At a Glance

Part I Malware

1 Malware Propagation 7

2 Malware Functionality 41

Part II Rootkits

3 User-Mode Rootkits 77

4 Kernel-Mode Rootkits 109

5 Virtual Rootkits 161

6 The Future of Rootkits 187

Part III Prevention Technologies

7 Antivirus 203

8 Host Protection Systems 221

9 Host-Based Intrusion Prevention 233

10 Rootkit Detection 249

11 General Security Practices 289
Appendix System Integrity Analysis: Building Your Own Rootkit Detector 299

Index 337

Contents

Foreword xvii
Acknowledgments xix
Introduction xxi

Part I Malware

CASE STUDY: Please Review This Before Our Quarterly Meeting 2

1 **Malware Propagation** 7
Malware Is Still King 8
The Spread of Malware 8
Why They Want Your Workstation 8
Intent Is Hard to Detect 9
It's a Business 10
Significant Malware Propagation Techniques 10
  Social Engineering 11
  File Execution 13
Modern Malware Propagation Techniques 16
  StormWorm 16
  Metamorphism 19
  Obfuscation 20
  Dynamic Domain Name Services 24
  Fast Flux 24
Malware Propagation Injection Vectors 26
  Email 26
  Malicious Websites 29
  Phishing 32
  Peer-to-Peer (P2P) 35
  Worms 38
Summary 40

2 Malware Functionality 41
What Malware Does Once It's Installed 42
Pop-ups 42
Search Engine Redirection 46
Data Theft 53
Click Fraud 54
Identity Theft 57
Keylogging 61
Malware Behaviors 65
Identifying Installed Malware 68
Typical Install Locations 68
Installing on Local Drives 69
Modifying Timestamps 69
Affecting Processes 69
Disabling Services 70
Modifying the Windows Registry 70
Summary 71

Part II Rootkits

CASE STUDY: The Invisible Rootkit That Steals Your Bank Account Data 74
Disk Access 75
Firewall Bypassing 75
Backdoor Communication 75
Intent 76
Presence and Significance 76

3 User-Mode Rootkits 77
Rootkits 79
Timeline 80
Major Features of Rootkits 81
Types of Rootkits 83
User-Mode Rootkits 83
What Are User-Mode Rootkits? 83
Background Technologies 84
Injection Techniques 87
Hooking Techniques 98
User-Mode Rootkit Examples 100
Summary 108

4 Kernel-Mode Rootkits 109
Ground Level: x86 Architecture Basics 110
Instruction Set Architectures and the Operating System 111
Protection Rings 112

Bridging the Rings 113
Kernel Mode: The Digital Wild West 113
The Target: Windows Kernel Components 114
The Win32 Subsystem 114
What Are These APIs Anyway? 116
The Concierge: NTDLL.DLL 116
Functionality by Committee: The Windows Executive (NTOSKRNL.EXE) 117
The Windows Kernel (NTOSKRNL.EXE) 117
Device Drivers 118
The Windows Hardware Abstraction Layer (HAL) 118
Kernel Driver Concepts 119
Kernel-Mode Driver Architecture 119
Gross Anatomy: A Skeleton Driver 121
WDF, KMDF, and UMDF 122
Kernel-Mode Rootkits 122
What Are Kernel-Mode Rootkits? 123
Challenges Faced by Kernel-Mode Rootkits 123
Methods and Techniques 126
Kernel-Mode Rootkit Samples 145
Klog by Clandestiny 145
AFX by Aphex 148
FU and FUTo by Jamie Butler, Peter Silberman, and C.H.A.O.S 151
Shadow Walker by Sherri Sparks and Jamie Butler 152
He4Hook by He4 Team 155
Sebek by The Honeynet Project 158
Summary 159
Summary of Countermeasures 159

5 Virtual Rootkits 161
Overview of Virtual Machine Technology 162
Types of Virtual Machines 163
The Hypervisor 164
Virtualization Strategies 166
Virtual Memory Management 166
Virtual Machine Isolation 167
Virtual Machine Rootkit Techniques 167
Rootkits in the Matrix: How Did We Get Here?! 167
What Is a Virtual Rootkit? 168
Types of Virtual Rootkits 169
Detecting the Virtual Environment 170
Escaping the Virtual Environment 177
Hijacking the Hypervisor 178
Virtual Rootkit Samples 179
Summary 185

6 The Future of Rootkits 187
Increases in Complexity and Stealth 188
Custom Rootkits 195
Digitally Signed Rootkits 196
Summary 196

Part III Prevention Technologies

CASE STUDY: A Wolf in Sheep's Clothing 200
Scareware 200
Fakeware 200
Look of Authenticity 200
Countermeasures 201

7 Antivirus 203
Now and Then: The Evolution of Antivirus Technology 204
The Virus Landscape 205
Definition of a Virus 205
Classification 206
Simple Viruses 208
Complex Viruses 210
Antivirus—Core Features and Techniques 212
Manual or "On-Demand" Scanning 212
Real-Time or "On-Access" Scanning 212
Signature-Based Detection 213
Anomaly/Heuristic-Based Detection 214
A Critical Look at the Role of Antivirus Technology 215
Where Antivirus Excels 216
Top Performers in the Antivirus Industry 216
Challenges for Antivirus 216
The Future of the Antivirus Industry 219
Summary and Countermeasures 219

8 Host Protection Systems 221
Personal Firewall Capabilities 222
Personal Firewall Limitations 223
Pop-Up Blockers 225
Chrome 225
Firefox 226
Microsoft Edge 226
Safari 226
Example Generic Pop-Up Blocker Code 228
Summary 231

9 Host-Based Intrusion Prevention **233**
HIPS Architectures 234
Growing Past Intrusion Detection 237
Behavioral vs. Signature 238
Behavioral Based 239
Signature Based 240
Anti-Detection Evasion Techniques 241
How Do You Detect Intent? 245
HIPS and the Future of Security 246
Summary 247

10 Rootkit Detection **249**
The Rootkit Author's Paradox 250
A Quick History 251
Details on Detection Methods 254
System Service Descriptor Table Hooking 254
IRP Hooking 255
Inline Hooking 256
Interrupt Descriptor Table Hooks 256
Direct Kernel Object Manipulation 256
IAT Hooking 256
Legacy DOS or Direct Disk Access Hooking 257
Windows Anti-Rootkit Features 257
Software-Based Rootkit Detection 258
Live Detection vs. Offline Detection 259
System Virginity Verifier 260
IceSword and DarkSpy 261
RootkitRevealer 262
F-Secure's BlackLight Technology 264
Rootkit Unhooker 265
GMER 266
Helios and Helios Lite 268
McAfee Rootkit Detective and RootkitRemover 271
TDSSKiller 272
Bitdefender Rootkit Remover 274
Trend Micro Rootkit Buster 275
Malwarebytes Anti-Rootkit 275
Avast aswMBR 275
Commercial Rootkit Detection Tools 276
Offline Detection Using Memory Analysis: The Evolution ofMemory Forensics 277
Virtual Rootkit Detection 285
Hardware-Based Rootkit Detection 286
Summary 287

11 General Security Practices 289
End-User Education 290
Security Awareness Training Programs 290
Defense-in-Depth 293
System Hardening 295
Automatic Updates 295
Virtualization 296
Baked-In Security (from the Beginning) 297
Summary 297

Appendix System Integrity Analysis: Building Your Own Rootkit Detector 299
What Is System Integrity Analysis? 301
The Two *Ps* of Integrity Analysis 303
Pointer Validation: Detecting SSDT Hooks 305
Patch/Detour Detection in the SSDT 310
The Two *Ps* for Detecting IRP Hooks 323
The Two *Ps* for Detecting IAT Hooks 327
Our Third Technique: Detecting DKOM 327
Sample Rootkit Detection Utility 335

Index 337