

CONTENTS IN DETAIL

ABOUT THE AUTHOR	vii
ABOUT THE TECHNICAL REVIEWER	vii

ACKNOWLEDGMENTS	xvii
------------------------	-------------

INTRODUCTION	xix
---------------------	------------

The Web, the Deep Web, and the Dark Web	xx
Who This Book Is For	xxi
What Is in This Book.	xxi
Exercises.	xxiv

1

A VISIT TO THE DARK WEB **1**

Accessing the Dark Web.	2
Ensuring Good OPSEC	2
Browsing with Tor and Whonix.	3
Finding and Navigating to Dark Web Sites	6
The People	7
The Products	8
Data	9
Tools	10
Services.	11
The Payment	13
Securing Transactions	13
Buying vs. Renting.	13
The Stages of a Cyberattack	14
Malware Analysis Basics.	15
Best Practices for Handling Malware	16
Static Analysis	18
Dynamic Analysis	22
Conclusion	23

2

VULNERABILITIES, EXPLOITS, AND ACCESS **25**

Buying Access	26
Initial Access Brokers	26
Proofs of Concept and Exploits	27
Exploit Builders	30
Obtaining Credentials	32
Verifying Stolen Credentials with Checkers.	32
Guessing Credentials with Brute-Forcers.	33
Case Study: TMChecker's Corporate Access Verification	35

Leveraging Phishing Kits	38
Case Study: The Greatness Phishing Kit	42
Generating the Web Page Skeleton	43
Retrieving the Payload	45
Redirecting Logins to a Fake Page	47
Retooling	48
Conclusion	50
Exercise: Exploring Proofs of Concept for Log4Shell	50

3 MALWARE DELIVERY TECHNIQUES 53

Loaders.	54
Loaders for Sale	54
Analysis Challenges	55
Case Study: SmokeLoader’s Evasion Techniques	57
Checking for Debug-Related Flags	58
Obfuscating Control Flow	62
Case Study: BunnyLoader’s Core Functionality	62
String Obfuscation	63
File Download and Execution	67
Anti-Analysis Techniques	70
What Is a Botnet?	71
Botnet Access on the Dark Web	71
Infection and Communication	72
The Mirai Family	73
Setting Default Credentials	74
Contacting IP Addresses	74
Logging In	75
Case Study: The CosaNostra Botnet	77
Conclusion	79
Exercise: Reading Mirai’s Source Code	79

4 INFORMATION STEALERS 81

Harvesting Device Information	82
The Infostealer Process	85
Victim Download	86
Data Collection	88
Exfiltration	90
Case Study: Raccoon Stealer’s Information Collection	93
Strings	93
Browser Data	95
Autofill Passwords	97
Screenshots	98
Wallets	100
Installed Programs	101
System Information	102
Why Do Stealers Still Work?	104
Conclusion	105
Exercise: Analyzing SapphireStealer	105

5		
BANKING TROJANS		107
Banking Credential Theft		108
How Android Bankers Abuse the Accessibility API		110
Declaring Permissions in the Android Manifest		110
Using WebViews to Create Malicious Overlays		112
Case Study: Cerberus’s Application Overlays		113
Requesting Permissions for the Accessibility API		113
Defining Callbacks		113
Generating the WebView Overlay		115
Case Study: TrickBot’s Use of Windows Trojan Techniques		116
Process Injection		117
Function Hooking		119
RATs vs. Banking Trojans		123
Conclusion		123
Exercises		124
Designing a Secure Banking App		124
Uncovering Cerberus’s Other Functionality		125
6		
PACKERS AND CRYPTERS		127
Crypters in the Criminal Underground		128
Reverse Engineering Crypted or Packed Malware		133
Meaningless or Benign Strings		133
Nonsense Code		134
Entropy		136
Binary Structure		137
Case Study: A Packed Malware Sample		142
Stage 1: Memory Allocation		143
Stage 2: The Newly Allocated Memory		149
Stage 3: Final Payload Retrieval		154
Conclusion		157
Exercise: Packing and Analyzing Software		157
7		
COMMAND-AND-CONTROL FRAMEWORKS		161
Components of Command-and-Control Frameworks		162
The Framework Ecosystem		164
How Well-Known Tools Evade Detection		164
Tutorials Shared on the Dark Web		167
Cracked Software and Resold Licenses		168
Case Study: Comparing Vermilion Strike and Cobalt Strike		171
A Brief Introduction to Cobalt Strike		171
Configuration Data Decryption		172
String Deobfuscation		175
Victim Metadata Collection		176
Data Encryption and Exfiltration		177
Implant Tasking		178
Conclusion		180
Exercise: Investigating the Sliver Framework		180

8		
POST-EXPLOITATION TOOLKITS		183
Targeting Active Directory		184
Post-Exploitation on the Dark Web		186
Tutorials, Results, and Tips		186
Repackaged Open Source Tools		189
Case Study: Impacket's Utilities		190
Use by Threat Actors		191
NTLM Hash Retrieval with secretsdump		192
Command Execution with wmiexec		194
Remote Code Execution with psexec		199
Conclusion		205
Exercise: Exploring Metasploit's Post-Exploitation and Evasion Modules		206
9		
LIVING OFF THE LAND		209
Using Legitimate Tools to Evade Detection		210
Common Living-Off-the-Land Binaries		210
Malicious PowerShell Usage		210
How Ransomware Lives Off the Land		212
Identification of Network Resources		213
Active Directory Enumeration		215
Lateral Movement		218
Privilege Escalation		221
Data Exfiltration		222
Deployment		224
Case Study: Comparing StealBit to LOLBins		229
Configuration		229
Anti-Analysis Techniques		230
Function Imports		232
String Encryption		234
Self-Deletion and Hiding		235
File and Directory Traversal		237
Network and Exfiltration Functionality		238
Comparison to Living-Off-the-Land Techniques		240
Mitigations		240
Conclusion		241
Exercise: Running Living-Off-the-Land Binaries Yourself		241
10		
WINDOWS RANSOMWARE		243
A Brief History of Ransomware		244
The Rise of the Ransomware-as-a-Service Model		247
How Lockers Work		250
Generating Keys		250
Increasing the Encryption Speed		254
Escalating Privileges		255
Excluding Sensitive Locations		257
Whitelisting Files and Directories		257

Making Recovery Harder	258
Complicating Analysis	261
Case Study: Comparing Versions of REvil's Locker	263
The Early Version	263
The New and Improved Version	279
How Defenders Create Ransomware Decryptors	286
Conclusion	287
Exercise: Exploring Babuk's Leaked Source Code	287

11

LINUX AND ESXi RANSOMWARE 291

The Evolution of Linux and ESXi Threats	292
The ESXi Hypervisor	293
Advantages of Targeting Linux and ESXi	293
The Move to Go and Rust	294
Case Study: REvil's Linux and ESXi Locker	296
A Simpler Approach to Ransomware	296
Virtual Machine Shutdown	298
File Encryption	299
Information Collection	301
Case Study: ALPHV's Rust-Based Locker	304
Configuration and Strings	304
Whitelisted Directories	306
Stopping Processes and Services	307
Post-Encryption	308
Windows vs. Linux and ESXi Lockers	310
Other Linux Malware	310
Conclusion	311
Exercise: Uncovering Mistakes in ESXiArgs	312

12

LESSONS FROM THE UNDERGROUND ECONOMY 315

Threat Actor Habits	315
Reactive Development	316
Rebranding	316
Stealth vs. Ease of Use	317
The Use of Red Team Tools	317
The Reuse of Existing Code	317
Lowered Barriers to Entry	319
Future Developments in Cybersecurity	319
Reactions to Takedowns	319
Artificial Intelligence	320
Increased Automation	322
The Evolution of Ransomware	323
Conclusion	323

EXERCISE SOLUTIONS 325

INDEX 355