Advances in Information Security 70

Ali Dehghantanha
Mauro Conti
Tooska Dargahi *Editors*

Cyber Threat Intelligence

Springer

Advances in Information Security

Volume 70

Series editor
Sushil Jajodia, George Mason University, Fairfax, VA, USA

More information about this series at http://www.springer.com/series/5576

Ali Dehghantanha • Mauro Conti
Tooska Dargahi
Editors

Cyber Threat Intelligence

BIBLIOTEKA
Nr ewid. ....
Akademii Sztuki Wojennej

Springer

Editors
Ali Dehghantanha
Department of Computer Science
University of Sheffield
Sheffield, UK

Mauro Conti
Department of Mathematics
University of Padua
Padua, Italy

Tooska Dargahi
Department of Computer Science
University of Salford
Manchester, UK

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-030-08891-0 ISBN 978-3-319-73951-9 (eBook)
https://doi.org/10.1007/978-3-319-73951-9

© Springer International Publishing AG, part of Springer Nature 2018
Softcover re-print of the Hardcover 1st edition 2018
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

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

Advances in Infor

Biblioteka Główna
Akademii Sztuki Wojennej
26638/III (CB)
03-026638-000-0

Ali Dehghantanha

Cyber Threat

Computer Science

ISBN 978-3-030-08891-0
9 783030 088910
▸ springer.com