

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

What Is Malware?	xxii
What Is Malware Analysis?	xxv
Why Does Malware Use Evasion?	xxv
Why I Wrote This Book	xxvi
Who Should Read This Book	xxvi
How This Book Is Organized	xxvii
Malware Samples for This Book	xxviii

PART I: THE FUNDAMENTALS **1**

1	
WINDOWS FOUNDATIONAL CONCEPTS	3

Windows Architecture Overview	3
User and Kernel Modes	4
Processes and Threads	5
Objects and Handles	6
The Windows API	6
Process Internals	9
EPROCESS Structures	9
Process Environment Blocks	10
Thread Environment Blocks	10
Stacks and Heaps	11
Virtual Memory	11
The PE File Format	13
Headers and Sections	13
Imports and Exports	14
The Windows PE Loading Process	14
The Registry	16
Summary	17

2	
MALWARE TRIAGE AND BEHAVIORAL ANALYSIS	19

The Analysis Environment	20
The Malware Analysis Process	20
Initial Malware Triage	21
Identifying the File Type	22
Obtaining the File's Hash	23
Triaging with VirusTotal	24
Querying Search Engines and Other Resources	25

Identifying and Classifying Unknown Malware with Yara	26
Analyzing Static Properties	27
Automated Malware Triage with Sandboxes	31
Interactive Behavioral Analysis	36
Monitoring Malware Behaviors	37
Inspecting Malware Network Traffic	39
Summary	41

3

STATIC AND DYNAMIC CODE ANALYSIS **43**

Introduction to Assembly Code	44
CPU Registers	44
x64 and x86 Instructions	47
Static Code Analysis	51
Choosing a Disassembler	52
Analyzing with IDA	53
Analyzing with CAPA	56
Dynamic Code Analysis	58
Choosing a Debugger	58
Starting a Debugging Session in x64dbg	58
Analyzing with x64dbg	62
Patching and Modifying Code	68
Tracing API Calls with API Monitor	69
Summary	71

PART II: CONTEXT AWARENESS AND SANDBOX EVASION **73**

4

ENUMERATING OPERATING SYSTEM ARTIFACTS **75**

Processes	76
Directories and Files	78
Shared Folders	79
The Registry	80
Services	83
Installed Software	84
Mutexes	85
Pipes	86
Devices and Drivers	88
Usernames and Hostnames	90
Locale and Language Settings	90
Operating System Version Information	92
Summary	93

5

USER ENVIRONMENT AND INTERACTION DETECTION **95**

Browser Cookies, Cache, and Browsing History	96
Recent Office Files	97

User Files and Directories	98
Desktop Wallpaper	98
Desktop Windows	98
Mouse and Keyboard Interaction	100
System Uptime	101
Summary	102

6 ENUMERATING HARDWARE AND NETWORK CONFIGURATIONS 103

Hardware and Device Configurations	103
CPU	104
RAM	105
Hard Disks	105
Monitor Configurations	106
USB Controllers	107
Firmware Tables	107
Other Hardware Devices	108
Networking-Related Artifacts	109
IP Address Configurations	109
Domain Configurations	110
MAC Address Configurations	110
External IP Address and Internet Connectivity	112
TCP Connection States	114
Summary	115

7 RUNTIME ENVIRONMENT AND VIRTUAL PROCESSOR ANOMALIES 117

Detecting Analysis and Runtime Anomalies	117
Run Paths, Filenames, and Arguments	118
Loaded Modules	119
Anomalous Strings in Memory	120
Hooked Functions and Acceleration Checks	121
Using Performance and Timing Indicators	122
The rdtscl instruction	122
Function Execution Timing	123
Performance Counters	123
Abusing the Virtual Processor	123
The Red Pill and No Pill Techniques	123
IO Ports	124
The cpuid instruction	125
Unsupported Instruction Sets	125
The Trap Flag and Other Techniques	126
The Risks of Using Detection Techniques	127
Summary	127

8	EVADING SANDBOXES AND DISRUPTING ANALYSIS	129
Self-Termination		130
Delayed Execution		130
Sleep Function Calls		131
Timeouts		131
Time and Logic Bombs		132
Dummy Code and Infinite Loops		132
Forcing Reboots and Logouts		134
Decoys and Noise		134
API Hammering		135
Unnecessary Process Spawning		136
Decoy Network Communication		136
Anti-hooking		137
Hook Detection		138
Hook Removal (Unhooking)		139
Hook Circumvention		140
Anti-hooking Toolsets		143
Circumventing Sandbox Analysis		144
Disrupting Manual Investigation		144
Hypervisor Exploits and VM Escaping		146
Evasion Countermeasures		146
Summary		147

PART III: ANTI-REVERSING **149**

9	ANTI-DISASSEMBLY	151
Breaking Disassemblers		152
Control Flow Obfuscation		154
Unnecessary Jumps		154
Unnecessary Code		155
Control Flow Flattening		156
Opaque Predicates		157
Return Pointer Abuse		158
SEH Handler Abuse		158
Function Pointer Abuse		159
Control Flow Obfuscation Countermeasures		159
API Call and String Obfuscation		160
Dynamic API Function Resolution		161
Jump Tables and Indirect API Calls		161
Stack Strings		163
Data Hashing		164
Summary		165

10	ANTI-DEBUGGING	167
Using Windows API Functions to Access the PEB		167
IsDebuggerPresent and CheckRemoteDebuggerPresent		168
NtQueryInformationProcess		169
NtQuerySystemInformation		169
OutputDebugString		169
CloseHandle and NtClose		170
NtQueryObject		170
Heap Flags		170
Directly Accessing the PEB		171
Timing Checks		171
System Artifacts		172
Hunting for Debugger Windows		172
Enumerating Loaded Modules		173
Searching for Debugger Processes		173
Checking Parent Processes		173
Breakpoint Detection and Traps		174
Detecting Debuggers with Breakpoints		174
Detecting and Circumventing Software Breakpoints		174
Detecting and Circumventing Hardware and Memory Breakpoints		175
Using Memory Page Guards for Breakpoint Detection		177
Using Breakpoint Traps		177
Unhandled Exceptions		178
Checksums, Section Hashing, and Self-Healing		178
Exploiting, Crashing, and Interfering with the Debugger		179
Debug Blocking and Anti-attach Techniques		180
Other Anti-debugging Techniques		180
Countering Anti-debugging Techniques		181
Summary		183

11	COVERT CODE EXECUTION AND MISDIRECTION	185
Callback Functions		186
TLS Callbacks		186
Structured Exception Handling		189
VEH and 64-Bit SEH		192
Hidden Threads		193
Summary		194

PART IV: DEFENSE EVASION **195**

12	PROCESS INJECTION, MANIPULATION, AND HOOKING	197
Process Injection		198
Random vs. Specific Target Processes		198
Shellcode Injection		199

DLL Injection	203
Reflective DLL Injection	204
Process Hollowing	205
Thread Hijacking	207
APC Injection	207
Atom Bombing	209
Process Injection Wrap-up	209
Process Image Manipulation	210
Process Herpaderping	211
Process Doppelganging	212
Process Reimaging and Ghosting	214
DLL and Shim Hijacking	214
DLL Hijacking	214
Shim Hijacking	216
Hooking	218
SetWindowsHookEx Hooking and Injection	218
Inline Hooking	219
Mitigations for Process and Hook Injection	221
Summary	222

13

EVADING ENDPOINT AND NETWORK DEFENSES

223

An Endpoint Defense Primer	224
A Brief History of Endpoint Defense Technology	224
Anti-malware	225
Endpoint Detection and Response	227
Identifying Endpoint Defenses	232
Actively Circumventing Endpoint Defenses.	235
Disabling Host Defenses.	235
Adding Anti-malware Exclusions	236
Disabling Other Security Controls	237
Blinding Defenses by Unhooking.	238
Exploiting Vulnerabilities in Host Defense Tooling	238
Passively Circumventing Endpoint Defenses	239
Circumventing Monitoring	239
Circumventing Signature-Based Detection	243
Using Uncommon Programming Languages	244
Abusing Certificate Trust and Signing	245
Abusing Engine Limitations	246
Masquerading as a Safe File	247
Privilege Elevation for Defense Evasion	248
Bypassing User Account Control	248
Impersonating and Manipulating Access Tokens	253
Extracting and Reusing Credentials	254
Exploiting Vulnerabilities for Privilege Elevation.	255
Circumventing Network Defenses	256
Introducing Modern Network Defenses	256
Obfuscating and Obscuring Network Traffic.	257
Concealing Infrastructure Using Geofencing	259
Generating New Infrastructure Using DGAs	260
Executing the Fast-Flux Technique	261

Multistage and Complex Attacks	262
Summary	263

14
INTRODUCTION TO ROOTKITS **265**

Rootkit Fundamentals	266
Kernel Modules and Drivers	266
Rootkit Components	267
Rootkit Installation	269
BYOVD Attacks	271
Direct Kernel Object Manipulation	272
“Legacy” Kernel Hooking	274
SSDT Hooks	275
Inline Kernel Hooks	276
IRP Hooks	278
IRP Interception by Filtering	281
Abusing Kernel Callbacks	283
Bootkits	285
Defenses Against Rootkits	286
Summary	288

15
FILELESS, LIVING OFF THE LAND, AND
ANTI-FORENSICS TECHNIQUES **289**

How Fileless Attacks Work	290
Persistence and Registry-Resident Malware	292
Living Off The Land Binaries	294
VBA Macro-Based Malware	295
System Binary Proxy Execution	296
Windows Command Line and Other Utilities	300
PowerShell	302
Dynamically Compiled Code	304
Anti-forensics	306
Hiding Artifacts and Code	306
Tampering with Logs and Evidence	312
Destroying the System	316
Summary	317

16
ENCODING AND ENCRYPTION **319**

Basic Encoding	320
Data Hashing	323
Encryption and Decryption	325
Symmetric and Asymmetric Encryption	326
Windows CryptoAPI	332
Windows Cryptographic API: Next Generation	335
Practical Tips for Overcoming Encryption in Malware	336
Locating and Identifying Cryptographic Routines	336
Decrypting Encrypted Malware Data	339
Summary	343

17

PACKERS AND UNPACKING MALWARE **345**

Types of Packers	346
Packer Architecture and Functionality	347
Unpacking the Malware Payload	348
Resolving Imports	349
Transferring Execution to the OEP	350
How to Identify Packed Malware	350
Viewing Imports	350
Inspecting Strings	352
Calculating the Entropy Value	352
Checking PE Sections	353
Using Automated Packer Detection	353
Automated Unpacking	354
Fully Automated Unpacking	355
Sandbox-Assisted Unpacking	355
Manual Dynamic Unpacking	357
The Quick-and-Dirty Option: Letting the Malware Do the Work	357
Memory Operation Monitoring	359
Process Injection Monitoring	366
Process Injection Tracing with API Monitor	369
Library Loading and Address Resolution	370
OEP Location	371
Unpacked Malware Extraction	374
Unpacked Executable Repair	375
General Tips for Dynamic Unpacking	377
Helpful Tools for Dynamic Unpacking	379
Manual Static Unpacking	382
Analyzing Without Unpacking	383
Anti-unpacking Techniques	383
Summary	385
Closing Thoughts	385

A

BUILDING AN ANTI-EVASION ANALYSIS LAB **387**

Lab Architecture	388
The Host Machine	388
The Hypervisor	388
Victim Windows VMs	389
Services Windows VMs	389
Linux VMs	389
Building Your Lab	390
Choosing a Hypervisor	390
Verifying Hypervisor Network Settings	391
Obtaining a Windows Image	391
Creating the Windows Victim VM	392
Tuning VM Settings for Concealment and Isolation	394
Installing Windows Malware Analysis Tools	401
Installing VM Tools	402
Installing and Configuring a Linux VM	404

Manually Installing Linux VM Tools	405
Configuring and Verifying Network Settings	405
Taking and Restoring VM Snapshots	408
Windows Configurations for Concealment	409
Registry Data	409
Hostname and Domain Name	410
Additional Tips and Tricks	411
Advanced VM and Hypervisor Hardening	412
Hardening VMware	413
Hardening VirtualBox	414
Stress-Testing Your VM	415
Tips for Operational Security and Effectiveness	416
Simulating Network Services	416
Concealing Your IP	418
Shared Folders and File Transferring	418
Updating Software	419
Bare-Metal Analysis	419
Binary Instrumentation and Emulation	420
Summary	421

B
WINDOWS FUNCTIONS USED FOR EVASION **423**

C
FURTHER READING AND RESOURCES **435**

INDEX **439**