Índice

Introducción 13

1. Para quién es este libro 13

2. Requisitos previos 13

3. Metodología de análisis 14

4. Contenido de una aplicación Android 16

5. AndroidManifest.xml 17

Permisos 18
Requisitos software y hardware 21
Componentes de una aplicación 22
Otras etiquetas en <application> 29

6. Código nativo 29

7. Instalación de aplicaciones 30

Market oficial 30
Orígenes desconocidos 31
Firma de aplicaciones 32
Resultado del proceso de instalación 33

Capítulo I
Preparando el entorno de análisis 35

1. Presentación de comandos 36

2. Configurando la máquina virtual Android 36

3. Configurando la máquina virtual de análisis 39

Preparativos en VirtualBox 39
Servicio DHCP 40
Enrutado de paquetes 41
Sniffing del tráfico de red 42
Automatizando el arranque del entorno 44
Android Studio, SDK y NDK 44

Repositorio de muestras y herramientas 49
Herramientas adicionales 49
Ajustes finales e interacción con Android 51
4. Gestión de instantáneas 53
5. Interacción con la máquina virtual Android 54
Instalación de muestras 54
Atajos 55

Capítulo II
Reuniendo información 57
1. Muestra de malware: Servicio SMS premium 57
2. Obteniendo el APK 59
3. Examinando el fichero AndroidManifest.xml 60
Métodos para obtener el AndroidManifest.xml 60
Interpretando la información 63
4. Analizando el contenido del APK 65
Datos del certificado 65
Ficheros almacenados en ***assets*** ***66***
Ficheros de recursos almacenados en res 67
Librerías nativas 67
Otros ficheros 68
Cadenas de texto 71
Construyendo una línea temporal 75
5. SDK Tools 76
adb 76
aapt 77
6. Resumen de muestra Servicio SMS Premium 78
7. Automatizando la recuperación de información 78

Capítulo III
Análisis estático 81
1. Iniciando el análisis 81
2. Código Java 82
Herramientas 83
3. Código incluido en los assets 89
4. Código nativo 91
Herramientas 91

5. Código smali 97
Herramientas 98
Sintaxis básica 98
6. Código Jasmin 108
Herramientas 108
Sintaxis básica 109
7. Opcodes 113
Herramientas 114
8. Ofuscación 115
Herramientas 118
9. Completando el arsenal 130
Enjarify 131
Dare 132
Dedexer 132
10. Extracción automatizada de código 133

Capítulo IV
Análisis dinámico 137

1. Consideraciones iniciales 138
Conexión con el dispositivo Android 138
Instalación de aplicaciones en el dispositivo Android 138
Acceder a la shell del dispositivo Android de forma remota 139
Obteniendo ficheros del dispositivo Android 141
Ejecución de comandos en shell 141
Restauración de la máquina virtual Android 141
2. Observando la ejecución 142
Logcat 142
Captura de tráfico de red 144
Inspección de cambios en el sistema de ficheros 148
Volcado de información del sistema 150
Ejecución externa de código 150
3. Alterando la ejecución en nuestro favor 152
Técnicas y herramientas 152
Activity manager 154
Modificación de código 158
App hooking 162
System hooking 168
4. Monitorización aplicando hooking con android-hooker 171
5. Técnicas basadas en depuración 176

Código Java 176
Código nativo 182
6. Sandboxing 187
Droidbox 188
Automatizando la interacción 193

Capítulo V
Tipos y muestras de malware 195
1. Persistencia 195
Ocultación 195
Denegación de servicio 197
2. Adware 199
Características 199
3. Phishing 202
Características 202
4. Spyware 205
Características 205
5. RAT 211
Características 212
6. Keyloggers 216
Características 216
7. Tap-jacking 219
Características 219
8. Clickers 222
Características 222
9. Ransomware 225
Características 226
10. Servicios de pago 230
Características 231
11. Laboratorio de pruebas 234
Cuestiones 234
Respuestas 235

Capítulo VI
Investigación con Tacyt 241
1. Localización de aplicaciones sospechosas 241
2. Malware y técnicas OSINT: Fobus 246

■ ■ ■

Índice alfabético 253

Libros publicados.....263