Malware Analysis Using Artificial Intelligence and Deep Learning

Mark Stamp · Mamoun Alazab ·
Andrii Shalaginov
Editors

Malware Analysis Using Artificial Intelligence and Deep Learning

Springer

Editors
Mark Stamp
Department of Computer Science
San Jose State University
San Jose, CA, USA

Mamoun Alazab
College of Engineering, IT & Environment
Charles Darwin University
Darwin, NT, Australia

Andrii Shalaginov
Faculty of Information Technology
and Electrical Engineering
Norwegian University of Science
and Technology
Gjøvik, Norway

ISBN 978-3-030-62581-8 ISBN 978-3-030-62582-5 (eBook)
https://doi.org/10.1007/978-3-030-62582-5

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

Preface

Artificial intelligence (AI) is changing the world as we know it. From its humble beginnings in the late 1940s as little more than an academic curiosity, AI has gone through multiple boom and bust cycles. With recent advances in machine learning (ML) and deep learning (DL), AI has finally taken root as a fundamental transformative technology. The changes wrought by AI already affect virtually every aspect of daily life, yet we are clearly only in the early stages of an AI-based revolution.

In the field of information security, there is no topic that is more significant than malware. The sheer volume of malware and the cost of dealing with its consequences are truly staggering. It is therefore timely to consider ML, DL, and AI in the context of malware analysis.

The chapters in this book apply numerous cutting-edge AI techniques to a wide variety of challenging problems in the malware domain. The book includes no less than 8 survey articles, which can serve to bring a reader quickly up to speed with the current state of the art. The heart of the book consists of 11 chapters that are tightly focused on AI-based techniques for malware analysis. We have also included 6 chapters where AI is applied to information security topics that are not strictly malware, but are closely related.

We are confident that this book will prove equally valuable to practitioners working in the trenches and to researchers at all levels. New and novel techniques as well as clever applications abound, yet we have strived to make the material accessible to the widest possible audience. It is our fervent hope—and firm belief—that the tools and techniques presented in the chapters of this book will play a major role in taming the malware threat.

San Jose, USA — Mark Stamp
Darwin, Australia — Mamoun Alazab
Gjøvik, Norway — Andrii Shalaginov
December 2020

Contents