Mobile Mal
Attacks and
Defense

Ken Dunham Technical Editor

Saeed Abu-Nimeh
Michael Becher
Seth Fogie
Brian Hernacki
Jose Andre Morales
Craig Wright

Contents

Chapter 1 Introduction to Mobile Malware . . . 1
Introduction . . . 2
Understanding Why Mobile Malware Matters Today . . . 3
An Introduction to MM Threats . . . 6
An Introduction to Mobile Security Terminology . . . 9
Vectors for Spreading MM . . . 9
Bluetooth . . . 10
MMC . . . 10
Multimedia Messaging Service (MMS) . . . 10
HTTP . . . 10
SMS . . . 10
Attack Types . . . 11
Hacking Defaults . . . 11
Denial-of-Service (DoS) . . . 11
Exploit . . . 11
Bloover/II . . . 11
Bluebug . . . 11
BlueBump . . . 11
BlueChop . . . 11
BlueDump . . . 12
Bluejacking . . . 12
Blueprinting . . . 12
BlueSmack . . . 12
Bluesnarf/++ . . . 12
BlueSniff . . . 12
Bluetooone . . . 12
CarWhispherer . . . 12
HeloMoto . . . 13
RedFang . . . 13
Snarf . . . 13
Warnibbling . . . 13
MM Terms . . . 13
Ad/Spyware . . . 13
Mobile Malware . . . 13

Payload . . . 14
Rogue Software . . . 14
Trojan . . . 14
Virus . . . 14
Worm . . . 14
Summary . . . 15
Solutions Fast Track . . . 15
Frequently Asked Questions . . . 17

Chapter 2 Visual Payloads . . . 19
Introduction . . . 20
F-Secure RF Lab . . . 20
Identifying Visual Payloads of MM . . . 23
Cabir . . . 23
Skulls . . . 25
CommonWarrior . . . 29
BlankFont . . . 32
Summary . . . 33
Solutions Fast Track . . . 33
Frequently Asked Questions . . . 34

Chapter 3 Timeline of Mobile Malware, Hoaxes, and Threats . . . 35
Introduction . . . 36
Qualifying Fear, Uncertainty, and Doubt (FUD) in the Mobile Market . . . 36
Global Demand for Mobile Devices . . . 37
An Historical Timeline of MM . . . 38
Genesis (2004) . . . 55
Telefonica . . . 55
Epoc.Fake.A . . . 55
Hacktool.SMSDOS . . . 56
Worm.SymbOS.Cabir.A . . . 56
Virus.WinCE.Duts . . . 57
Backdoor.WinCE.Brador . . . 57
Trojan.Skulls.A . . . 57
Middle Ages (2005) . . . 58
Trojan.SymbOS.Cardtrap . . . 58
Trojan.SymbOS.PbStealer . . . 59
Industrial Era (2006-2007) . . . 59
Trojan.SMSJ2ME.RedBrowser . . . 59

Worm.MSIL.Cxover . . . 60
Trojan-Spy.SymbOS.Flexispy . . . 61
Worm.SymbOS.Mobler.A . . . 61
SymbOS.Viver.A . . . 62
Modern Times and Beyond (2008 -) . . . 62
Trojan.iPhone.A . . . 62
WinCE.InfoJack.A . . . 63
Trojan.POC.MM.Gotcha.A . . . 63
Worm.POC.MM.Stranger.A . . . 64
Future Threats . . . 64
Summary . . . 67
Solutions Fast Track . . . 67
Frequently Asked Questions . . . 69
Notes . . . 70

Chapter 4 Overview of Mobile Malware Families . . . 71
Introduction . . . 72
Cabir . . . 72
Skuller . . . 78
Doomboot . . . 83
Cardtrap . . . 87
Summary . . . 90
Solutions Fast Track . . . 91
Frequently Asked Questions . . . 92

Chapter 5 Taxonomy of Mobile Malware . . . 93
Introduction . . . 94
Infection Strategy . . . 95
Wireless Communication . . . 95
MMS . . . 95
Bluetooth . . . 99
E-mail . . . 102
Wired Communication . . . 103
Removable Storage . . . 103
Device-to-PC (D2P) Synchronization . . . 105
Other Infection Strategies . . . 106
SMS . . . 106
Vi-Fi . . . 107
OS Vulnerabilities . . . 107

Distribution . . . 108
Wireless Communication . . . 109
SMS . . . 109
Bluetooth . . . 112
Wired Communication . . . 113
Removable Storage . . . 113
Payload . . . 114
Communications Component . . . 114
Sending SMS Messages: Nuisance . . . 115
File System . . . 115
Infecting Files: Nuisance . . . 115
Overwriting Files: Nuisance . . . 115
Multimedia Components . . . 116
Taking Photos: Devious . . . 116
Recording Voices: Devious . . . 116
Clandestine Video Recorder: Devious . . . 116
Playback: Devious . . . 117
Telephone Component . . . 117
Dialing Other Phone: Nuisance . . . 117
Dialing Your Own Phone: Nuisance . . . 117
Using the Phone to Cover Your Tracks: Devious . . . 118
Data Farming . . . 118
Stealing Contacts: Devious . . . 118
Summary . . . 121
Solutions Fast Track . . . 121
Frequently Asked Questions . . . 123

Chapter 6 Phishing, SMishing, and Vishing . . . 125
Introduction to Phishing andVishing . . . 126
Introduction to Phishing . . . 127
Phishing Mobile Devices . . . 130
Bluetooth Phishing . . . 131
SMS Phishing . . . 132
Voice over IP Phishing . . . 134
Breaking Phishing Filters via Pharming . . . 136
Introduction to Pharming . . . 137
Attack Details . . . 140
Attack Setup . . . 141
Hiding the Attack . . . 142
pf Firewall Rules . . . 143

Web Server vhost File . . . 143
The hosts.allow File . . . 143
Packet Capture Analysis . . . 144
The EarthLmk Toolbar . . . 144
The Netcraft Toolbar . . . 146
SpoofGuard . . . 148
The Google Toolbar . . . 150
Internet Explorer . . . 152
Firefox . . . 153
The Opera Browser . . . 154
SpoofStick . . . 156
Attack Prevention . . . 157
IP Verification . . . 158
OpenDNS . . . 158
SSL and HTTPS . . . 158
Virtual Private Networks . . . 158
Web Proxies . . . 158
Applying Machine Learning for Phishing Detection' . . . 159
Bayesian Additive Regression Trees . . . 160
Classification and Regression Trees . . . 161
Logistic Regression . . . 162
Neural Networks . . . 162
Random Forests . . . 163
Support Vector Machines . . . 163
Detecting Mobile Phishing Using a Distributed Framework . . . 164
Learning Phishing E-mails . . . 166
Data Standardization, Cleansing, and Transformation . . . 167
Textual Analysis . . . 170
Structural Analysis . . . 171
Experimental Studies . . . 174
Evaluation Metrics . . . 174
Experimental Setup . . . 175
Experimental Results . . . 176
Discussion . . . 179
An Introduction toVishing . . . 180
How Can I Spot a Vishing Attack? . . . 181
Understanding Vishers'Tools and Techniques . . . 182
VoIP Server . . . 183
VoIP Phone Management Software . . . 184
Interactive Voice Management (IVM) Software . . . 184

Text-To-Speech (TTS) and Interactive Voice Recording (IVR) . . . 186
Outbound Calling . . . 187
Vishing Packs . . . 187
Mitigating Vishing Attacks . . . 188
Consumer Education . . . 188
Notifications . . . 189
Summary . . . 190
Solutions Fast Track . . . 190
Frequently Asked Questions . . . 194
Notes . . . 196

Chapter 7 Operating System and Device Vulnerabilities . . . 197
Introduction . . . 198
Windows Mobile . . . 198
WM Details . . . 199
File System . . . 199
Xip . . . 199
Encryption . . . 199
Code Signing . . . 200
Operating System . . . 200
Kernel Mode vs. User Mode . . . 200
Drivers . . . 201
Memory/Process Limitation . . . 201
Vulnerability Details . . . 202
Core Operating System . . . 202
KDataStruct . . . 202
Pocket IE . . . 203
Active Sync . . . 204
Bluetooth . . . 205
PocketPC MMS-Based Vulnerabilities . . . 205
The MMS Client . . . 205
PocketPC MMS Composer . . . 206
Code Execution via SMIL . . . 206
SheUcode Walkthrough . . . 207
Denial-of-Service via WAP Push and Wi-Fi . . . 208
Attack Details . . . 209
Bypassing Code-Signing Protections . . . 210
Installing Your Own Certificate . . . 210

Registry Hack . . . 211
Buffer Overflow vs. Code Signing . . . 211
Exploiting WM . . . 212
The Tools . . . 212
IDA Pro . . . 212
Visual Studio 2005 . . . 213
WM Applications . . . 213
The Process . . . 213
An Example - FlexWallet . . . 214
Setup . . . 214
Initial Analysis and Target Selection . . . 215
Probe Target . . . 216
Analyze Crash . . . 217
Building the Exploit . . . 219
iPhone . . . 222
iPhone System Details . . . 222
Operating System . . . 222
Applications . . . 223
Open Source Tool Chain . . . 225
Exploiting the iPhone . . . 225
iPhone Hacking . . . 225
The Jailbreak Process . . . 225
Exploit Details . . . 227
A Flawed Shell Model . . . 228
Root Account . . . 228
Static Addressing . . . 228
Static Systems . . . 228
Reuse of Old Code . . . 228
Metasploit . . . 229
An iPhone Exploit in Action . . . 229
Metasploit vs. libtiff . . . 231
Tool Tip — Iphonedbg . . . 234
Symbian . . . 234
Symbian Details . . . 234
File System . . . 235
Operating System . . . 235
Security . . . 235
Platform Security . . . 235
Code Signing . . . 236

Vulnerability Landscape for Symbian . . . 237
Warezed Installers . . . 237
Social Engineering . . . 239
BlackBerry . . . 240
BlackBerry Details . . . 241
BlackBerry Vulnerabilities . . . 241
General Security Issues . . . 242
BlackBerry Enterprise Server Issues . . . 242
BBProxy . . . 242
J2ME -Java 2 Micro Edition . . . 245
MIDlets - J2ME Applications . . . 245
J2ME Security . . . 245
MIDlet Permissions and Signing . . . 246
Past Vulnerabilities . . . 246
Siemens S55 Permission Request Race Condition . . . 247
KVM Buffer Overflow Vulnerability . . . 247
Current Vulnerabilities . . . 247
The Nokia 6131 NFC Silent MIDlet Installation Vulnerability . . . 247
PushRegistry.Abuse on the Nokia 6131 NFC . . . 248
Other Notable Platforms . . . 248
Palm OS . . . 248
Palm OS Security . . . 249
The Palm OS Password Issue . . . 249
Palm OS Security Lock ByPass Vulnerabilities . . . 249
Palm OS Malware . . . 249
The LibertyCrack Trojan . . . 250
The Phage Virus . . . 250
The Vapor Trojan . . . 250
Linux . . . 250
Android . . . 250
Exploit Prevention . . . 252
WM-Defense . . . 252
iPhone Defense . . . 252
J2ME Defense . . . 252
Symbian Defense . . . 253
. Handheld Exploitation . . . 253
Wireless Attacks . . . 253
802. 11 Wardriving . . . 253
802.11 Jamming . . . 256

Mobile Bluetooth Attacks . . . 257
btCrawler . . . 257
btscanner/btaudit . . . 259
Silica . . . 259
Summary . . . 261
Solutions Fast Track . . . 261
Frequently Asked Questions . . . 263
Links . . . 263
Wm . . . 263
iPhone . . . 264
J2me . . . 264
Rim . . . 264
Symbian . . . 264
Palm . . . 265

Chapter 8 Analyzing Mobile Malware . . . 267
Introduction . . . 268
Learning about Dynamic Software Analysis . . . 268
Designing a Sandbox Solution . . . 268
General Design Considerations . . . 268
Components of MobileSandbox . . . 271
Prolog and Epilog . . . 271
Extracting Additional API Parameter Information . . . 273
DLL Injection . . . 273
Talking with the Host Computer . . . 274
Dereferencing Pointer Parameters . . . 274
Import Address Table Patching . . . 275
Environment . . . 275
Patching the Loaded Executable . . . 276
Kernel-Level Interception . . . 276
Environment . . . 276
Windows CE System Calls . . . 276
Protected Server Libraries . . . 277
Internal Kernel Data Structures . . . 279
Implementing Kernel-Level Interception . . . 279
Preventing Kernel Mode . . . 281
Pojting to Other Mobile Operating Systems . . . 282
Notes on Interception Completeness . . . 282
Interception . . . 282
Signature Recognition . . . 283

Using MobileSandbox . . . 283
Using the Local Interface . . . 283
Connecting the Device . . . 283
Choosing an Analysis Mode . . . 284
Using the Web Interface . . . 285
Analyzing within the Device Emulator . . . 286
Analyzing on a Real Device . . . 287
Reading an Analysis Report . . . 288
Analyzing Mobile Malware . . . 290
Duts . . . 290
Improving the Analysis . . . 291
Summary . . . 293
Solutions Fast Track . . . 293
Frequently Asked Questions . . . 294
Notes . . . 294

Chapter 9 Forensic Analysis of Mobile Malware . . . 295
Introduction . . . 296
Investigating Mobile Forensics . . . 296
The Components of a Mobile Device . . . 296
Investigative Methods of Mobile Forensics . . . 297
Step 1: Examination . . . 298
Step 2: Identification . . . 298
Step 3: Collection . . . 298
Step 4: Documentation . . . 299
Mobile Investigative Tips . . . 299
Device Switched On . . . 300
Device Switched Off . . . 300
Device in Its Cradle . . . 300
Device Not in Its Cradle . . . 301
Radio and Other Wireless Connections . . . 301
Expansion Card in Slot . . . 301
Expansion Sleeve Removed . . . 301
Deploying Mobile Forensic Tools . . . 302
PDA Secure . . . 302
PDA Seizure (Paraben) . . . 303
EnCase . . . 303
PalmDD (PDD) . . . 303
Autopsy and Open Source . . . 303
BitPim . . . 304

DataPilot Secure View . . . 304
Oxygen Forensic Suite . . . 304
PDA and Smartphone Forensics . . . 304
Hex Dumps of the Filesystem . . . 305
Special Hardware . . . 307
Operating Systems . . . 307
Symbian . . . 307
Microsoft . . . 308
Linux Variants . . . 308
Issues in Forensics . . . 308
Mobile Device Assets and MM Payloads . . . 308
Using the Mobile as a Listening Device . . . 309
Remotely Installing Software on Your SIM . . . 309
Intercepting Your Voice Calls . . . 309
Riscure GSM Hack . . . 309
Mobile Locate . . . 309
Performing BlackBerry Forensics . . . 310
BlackBerry Operating System . . . 310
BlackBerry Operation and Security . . . 310
Wireless Security . . . 310
Security for Stored Data . . . 310
Forensic Examination of a BlackBerry . . . 311
Acquisition of Information Considerations . . . 311
Device Is in the "Off" State . . . 311
Device Is in the "On" State . . . 311
Password Protected . . . 312
Evidence Collection . . . 312
Unit Control Functions . . . 312
Imaging and Profiling . . . 312
Attacking the BlackBerry . . . 313
Securing the BlackBerry . . . 313
Information Hiding in a BlackBerry . . . 313
The BlackBerry Signing Authority Tool . . . 313
Performing iPhone Forensics . . . 314
Misuse of an iPhone . . . 314
SQLite . . . 315
SMS Messages . . . 315
Voice Mail . . . 315
iPhone Investigation . . . 316
User Accounts . . . 316

Deleted Files . . . 317
iPhone Time Issues . . . 317
iPhone Tools . . . 317
Writing the Image to a Remote Machine
Using netcat . . . 317
iLiberty+ . . . 318
iPHUC . . . 318
Forensic Investigation of MM
on a Mobile Device . . . 318
Reproducibility of Evidence in the Case
of Dead Forensic Analysis . . . 319
Connectivity Options and Their Impact on Dead
and Live Forensic Analysis . . . 319
Operating Systems (OS) and File Systems (FS) . . . 320
Available Hardware . . . 320
Existing Forensic Tools and Toolkits . . . 321
Forensic Investigation of MM on a Mobile Device . . . 322
New Techniques to Extract Data . . . 322
Unsoldering Flash to Read It Externally . . . 324
EM Monitoring . . . 324
Summary . . . 325
Solutions Fast Track . . . 325
Frequently Asked Questions . . . 328
Notes . . . 329
References . . . 329

Chapter 10 Debugging and Disassembly of MMC . . . 331
Introduction . . . 332
Examining the General Analysis Process . . . 332
Preparing an Isolated Environment . . . 332
Collecting the Necessary Tools . . . 332
Performing a Static Analysis . . . 333
Dynamic Analysis . . . 334
Emulation . . . 334
Sandboxing . . . 335
Live Debugging . . . 335
Detailing the Analysis of FlexiSPY . . . 335
Wnat Is FlexiSPY . . . 336
Static Analysis of FlexiSPY . . . 336
Installer Analysis . . . 336

File Analysis . . . 337
Setting File Analysis . . . 338
Dynamic Analysis . . . 340
Sniffers and Proxies . . . 340
Debugging DLLs . . . 342
Monitoring API Calls . . . 344
Debugging Infojack . . . 345
Summary . . . 349
Solutions Fast Track . . . 349
Frequently Asked Questions . . . 351
Note . . . 351

Chapter 11 Mobile Malware Mitigation Measures . . . 353
Introduction . . . 354
Evaluating the Target . . . 354
The Value of the Device . . . 356
The Value of Information . . . 356
The Address Book . . . 357
Documents . . . 357
Activity History . . . 358
Application Data . . . 358
The Value of Access . . . 358
Impersonation . . . 358
Financial Access . . . 359
E-mail . . . 359
VPN . . . 359
Class of Threats . . . 359
Device Loss . . . 360
Network Attacks . . . 361
IP (EDGE/3G/etc) . . . 362
Browsing . . . 362
Discovery . . . 363
DoS . . . 363
Bluetooth . . . 364
MMS . . . 365
Local Attacks . . . 365
Defensive Measures . . . 366
Best Practices . . . 366
Policy . . . 366

Configuration . . . 367
Pass Codes and Locking . . . 368
Bluetooth . . . 368
Wi-Fi . . . 369
Caller ID . . . 370
Browser . . . 370
IR . . . 370
GPS/Location . . . 371
Basic Info . . . 371
Backup . . . 371
Audit . . . 372
Encryption . . . 372
Applications . . . 373
Updates . . . 373
Products . . . 373
Protective Defenses . . . 374
Bluetooth . . . 374
Anti-Virus . . . 375
Anti-Spam . . . 375
Mobile Security Packages . . . 375
Device/OS Vendor . . . 375
Symantec . . . 376
McAfee . . . 376
F-Secure . . . 376
Kaspersky . . . 376
Bluefire . . . 376
Eset . . . 376
Tracing Products . . . 377
Remote Management . . . 377
Remote Access . . . 378
Encryption . . . 378
Insurance . . . 378
Remediation . . . 378
Detection . . . 378
Device Loss . . . 379
Device Loss Reporting Procedure . . . 379
^Explicit Detection . . . 380
Vulnerability Warning . . . 380
Behaving Oddly . . . 380

Data Restore 380
Disablement 381
Summary 382
Solutions Fast Track 382
Frequently Asked Questions 384

Glossary 385

Index 401