
Contents

	Foreword	xiii
	Acknowledgments	xxxv
	Introduction	xxxv
Chapter 1	State of the Advanced Cyber Threat	1
	Have You Heard About the APT?	2
	APT Defined	2
	What Makes a Threat Advanced and Persistent?	3
	Examples of Advanced and Persistent Threats	7
	Moonlight Maze	8
	Stakkato	9
	Titan Rain	10
	Stormworm	11
	GhostNet	12
	Byzantine Hades/Foothold/Candor/Raptor	13
	Operation Aurora	14
	Stuxnet	15
	Russian Business Network	16
	New Generation of Botnets and Operators	18
	Operation Payback	19
	Conclusion	20
Chapter 2	What Is Deception?	23
	How Does Deception Fit in Countering Cyber Threats?	24
	Six Principles of Deception	25
	Focus	25
	Objective	26
	Centralized Planning and Control	26
	Security	26

Timeliness	27
Integration	27
Traditional Deception	28
Feints — Cowpens	28
Demonstrations — Dorchester Heights	30
Ruses — Operation Mincemeat (the Unlikely Story of Glyndwr Michael)	30
Displays — A Big Hack Attack	31
Why Use Deception?	35
The First US Army Group Deception	37
Russian Maskirovka	39
Deception Maxims	40
“Magruder’s Principle” — Exploitation of a COG’s Perception or Bias	40
“Limitations to Human Information Processing”	41
“Multiple Forms of Surprise”	42
“Jones’ Dilemma”	42
“Choice of Types of Deception”	42
“Husbanding of Deception Assets”	43
“Sequencing Rule”	43
“Importance of Feedback”	43
“Beware of Possible Unwanted Reactions”	43
“Care in the Design of Planned Placement of Deceptive Material”	44
Understanding the Information Picture	44
Half-Empty Version	45
Half-Full Version	46
A Question of Bias	46
Totally Full Version	48
Step-Beyond Version	48
Two-Steps-Beyond Version	49
Conclusion	49
Chapter 3	
Cyber Counterintelligence	51
Fundamental Competencies	52
Applying Counterintelligence to the Cyber Realm	63
Sizing Up Advanced and Persistent Threats	64
Attack Origination Points	65
Numbers Involved in the Attack	67
Risk Tolerance	68

	Timeliness	69
	Skills and Methods	70
	Actions	72
	Objectives	73
	Resources	74
	Knowledge Source	75
	Conclusion	84
Chapter 4	Profiling Fundamentals	85
	A Brief History of Traditional Criminal Profiling	87
	The Emergence of Cyber Profiling	90
	Acquiring an Understanding of the Special Population	92
	The Objectives of Profiling	97
	The Nature of Profiling	98
	Basic Types of Profiling	100
	Two Logical Approaches to Profiling: Inductive vs. Deductive	103
	Information Vectors for Profiling	104
	Time	104
	Geolocation	106
	Skill	108
	Motivation	109
	Weapons and Tactics	111
	Socially Meaningful Communications and Connections	113
	Conclusion	117
	References	117
Chapter 5	Actionable Legal Knowledge for the Security Professional	121
	How to Work with a Lawyer	123
	What You Should Know About Legal Research	125
	Online Legal Resources	126
	Common Legal Terms	129
	The Role of Statutes in Our Legal System	131
	How to Find a Law	131
	Do Your Background Homework	132
	Reading the Law	133
	Communicating with Lawyers	134
	Ethics in Cyberspace	134
	Conclusion	136

Chapter 6	Threat (Attacker) Tradecraft	137
	Threat Categories	138
	Targeted Attacks	140
	Opportunistic Attacks	143
	Opportunistic Turning Targeted	147
	Evolution of Vectors	148
	Meet the Team	152
	Criminal Tools and Techniques	154
	Tailored Valid Services	154
	Academic Research Abuse	159
	Circles of Trust	161
	Injection Vectors	164
	Conclusion	170
Chapter 7	Operational Deception	171
	Deception Is Essential	173
	Tall Tale 1	177
	Postmortem	180
	Tall Tale 2	183
	Postmortem	187
	Tall Tale 3	187
	Postmortem	191
	Tall Tale 4	192
	Honeypot 1	193
	Postmortem	197
	Conclusion	198
Chapter 8	Tools and Tactics	199
	Detection Technologies	201
	Host-Based Tools	202
	Antivirus Tools	203
	Digital Forensics	203
	Security Management Tools	204
	Network-Based Tools	205
	Firewalls	206
	Intrusion Detection/Prevention Systems	207

Deception Technologies	207
Honeywalls	209
Honeynets as Part of Defense-in-Depth	220
Research vs. Production Honeynets	221
Honeynet Architectures	223
Honeywall Accreditation	225
Content Staging	226
Content Filling	229
Honeynet Training	230
Honeynet Objectives	230
Honeynet Risks and Issues	231
Check Yourself Before You're Wrecked	233
What's the Status of Your Physical Security?	234
How Does Your Wireless Network Look?	234
What's Traveling on Your Network?	236
What About Your Host/Server Security?	238
How Are Your Passwords?	241
How's Your Operational Security?	243
Crimeware/Analysis Detection Systems	245
What Happened on Your Box?	245
What Did That Malicious Software Do?	246
Conclusion	247
Chapter 9 Attack Characterization Techniques	249
Postincident Characterization	250
Another Tall Tale	252
Discovery	253
Malware	254
Aftermath	255
Real-World Tactics	256
Engaging an Active Threat	256
Traffic, Targets, and Taxonomy	265
Aftermath	278
Conclusion	279

10	Attack Attribution	281
	A Brief Note About Levels of Information Present in Objects	283
	Profiling Vectors	285
	Time	285
	Motivations	287
	Social Networks	298
	Skill Level	304
	Vector Summary	307
	Strategic Application of Profiling Techniques	308
	Example Study: The Changing Social Structure of the Hacking Community	308
	Micro- and Macro-Level Analyses	312
	The Rise of the Civilian Cyber Warrior	313
	The Balance of Power	314
	Potential Civilian Cyber Warrior Threats	316
	Conclusion	317
	References	318
11	The Value of APTs	321
	Espionage	322
	Costs of Cyber Espionage	323
	Value Network Analysis	324
	APTs and Value Networks	325
	The RSA Case	327
	The Operation Aurora Case	329
	APT Investments	333
	APTs and the Internet Value Chain	333
	It's All Good(s)	334
	Bitcoin in the Future?	335
	Conclusion	337
12	When and When Not to Act	339
	Determining Threat Severity	340
	Application Vulnerability Scenario	341
	Targeted Attack Scenario	341
	What to Do When It Hits the Fan	342
	Block or Monitor?	342
	Isolating the Problem	343
	Distinguishing Threat Objectives	344
	Responding to Actionable Intelligence	345

	Cyber Threat Acquisition	346
	Distinguishing Between Threats	346
	Processing Collected Intelligence	357
	Determining Available Engagement Tactics	358
	Engaging the Threat	359
	Within Your Enterprise	359
	External to Your Enterprise	360
	Working with Law Enforcement	361
	To Hack or Not to Hack (Back)	361
	To What End?	362
	Understanding Lines (Not to Cross)	363
	Conclusion	363
13	Implementation and Validation	365
	Vetting Your Operations	366
	Vetting Deceptions	369
	Vetting Perceptual Consistency in a Deception	370
	Vetting Engagements	372
	Putting This Book to Use with Aid from Professionals	375
	How to Evaluate Success	377
	Getting to the End Game	378
	Conclusion	390
	Glossary	393
	Index	403