

CONTENTS

| | |
|-----------------------|-----|
| Foreword | xv |
| Acknowledgments | xix |
| Introduction | xxi |

Part I Malware

| | |
|--|----|
| Case Study: Please Review This Before Our Quarterly Meeting | 2 |
| ▼ 1 Method of Infection | 7 |
| This Security Stuff Might Actually Work | 8 |
| Decrease in Operating System Vulnerabilities | 9 |
| Perimeter Security | 10 |
| Why They Want Your Workstation | 11 |
| Intent Is Hard to Detect | 12 |
| It's a Business | 13 |
| Significant Malware Propagation Techniques | 14 |
| Social Engineering | 15 |
| File Execution | 17 |
| Modern Malware Propagation Techniques | 21 |
| StormWorm (Malware Sample: trojan.peacomm) | 22 |
| Metamorphism (Malware Sample: W32.Evol, W32.Simile) | 24 |
| Obfuscation | 25 |
| Dynamic Domain Name Services (Malware Sample: W32.Reattle.E@mm) | 29 |
| Fast Flux (Malware Sample: trojan.peacomm) | 29 |
| Malware Propagation Injection Vectors | 31 |
| Email | 31 |
| Malicious Websites | 35 |
| Phishing | 37 |
| Peer-To-Peer (P2P) | 43 |
| Worms | 46 |

| | |
|---|----|
| Samples from the Companion Website | 47 |
| Summary | 48 |
| ▼ 2 Malware Functionality | 49 |
| What Malware Does Once It's Installed | 50 |
| Pop-Ups | 50 |
| Search Engine Redirection | 54 |
| Data Theft | 62 |
| Click Fraud | 63 |
| Identity Theft | 65 |
| Keylogging | 69 |
| Malware Behaviors | 73 |
| Identifying Installed Malware | 76 |
| Typical Install Locations | 76 |
| Installing on Local Drives | 77 |
| Modifying Timestamps | 77 |
| Affecting Processes | 77 |
| Disabling Services | 78 |
| Modifying the Windows Registry | 79 |
| Summary | 79 |

Part II Rootkits

| | |
|--|-----|
| Case Study: The Invisible Rootkit That Steals Your Bank Account Data ... | 82 |
| Disk Access | 83 |
| Firewall Bypassing | 83 |
| Backdoor Communication | 83 |
| Intent | 84 |
| ▼ 3 User-Mode Rootkits | 85 |
| Maintain Access | 86 |
| Network-Based Backdoors | 87 |
| Stealth: Conceal Existence | 87 |
| Types of Rootkits | 88 |
| Timeline | 89 |
| User-Mode Rootkits | 89 |
| What Are User-Mode Rootkits? | 91 |
| Background Technologies | 92 |
| Injection Techniques | 94 |
| Hooking Techniques | 106 |
| User-Mode Rootkit Examples | 107 |
| Summary | 117 |

| | | |
|-----|---|-----|
| ▼ 4 | Kernel-Mode Rootkits | 119 |
| | Ground Level: x86 Architecture Basics | 120 |
| | Instruction Set Architectures and the Operating System | 121 |
| | Protection Rings | 121 |
| | Bridging the Rings | 123 |
| | Kernel Mode: The Digital Wild West | 123 |
| | The Target: Windows Kernel Components | 124 |
| | The Win32 Subsystem | 124 |
| | What Are These APIs Anyway? | 126 |
| | The Concierge: NTDLL.DLL | 126 |
| | Functionality by Committee: The Windows Executive (NTOSKRNL.EXE) | 127 |
| | The Windows Kernel (NTOSKRNL.EXE) | 127 |
| | Device Drivers | 128 |
| | The Windows Hardware Abstraction Layer (HAL) | 128 |
| | Kernel Driver Concepts | 129 |
| | Kernel-Mode Driver Architecture | 129 |
| | Gross Anatomy: A Skeleton Driver | 131 |
| | WDF, KMDF, and UMDF | 132 |
| | Kernel-Mode Rootkits | 133 |
| | What Are Kernel-Mode Rootkits? | 133 |
| | Challenges Faced by Kernel-Mode Rootkits | 134 |
| | Getting Loaded | 134 |
| | Gaining Execution | 135 |
| | Communicating with User Mode | 135 |
| | Remaining Stealthy and Persistent | 136 |
| | Methods and Techniques | 136 |
| | Kernel-Mode Rootkit Samples | 156 |
| | Klog by Clandestiny | 156 |
| | AFX by Aphex | 160 |
| | FU and FUTO by Jamie Butler, Peter Silberman, and C.H.A.O.S | 162 |
| | Shadow Walker by Sherri Sparks and Jamie Butler | 164 |
| | He4Hook by He4 Team | 167 |
| | Sebek by The HoneyNet Project | 170 |
| | Summary | 171 |
| | Summary of Countermeasures | 171 |
| ▼ 5 | Virtual Rootkits | 173 |
| | Overview of Virtual Machine Technology | 174 |
| | Types of Virtual Machines | 174 |
| | The Hypervisor | 175 |
| | Virtualization Strategies | 178 |
| | Virtual Memory Management | 178 |
| | Virtual Machine Isolation | 179 |

| | |
|--|-----|
| Virtual Machine Rootkit Techniques | 179 |
| Rootkits in the Matrix: How Did We Get Here?! | 179 |
| What Is a Virtual Rootkit? | 180 |
| Types of Virtual Rootkits | 181 |
| Detecting the Virtual Environment | 182 |
| Escaping the Virtual Environment | 189 |
| Hijacking the Hypervisor | 190 |
| Virtual Rootkit Samples | 191 |
| Summary | 198 |
| ▼ 6 The Future of Rootkits: If You Think It's Bad Now... | 199 |
| Increases in Complexity and Stealth | 200 |
| Custom Rootkits | 207 |
| Summary | 208 |

Part III Prevention Technologies

| | |
|---|-----|
| Case Study: A Wolf in Sheep's Clothing | 210 |
| Rogue Software | 210 |
| Great Interface | 213 |
| They Work! Sometimes... | 213 |
| ▼ 7 Antivirus | 215 |
| Now and Then: The Evolution of Antivirus Technology | 216 |
| The Virus Landscape | 217 |
| Definition of a Virus | 218 |
| Classification | 218 |
| Simple Viruses | 220 |
| Complex Viruses | 222 |
| Antivirus—Core Features and Techniques | 224 |
| Manual or “On-Demand” Scanning | 224 |
| Real-Time or “On-Access” Scanning | 225 |
| Signature-Based Detection | 225 |
| Anomaly/Heuristic-Based Detection | 227 |
| A Critical Look at the Role of Antivirus Technology | 228 |
| Where Antivirus Excels | 228 |
| Top Performers in the Antivirus Industry | 229 |
| Challenges for Antivirus | 232 |
| Antivirus Exposed: Is Your Antivirus Product a Rootkit? | 238 |
| Patching System Services at Runtime | 239 |
| Hiding Threads from User Mode | 241 |
| A Bug? | 241 |
| The Future of the Antivirus Industry | 243 |
| Fighting for Survival | 243 |

| | | |
|------|---|-----|
| | Death of an Industry? | 244 |
| | Possible Antivirus Replacement Technologies | 245 |
| | Summary and Countermeasures | 247 |
| ▼ 8 | Host Protection Systems | 249 |
| | Personal Firewall Capabilities | 250 |
| | McAfee | 251 |
| | Symantec | 252 |
| | Checkpoint | 254 |
| | Personal Firewall Limitations | 255 |
| | Pop-Up Blockers | 258 |
| | Internet Explorer | 258 |
| | Firefox | 259 |
| | Opera | 259 |
| | Safari | 259 |
| | Chrome | 260 |
| | Example Generic Pop-Up Blocker Code | 261 |
| | Summary | 264 |
| ▼ 9 | Host-Based Intrusion Prevention | 267 |
| | HIPS Architectures | 268 |
| | Growing Past Intrusion Detection | 271 |
| | Behavioral vs. Signature | 272 |
| | Behavioral Based | 273 |
| | Signature Based | 274 |
| | Anti-Detection Evasion Techniques | 275 |
| | How Do You Detect Intent? | 279 |
| | HIPS and the Future of Security | 280 |
| | Summary | 281 |
| ▼ 10 | Rootkit Detection | 283 |
| | The Rootkit Author's Paradox | 284 |
| | A Quick History | 285 |
| | Details on Detection Methods | 288 |
| | System Service Descriptor Table Hooking | 288 |
| | IRP Hooking | 289 |
| | Inline Hooking | 290 |
| | Interrupt Descriptor Table Hooks | 290 |
| | Direct Kernel Object Manipulation | 290 |
| | IAT Hooking | 290 |
| | Windows Anti-Rootkit Features | 291 |
| | Software-Based Rootkit Detection | 292 |
| | Live Detection vs. Offline Detection | 293 |
| | System Virginty Verifier | 293 |
| | IceSword and DarkSpy | 295 |

| | | |
|------|---|-----|
| | RootkitRevealer | 297 |
| | F-Secure's Blacklight | 297 |
| | Rootkit Unhooker | 298 |
| | GEMER | 301 |
| | Helios and Helios Lite | 302 |
| | McAfee Rootkit Detective | 305 |
| | Commercial Rootkit Detection Tools | 306 |
| | Offline Detection Using Memory Analysis: The Evolution of Memory Forensics | 307 |
| | Virtual Rootkit Detection | 316 |
| | Hardware-Based Rootkit Detection | 316 |
| | Summary | 317 |
| ▼ 11 | General Security Practices | 319 |
| | End-User Education | 320 |
| | Security Awareness Training Programs | 320 |
| | Defense in Depth | 323 |
| | System Hardening | 324 |
| | Automatic Updates | 325 |
| | Virtualization | 325 |
| | Baked-In Security (from the Beginning) | 326 |
| | Summary | 327 |
| ▼ | Appendix System Integrity Analysis: Building Your Own Rootkit Detector | 329 |
| | What Is System Integrity Analysis? | 331 |
| | The Two <i>Ps</i> of Integrity Analysis | 333 |
| | Pointer Validation: Detecting SSDT Hooks | 335 |
| | Patch/Detour Detection in the SSDT | 340 |
| | The Two <i>Ps</i> for Detecting IRP Hooks | 353 |
| | The Two <i>Ps</i> for Detecting IAT Hooks | 358 |
| | Our Third Technique: Detecting DKOM | 358 |
| | Sample Rootkit Detection Utility | 366 |
| ▼ | Index | 367 |