

CONTENTS IN DETAIL

FOREWORD	xvii
ACKNOWLEDGMENTS	xix
INTRODUCTION	xxi
What You'll Find in This Book	xxiii
Who Should Read This Book?	xxiv
The Code and Malware Specimens	xxv
Development Environment	xxvi
Code Signing Requirements	xxvi
Entitlements	xxvii
Safely Analyzing Malware	xxvii
Additional Resources	xxix
Books	xxix
Websites	xxix

PART I: DATA COLLECTION **1**

1	
EXAMINING PROCESSES	3
Process Enumeration	4
Audit Tokens	5
Paths and Names	6
Identifying Hidden Files and Directories	6
Obtaining the Paths of Deleted Binaries	7
Validating Process Names	8
Process Arguments	9
Process Hierarchies	13
Finding the Parent	14
Returning the Process Responsible for Spawning Another	16
Retrieving Information with Application Services APIs	17
Environment Information	19
Code Signing	24
Loaded Libraries	24
Open Files	28
proc_pidinfo	29
lsof	30
Other Information	31
Execution State	32
Execution Architecture	32
Start Time	34
CPU Utilization	35
Conclusion	36

2		
PARSING BINARIES		39
Universal Binaries		39
Inspecting		40
Parsing		42
Mach-O Headers		50
Load Commands		53
Extracting Dependencies		54
Finding Dependency Paths		54
Analyzing Dependencies		56
Extracting Symbols		59
Detecting Packed Binaries		62
Dependencies and Symbols		63
Section and Segment Names		63
Entropy Calculations		67
Detecting Encrypted Binaries		70
Conclusion		71
3		
CODE SIGNING		75
The Importance of Code Signing in Malware Detection		76
Disk Images.		78
Manually Verifying Signatures		78
Extracting Code Signing Information		79
Extracting Notarization Information		82
Running the Tool		84
Packages		84
Reverse Engineering pkgutil		86
Accessing Framework Functions		88
Validating the Package		90
Checking Package Notarization		91
Running the Tool		92
On-Disk Applications and Executables		93
Running Processes		95
Detecting False Positives		96
Code Signing Error Codes		97
Conclusion		97
4		
NETWORK STATE AND STATISTICS		101
Host-Based vs. Network-Centric Collection.		102
Malicious Networking Activity		102
Capturing the Network State		105
Retrieving Process File Descriptors		106
Extracting Network Sockets		106
Obtaining Socket Details		107
Running the Tool		111
Enumerating Network Connections.		111
Linking to NetworkStatistics		113
Creating Network Statistic Managers		113

Defining Callback Logic	114
Starting Queries	115
Running the Tool	115
Conclusion	117

5 PERSISTENCE 119

Examples of Persistent Malware	120
Background Task Management	123
Examining the Subsystem	124
Dissecting sfltool	127
Writing a Background Task Management Database Parser	130
Finding the Database Path	130
Deserializing Background Task Management Files	131
Accessing Metadata	134
Identifying Malicious Items	135
Using DumpBTM in Your Own Code	136
Conclusion	137

PART II: SYSTEM MONITORING 139

6 LOG MONITORING 141

Exploring Log Information	142
The Unified Logging Subsystem	143
Manually Querying the log Utility	144
Reverse Engineering log APIs	145
Streaming Log Data	146
Extracting Log Object Properties	148
Determining Resource Consumption	151
Conclusion	152

7 NETWORK MONITORING 155

Obtaining Regular Snapshots	156
DNS Monitoring	157
Using the NetworkExtension Framework	159
Activating a System Extension	160
Enabling the Monitoring	161
Writing the Extension	162
Filter Data Providers	170
Enabling Filtering	170
Writing the Extension	171
Querying the Flow	173
Running the Monitor	174
Conclusion	176

8		
ENDPOINT SECURITY		179
The Endpoint Security Workflow		180
Events of Interest		182
Clients, Handler Blocks, and Event Handling		185
Creating a Process Monitor		190
Subscribing to Events		191
Extracting Process Objects		191
Extracting Process Information		192
Stopping the Client		199
File Monitoring		200
Conclusion		203

9		
MUTING AND AUTHORIZATION EVENTS		205
Muting		206
Mute Inversion		209
Beginning Mute Inversion		210
Monitoring Directory Access		211
Authorization Events		213
Creating a Client and Subscribing to Events		213
Meeting Message Deadlines		215
Checking Binary Origins		217
Blocking Background Task Management Bypasses		219
Building a File Protector		223
Conclusion		228

PART III: TOOL DEVELOPMENT 231

10		
PERSISTENCE ENUMERATOR		233
Tool Design		234
Command Line Options		235
Plug-ins		235
Persistent Item Types		238
Exploring the Plug-ins		240
Background Task Management		241
Browser Extension		242
Dynamic Library Insertion		246
Dynamic Library Proxying and Hijacking		249
Conclusion		252

11		
PERSISTENCE MONITOR		253
Entitlements		254
Applying for Endpoint Security Entitlements		254
Registering App IDs		254

Creating Provisioning Profiles	255
Enabling Entitlements in Xcode	255
Tool Design	257
Plug-ins	258
Background Task Management Events	261
XPC	265
Creating Listeners and Delegates	265
Extracting Audit Tokens	266
Extracting Code Signing Details	268
Setting Client Requirements	270
Enabling Remote Connections	271
Exposing Methods	272
Initiating Connections	274
Invoking Remote Methods	275
Conclusion	276

12

MIC AND WEBCAM MONITOR 279

Tool Design	280
Mic and Camera Enumeration	281
Audio Monitoring	282
Camera Monitoring	285
Device Connections and Disconnections	286
Responsible Process Identification	288
Triggering Scripts	291
Stopping	293
Conclusion	294

13

DNS MONITOR 297

Network Extension Deployment Prerequisites	298
Packaging the Extension	299
Tool Design	301
The App	301
The Extension	302
Interprocess Communication	303
Building and Dumping DNS Caches	304
Blocking DNS Traffic	307
Classifying Endpoints	310
Conclusion	311

14

CASE STUDIES 313

Shazam's Mic Access	313
DazzleSpy Detection	315
Exploit Detection	315
Persistence	317
Network Access	319

The 3CX Supply Chain Attack	319
File Monitoring	320
Network Monitoring	322
Process Monitoring	323
Capturing Self-Deletion	325
Detecting Exfiltration	326
Conclusion	327

INDEX **329**