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

Contents

Foreword *page* vii

By George Cybenko

Preface ix

1 **Introduction** 1

2 **Moving to Proactive Cyber Threat Intelligence** 4

2.1 Introduction 4

2.2 Proactive Intelligence beyond the Deepweb and Darkweb 7

2.3 Showing Value 10

3 **Understanding Darkweb Malicious Hacker Forums** 13

3.1 Introduction 13

3.2 Background 14

3.3 Methodology and Scope 17

3.4 Forum Structure and Community Social Organization 18

3.5 The Content of Observed Forums 28

3.6 Conclusion 36

4 **Automatic Mining of Cyber Intelligence from the Darkweb** 38

4.1 Introduction 38

4.2 System Overview 40

4.3 Evaluation 42

4.4 Related Work 54

4.5 Conclusion 54

5 **Analyzing Products and Vendors in Malicious Hacking Markets** 56
- 5.1 Introduction 56
- 5.2 Marketplace Data Characteristics 57
- 5.3 Users Having Presence in Markets/Forums 57
- 5.4 Discovery of Zero-Day Exploits 58
- 5.5 Exploits Targeting Known Vulnerabilities 60
- 5.6 Identifying Specific Product Categories 61
- 5.7 Conclusion 66

6 **Using Game Theory for Threat Intelligence** 67
- 6.1 Introduction 67
- 6.2 Security Game Framework 70
- 6.3 Computational Complexity 75
- 6.4 Algorithms 83
- 6.5 Evaluation and Discussion 89
- 6.6 Conclusion 95

7 **Application: Protecting Industrial Control Systems** 96
- 7.1 Introduction 96
- 7.2 Background 97
- 7.3 Model 98
- 7.4 Computational Complexity 105
- 7.5 Algorithms 107
- 7.6 Experimental Results 112
- 7.7 Related Work 116
- 7.8 Conclusion 117

8 **Conclusion** 118
- 8.1 Introduction 118
- 8.2 Environmental Characteristics 119
- 8.3 Challenges 120
- 8.4 Conclusion 121

Glossary 123

References 127

Index 135