Contents

Aim xviii
Audience xix
Contributors xx
Acknowledgments xxi

Chapter 1 Cybersecurity and the Dark Web 1

Introduction 1
Cybercrime and Cybersecurity 1
Cybercrime 1
Cybersecurity 3
Web and Its Levels 5
Web Levels 5
Web Categories 5
The Consequences of Criminal Activity on the DW 8
Trojan Horses, Worms, and Malware 9
Ransomware 9
Distributed DoS Attack 10
Social Network (SN) Attacks 12
Scareware 12
Botnets and Zombies 12
Key Hitches 13
Categories of Crime 13
DW Malicious Activities 14
Malware Classification 15
Cyberspace Malware Challenges 15
Malware Analysis 16
Static Analysis 17
Dynamic Analysis 17
Hybrid Analysis (Includes Both Techniques Above) 18
Malware Defensive Measure 19
The DW and Emerging Criminal Threats 19
Trafficking in Human Beings and Sexual Services 19
Assassinations and Its Marketing 20
Terrorist and DW 21
Drug Transactions 21
Pornography Industry 21
Child Pornography 23
Methods and Challenges for Tracking Criminals on the DW 23
Summary 24

Chapter 2 A Guide to the Dark and Deep Web 25

The Beginning of the Internet 25
The Deep Web 26
The Dark Web 28
Criminals 29
Law Enforcement 29
Privacy 30
Journalism 31
Drugs and Illegal Substances 31
Counterfeit Goods 31
Stolen Information 33
Hackers 33
Summary 34

Chapter 3 Dark Web Access with Tor Browser 35

Tor Browser 35
Installing Tor on Linux 36
Tor Project Recommendation 39
The Mysterious Wiki 42

Chapter 4 The Dark Web's Perils 43

Online Scams 43
Avoiding the Risks of a Dark Web Market 46
The Dark Web's Perils 47
Access 48
Use and Misuse 49
The Truth about the Risks 49
Some General Dangers 49
Summary 51

Chapter 5 Cybercrime on the Dark Web 52

Categories of Cybercrime 52
Computer Fraud 52
Business Email Compromise 53
Data Infringe 53
Denial-of-Service 54
Malware 55
Email Account Compromise 55
Phishing 56
Ransomware 58
BadRabbit 60
Locky 60

NotPetya 60
Cyberterrorism 61
Cyberwarfare 63
Cyber Extortion 64
Using the Dark Web for Cybercrime 65
Drugs 65
Human Trafficking, Sex Trade, and Pornography 65
Weapons 66
Fake Documents 67
ATM PIN Pad Skimmers and ATM Malware 67
Counterfeit Currency 68
Data Dumps 68
Fake Websites 68
Exploit Kits 69
Data Exfiltration 69
Cybercrime Profitability 70
Extortion 71
Phishing 71
Adverts 72
Identity Theft by Using Login Information 72
Premium-Rate SMS 72
Banking Malware 73
Money Laundering and Malware-as-a-Service 73
Exploit Writers 74
Bot Herders 74
Malware Writers 74
Money Laundering 74
Summary 75

Chapter 6 Red Room Deep Web 77

What Is the Red Room Deep Web? 78
What Is Available on the Red Room Deep Web? 79
Child Pornography 79
Murder 79
Rape 79
General Torture 79
Chat 80
How to Join the Red Room Deep Web? 80
Red Room Deep Web Pricing Plans
and Payment Methods 80
Is Accessing Red Room Deep Web Illegal? 81
Why Is the Red Room Considered Non-Existent? 81
Deep Web Links to Access the Red Room 83

Chapter 7 Terrorist Acts on the Surface and Dark Web 84

Introduction 84
Terrorists' Online Activities 84
Propaganda 85
Propaganda and Social Media 86
Propaganda and the Dark Web 86
Content of Propaganda 86
Rhetorical Structures of Terrorist Websites 86
Crime as a Service 87
Communications 87
Dark Web and Encrypted Communication 88
Mail2Tor 91
Signal 91
Telegram 91
Surespot 92
Wickr 93
Zello 93
WhatsApp 94
Kik 94
Steganography, Internet Memes, and Watermarking 95
TerroristCrypt 95
Video Games 95
Email Dead Dropping 96
Cybersecurity in Voice Communication 96
Terrorist Media 96
Social Media and Surface Web 96
Twitter 96
YouTube 98
Facebook 98
Pinterest 98
Tumblr 98
Instagram 98
Ask.fm 98
Online Terrorist Recruitment 98
Surface Web 99
Social Media 99
Websites and Chat Rooms on the Internet 99
Video Games 99
Covert Recruitment and Training 100
Cyberterrorism 100
Concluding Remarks 101

Chapter 8 Dark Web Markets 102

Introduction 102

Dark Net Black Markets 102
Characteristics and Features 102
Goods and Services 103
Multisignature or Trusted Markets 104
Escrow Markets 104
'Finish Early' Markets 104
Invite/Referral Markets 104
Charges, Transactions, and Payments 105
Cryptocurrencies 105
Comparing Cryptocurrencies and Fiat Currencies 105
Cryptocurrencies and Digital Currencies Differences 106
How to Obtain Cryptocurrencies 106
Mining 106
Trading/Exchanging 107
Popular Cryptocurrencies 108
Bitcoin 108
Ethereum 108
Litecoin 109
Monero 109
Dash/Darkcoin 110
Active Markets 110
Wall Street Market 111
Dream Market 112
Nightmare Market 112
Empire Market 112
Point/T•chka Free Market 112
Silk Road 3.1 112
Cannabis Growers and Merchants Cooperative (CGMC) 113
Berlusconi Market 113
The Majestic Garden 113
Hydra 113
WayAway 114
RuTor 114
Cannazon 114
Active Vendor Shops 114
CharlieUK 114
DutchDrugz21 114
RechardSport 115
ElHerbolario 115
Gammagoblin-Pushing Taboo 115
The Church-Jesus of Rave (JOR) 115
ToYouTeam 115
The French Connection 115
EU Cocaine 115
GlassWerkz 115

Cocaine Market 115
ChemSpain 116
MaghrebHashish 116
Vendors and Markets That Are Full of Dead or Scammed People 116
AlphaBay 116
Agora 116
Evolution 116
Hansa Market 116
Outlaw Market 117
Aero Market 117
Libertas Market 117
TheRealDeal Market 117
Mercado Negro 117
Valhalla (Silkkitie) 118
Apple Market 118
Your Drug 118
Stoned 100 118
QualityKing 119
Fight Club 119
L33TER 119
Agora Market and Forum 119
Atlantis 119
Caravan Marketplace 120
Darknet Heroes League 120
The RealDeal Market 120
Sheep Marketplace 120
Russian Anonymous Marketplace 121
UK Guns and Ammo 121
USA/EU Fake Document Store 121
The Dark Web is a Market for Illegal Goods and Services 121
Drugs 121
Weapons 121
Communication Channels for Terrorists 122
Hacking 122
Assassinations 122
Fraud 123
Fake IDs/Driving Licenses 124
Illegal Wildlife Trade 124
Child Porn 124
Malware for Sale 125
Botnets 125
BTC Laundry 126
Information about Government and Celebrity Officials' Secrets is Being Leaked 127

BTC and Cryptocurrency Fraud 127
Terrorism 128
Policing the Dark Markets 129
Expectations Over the Next Five Years 129

Chapter 9 We Are Anonymous: We Do Not Forget We Do Not Forgive 130
Project Chanology 131
Operation Payback 131
Operation Tunisia 134
OpEgypt 136
The HBGary Hack 137
OpBART 138
Occupy Wall Street 139

Chapter 10 Hitman for Hire 141
The Con Artist of the Besa Mafia 141
Russia's Top Female Anticorruption Investigator was Shot and Killed in the Street 148
Sinaloa Cartel Hitman 150
Dark Mambia 150
Criminal Network 150
The Black Mob 152
Mara Salvatrucha 153
Assassination Network 153
Hitman from Murder Incorporated 155
Summary 155

Chapter 11 The Positive and Evil Side of the Dark Web 156
Onion Websites 157
Dark Web Black Market Transactions Involving the Use of Bitcoin 165

Chapter 12 Techniques for Analyzing Dark Web Content 167
Introduction 167
Deep Web versus Surface Web 167
Mechanisms of Conventional Web Crawlers 168
Surfacing Deep Web Content 169
Data Extraction 169
Schema Matching for Sources 170
Data Selection 170
Deep Web Websites Analysis 170

A Deep Web Website Search Analysis's Eligibility 170
The Number of Deep Web Websites: An Analysis 171
Deep Web Size Analysis 172
Analyze the Types of Content 173
Analyze the Popularity of the Website 173
Log Analysis 174
Summary 176

Chapter 13 Information Extraction from Dark Web Contents and Logs 178
Introduction 178
Examining Web Content and Logs 178
Web Content Analysis 179
Benefits of Content Analysis 180
Policy Guidelines for Log Analysis 182
Risk Assessment 182
Risk Assessment and Mitigation Duties and Responsibilities 183
Risk Mitigation 184
Web Content Logs Are the Responsibility of the Person in Charge of Them 185
Log Analysis Tools 185
Using the Hadoop Framework Has Many Benefits 187
Analyzing Files 187
Unstructured Data Analysis and Information Extraction 189
Summary 191

Chapter 14 Dark Web Forensics 192
Introduction 192
The Basics of Forensic 192
The Dark Web's Crypto Market and Cryptocurrencies 194
Money Laundering and Cryptocurrencies 196
ATMs for Bitcoin 198
Bitcoin Mixers 198
Monero 198
Bitcoin Property Exchanges 199
Schemes for Laundering Cryptocurrency Exposed 199
Bitcoin-Laundering Arrests 199
BTC-e 200
Models and Scope of Forensic Investigations 201
Scope 202
Policy and Procedure Making 202
Evidence Assessment 203

Evidence Acquisition 203
Examination of Evidence 204
Documentation and Reporting 205
Models for Digital Forensics 205
Digital Forensics Model (Abstract) 206
Investigative Model for Digital Forensics 206
Process of Integrated Digital Investigation 207
Forensic Toolkit 208
Anti-Forensics Analysis 210
Search Engine Characteristics 210
Detection of Virtual Machines and Sandboxes 210
Summary 211

Chapter 15 OsInt Opensource Intelligence 212

Introduction 212
Open-Source Intelligence 212
Security Intelligence and Its Challenges 213
Dark Web Security Intelligence Companies 214
Cybercrime-as-a-Service 214
Increasing the Return on Investment (ROI) for Cyber Weapons on the Dark Web 215
Intelligence-Gathering Focus 215
Hacking-as-a-Service 215
Stolen Intellectual Property 215
For Sale: Exploits 216
Vulnerabilities for Sale 216
Stolen Financial Data 217
Campaigns for Spam and Phishing 218
Threat Intelligence on the Dark Web and Its Value 218
Security Intelligence's Challenges 218
Monitoring Tools for Open-Source Intelligence 219
Recon-Ng 219
Maltego 220
The Harvester 221
Shodan 222
Google Dorks 223
Data Gathering 225
Direct Conversations 225
Chat Rooms 226
Advanced Search Queries 226
Market Listings 227
The Difficulties of Collecting Data from the Dark Web 227
Summary 229

Chapter 16 Emerging Dark Web Trends and Mitigation Techniques 230

Introduction 230
Recent Dark Web Evolution 230
Enhanced Security, Privacy, and Usability 230
Improvements in User Interface Design 232
Trust-Based Markets 233
Continuity 234
Crime Patterns 236
Terrorism on the Dark Web 236
Money Laundering via Cryptocurrencies 237
Botnets for Hire Are Increasingly Popular 239
Growth of Hacking-as-a-Service 239
Increased Malware for Sale Listings 240
The Black Market for Ivory and Rhino Horn 240
Preferred Cryptocurrencies 241
Stolen Data Listings for Sale 241
Threat Mapping 242
Fortinet 242
Norse 243
Checkpoint 243
FireEye 244
Arbor Networks 244
Threat Map by Kaspersky 245
Akamai 247
Trend Micro 247
Cutting-Edge Mitigation Techniques 247
Network Investigation Techniques 248
Memex 248
Some Conventional Techniques 249
Informants 249
Operation Undercover 249
Individuals' Tracking 250
Postal Interception 250
Cyber Patrols 251
Disruptions in Darknet Trade 252
Summary 254

Chapter 17 The Dark Web's Future 255

What Does the Deep Web's Future Hold for Us? 255
Dark Web Currency 256
The Tor Project 256
Dark Web Markets 258
ZeroNet 261

Public Interest in the Dark Web 262
Summary 264

Chapter 18 Your Business on the Dark Web 265

Business Companies 265
IT Professionals 267
Law Enforcement Agencies 270
Cybersecurity Professionals 272
Military Organizations 272
Summary 272

Glossary 274

Bibliography 277

Index 280