 71
Zhida Li, Qingye Ding, Soroush Haeri, and Ljiljana Trajković

Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection 93
Omar M. K. Alhawi, James Baldwin, and Ali Dehghantanha

Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware 107
James Baldwin and Ali Dehghantanha

BoTShark: A Deep Learning Approach for Botnet Traffic Detection 137
Sajad Homayoun, Marzieh Ahmadzadeh, Sattar Hashemi, Ali Dehghantanha, and Raouf Khayami

A Practical Analysis of the Rise in Mobile Phishing 155
Brad Wardman, Michael Weideman, Jakub Burgis, Nicole Harris, Blake Butler, and Nate Pratt

PDF-Malware Detection: A Survey and Taxonomy of Current Techniques 169
Michele Elingiusti, Leonardo Aniello, Leonardo Querzoni, and Roberto Baldoni

Adaptive Traffic Fingerprinting for Darknet Threat Intelligence 193
Hamish Haughey, Gregory Epiphaniou, Haider Al-Khateeb, and Ali Dehghantanha

A Model for Android and iOS Applications Risk Calculation: CVSS Analysis and Enhancement Using Case-Control Studies 219
Milda Petraityte, Ali Dehghantanha, and Gregory Epiphaniou

A Honeypot Proxy Framework for Deceiving Attackers with Fabricated Content 239
Jarko Papalitsas, Sampsa Rauti, Jani Tammi, and Ville Leppänen

Investigating the Possibility of Data Leakage in Time of Live VM Migration 259
Rehana Yasmin, Mohammad Reza Memarian, Shohreh Hosseinzadeh, Mauro Conti, and Ville Leppänen

Forensics Investigation of OpenFlow-Based SDN Platforms 281
Mudit Kalpesh Pandya, Sajad Homayoun, and Ali Dehghantanha

Mobile Forensics: A Bibliometric Analysis 297
James Gill, Ihechi Okere, Hamed HaddadPajouh, and Ali Dehghantanha

Emerging from the Cloud: A Bibliometric Analysis of Cloud Forensics Studies 311
James Baldwin, Omar M. K. Alhawi, Simone Shaughnessy, Alex Akinbi, and Ali Dehghantanha

Index 333