Darkweb Cyber Threat Intelligence Mining

The important and rapidly emerging new field known as "cyber threat intelligence" explores the paradigm that defenders of computer networks gain a better understanding of their adversaries by understanding what assets they have available for an attack. In this book, a team of experts examines a new type of cyber threat intelligence from the heart of the malicious hacking underworld—the darkweb. These highly secure sites have allowed anonymous communities of malicious hackers to exchange ideas, techniques, and buy/sell malware and exploits.

Aimed at both cybersecurity practitioners and researchers, this book represents a first step toward a better understanding of malicious hacking communities on the darkweb and what to do about them. The authors examine real-world darkweb data through a combination of human and automated techniques to gain insight into these communities, describing both methodology and results.

JOHN ROBERTSON is a student at Arizona State University pursuing undergraduate degrees in both Computer Science and Electrical Engineering where his work has been nominated for the Computing Research Association's Outstanding Undergraduate Researcher award. He is a recipient of an ARO Undergraduate Research Apprenticeship Program grant as well as two Fulton Undergraduate Research Initiative grants for his work involving the application of artificial intelligence techniques to cybersecurity problems in the Cyber-Socio Intelligent System Laboratory with Dr. Paulo Shakarian. John also has industry experience as a software engineering intern with Microsoft on the Windows Core Development team.

AHMAD DIAB is a Computer Engineering Ph.D. student at Arizona State University. His current work in the Cyber-Socio Intelligent System Laboratory focuses on the application of AI techniques to cybersecurity problems. Ahmad is a recipient of SIPGA award from ASTAR agency, Singapore. Previously, he was a Java developer at EtQ compliance Company. Ahmad holds a B.S. in computer engineering from Jordan University of Science and Technology.

ERICSSON MARIN is a Computer Science Ph.D. Student at Arizona State University. He works at the Cyber-Socio Intelligent System Laboratory under the guidance of Dr. Paulo Shakarian, with research projects at the intersection of Social Network Analysis, AI and Cybersecurity. He received his M.Sc. in Computer Science from Federal University of Goias, Brazil, and has published numerous papers in the area of social network analysis. He also has real-world experience as a software designer managing different software factories. In 2015, Ericsson was awarded with a Brazilian Science Without Borders scholarship to pursue his Ph.D.

ERIC NUNES is a Ph.D. student in the computer engineering program at Arizona State University. His research focuses on the intelligence techniques to cybersecurity problems. Previously, Eric was a Research Associate at the Brain Engineering Lab at Dartmouth College. Eric holds an M.S. in Electrical Engineering from Syracuse University, New York.

VIVIN PALIATH is a Computer Science Ph.D. student at Arizona State University. His research at ASU focuses on the application of artificial intelligence and game-theoretic techniques to cybersecurity problems. Vivin received both his B.S. in Computer Engineering and M.S. in Computer Science from Arizona State University. He has more than a decade of industry experience and is also currently working as a Senior Software Engineer at Infusionsoft, a company that develops marketing-automation software for small businesses.

JANA SHAKARIAN is a research scientist at Arizona State University and has been researching malicious hacking groups and their online activity since 2012. She has coauthored two books, *Introduction to Cyber-Warfare* and *Computational Analysis of Terrorist Groups: Lashkar-e-Taiba*. She holds M.A. degrees in Sociology and Cultural and Social Anthropology from the Johannes Gutenberg University, Mainz, Germany. Previously, she was a staff social scientist for the University of Maryland Institute for Advanced Computer Studies where she worked with computer scientists on the cultural modeling of non-state armed actors and the interpretation of nonverbal communication.

PAULO SHAKARIAN is an Assistant Professor at Arizona State University's School of Computing, Informatics, and Decision Support Engineering where he directs the Cyber-Socio Intelligent System Laboratory, specializing in cyber-security, social network analysis, and AI. He has written numerous articles in scientific journals and has authored several books, including *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. His work has been featured in news outlets such as *The Economist, Popular Science*, and *WIRED*. He is a recipient of the Air Force Young Investigator Award, Fulton Entrepreneurial Professor award, MIT Technology Review's "Best of 2013," and the DARPA Service Chiefs' Fellowship.

Darkweb Cyber Threat Intelligence Mining

JOHN ROBERTSON, AHMAD DIAB,
ERICSSON MARIN, ERIC NUNES, VIVIN PALIATH,
JANA SHAKARIAN, AND PAULO SHAKARIAN
Arizona State University

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi - 110002, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of
education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107185777
DOI: 10.1017/9781316888513

First published 2017

Printed in the United States of America by Sheridan Books, Inc.

A catalogue record for this publication is available from the British Library.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-107-18577-7 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of
URLs for external or third-party Internet Web sites referred to in this publication
and does not guarantee that any content on such Web sites is, or will remain,
accurate or appropriate.

Contents

Foreword

A human activity undergoes “industrialization” when it adopts systematic means for the creation, production, and distribution of goods. A key ingredient of industrialization is the division of labor—including the specialization of basic research, commercialization, and end-user delivery and support. The net effect of industrialization is a profound amplification of both technology development and production capacity, typically leading to broader distribution and consumption of the underlying goods.

Darkweb Cyber Threat Intelligence Mining is the first principled study of the ongoing industrialization of cyber offense. It exposes the extent to which malware and associated attacker technologies have become commodity goods that are globally produced, marketed, distributed, and consumed.

Like eBay and Amazon, the darkweb is an online marketplace that brings cyber offense developers, buyers, and middlemen together. However, unlike eBay and Amazon, the darkweb is deliberately difficult to access and interpret by the outsider. The authors make a valuable contribution to the cyber defense community by describing a variety of technologies and techniques they have developed and used to penetrate the otherwise opaque cyber offense industrial base. As such, this book represents a seminal step toward leveling the cyber playing field. Because cybersecurity pits the creativity, knowledge, and technology of defenders against those of the attackers, each player must make great effort to understand and exploit the strengths and weakness of the other players. Cyber-attackers have had a decided edge in this respect for many years. Targeted applications and operating systems are easy to obtain and reverse engineer. Virtually all defensive technologies are open source or commercially available. Cyber defense research and deployment advances are widely published, promoted, and taught.

Thanks to the determined efforts of the authors and the documentation of their work in *Darkweb Cyber Threat Intelligence Mining*, we are for the first time able to shine persistent light on the emerging technologies and capabilities of cyber-attackers.

Many of us try to understand why, despite the increasing investments in cyber defense research and products, cybersecurity remains a huge, and possibly growing, challenge. I can’t help but think that a significant reason is that the offensive community has been quietly and covertly industrializing itself at a pace that defenders have not fully appreciated. Without visibility into that industrial base, defenders do not know what is in the production pipeline and cannot properly prepare. They can only react, as has traditionally been the case. This book might change that.

Darkweb Cyber Threat Intelligence Mining represents a tipping point in cyber security. It is a must-read for anyone involved in the modern cyber struggle.

George Cybenko
Dartmouth College
Grantham, NH, USA
August 29, 2016

Preface

Rapidly emerging is an exciting new field known as "cyber threat intelligence." The key idea with this paradigm is that defenders of computer networks gain a better understanding of their adversaries by analyzing what assets they have available for an attack. In this book, we examine a new type of cyber threat intelligence that takes one into the heart of the malicious hacking underworld—the darkweb. These highly secure sites have allowed for an anonymous community of malicious hackers to exchange ideas, techniques, and buy/sell malware and exploits. This book examines how we explored this problem through a combination of human and automated techniques to grasp a better understanding of this community. We describe both methodology and some of the resulting insights. This book serves as a first step toward a better understanding of malicious hacking communities on the darkweb.

The authors would like to acknowledge the generous support from the Arizona State University Global Security Initiative (GSI), the Office of Naval Research Neptune program, the Arizona State University Institute for Social Science Research (ISSR), and CNPq-Brazil, which have enabled our research in the area of cyber threat intelligence mined from the darkweb. Specific individuals, we would like to thank include Jamie Winterton, Nadya Bliss, H. Russel Bernard, William Brandt, Andrew Gunn, Robert Morgus, Frank Grimmelmann, Amanda Thart, and Vineet Mishra. We also would like to extend a special thanks to Lauren Cowels, our editor at Cambridge University Press, whose assistance throughout the creation of this book was much appreciated.