

Оглавление

Введение	9
Что вы найдете в этой книге?	10
Для кого эта книга?	11
Предисловие ко второму изданию	11
Условные обозначения	12
Приложение AnTrack	12
 ЧАСТЬ I	13
 Глава 1. Пять столпов Android. Технологии, лежащие в основе самой популярной ОС	15
Виртуальная машина	15
Многозадачность	18
Binder	21
Сервисы Google	23
Ядро Linux и рантайм	24
Android Go	26
 Глава 2. От кнопки включения до рабочего стола	29
Шаг первый. Aboot и таблица разделов	29
Шаг второй. Раздел boot	31
Шаг второй, альтернативный. Раздел recovery	33
Шаг третий. Инициализация	33
Шаг четвертый. Zygote и app_process	35
 Глава 3. Treble, A/B-разметка, динамические и модульные обновления	39
Treble	40
A/B-разметка	41
Динамические обновления	44
Виртуальная A/B-разметка	46
Модульные обновления	46
Трюк с сохранением пространства	48

Глава 4. Броня Android	51
Полномочия.....	52
Ограничения.....	55
Запрет доступа к другим приложениям	56
Шифрование данных	57
Доверенная среда исполнения.....	59
Доверенная загрузка.....	61
Защита от срыва стека.....	62
SELinux.....	65
Seccomp-bpf.....	66
Виртуализация	68
Google Play Protect.....	69
Smart Lock	70
WebView.....	72
SafetyNet (Play Integrity API).....	73
Kill Switch.....	74
Цифровые подписи APK	74
Итог.....	76
Глава 5. Альтернативные прошивки, рутинг и кастомизация	77
GrapheneOS	77
Tor	79
Рутинг	80
SuperSU	82
Magisk.....	82
Модификации.....	83
ЧАСТЬ II.....	85
Глава 6. Основы взлома.....	87
Делаем платное бесплатным.....	87
Снаряжаемся	88
Вскрываем подопытного	89
Изучаем код	90
Вносим правки.....	92
Глава 7. Внедряемся в чужое приложение	95
Ищем точку входа.....	95
Пишем payload	97
Вызываем payload.....	98
Крадем данные.....	100
Периодические задачи.....	103
Глава 8. Продираемся сквозь обфусцированный код.....	105
Как работает обфускация	105
Упаковщики	109
Деобфускаторы	109
Небольшой пример.....	112

Глава 9. Взлом с помощью отладчика	117
Отладчик и реверсинг.....	117
Флаг отладки.....	118
Декомпиляция и дизассемблирование	118
Android Studio	118
Используем дизассемблированный код.....	121
Глава 10. Frida	123
Dynamic Instrumentation Toolkit	123
Первые шаги	124
Пишем код.....	126
Внедряемся.....	127
Ломаем CrackMe	129
Перехват нативных библиотек	131
Другие примеры применения Frida	132
Обход защиты на снятие скриншотов	133
Извлечение SSL-сертификата приложения из KeyStore.....	134
Обход детекта root.....	135
Обход упаковщиков	136
Выводы	137
Глава 11. Drozer и другие инструменты	139
Активности.....	140
Перехват интенгов	142
Перехват возвращаемого значения	143
Content Provider.....	144
Сервисы	145
Другие возможности	146
Другие уязвимости	146
Выводы.....	149
Другие инструменты	149
Статический анализ	149
Jadx	149
JEB.....	150
Apktool	150
APKiD.....	150
Simplify.....	151
DeGuard.....	151
Bytecode Viewer.....	152
QARK	153
Динамический анализ.....	153
Objection.....	154
Inspeckage.....	154
Что еще может пригодиться?.....	155
ЧАСТЬ III	157
Глава 12. История вирусописательства для Android.....	159
До нашей эры, или Как написать вирус за 15 минут	159
Geinimi и все-все-все	160

DroidDream и начало борьбы за чистоту маркета.....	161
Zeus-in-the-Mobile	162
Первый IRC-бот	164
Первый полиморфный троян	164
Вирус-матрешка	165
Действительно продвинутый троян	167
Ransomware	168
Adware	170
Click fraud	170
А как же другие ОС?	171
Глава 13. Современные образцы вредоносных программ.....	173
Toast Amigo	173
Android/Banker.GT!tr.spy	173
Chrysaor	174
Rootnik	175
Mandrake	176
Joker	177
MalLocker	178
Вредоносные библиотеки	180
Уязвимости, используемые троянами.....	181
StrandHogg — уязвимость с подменой приложений	181
Cloak & Dagger.....	182
Перекрытие диалогов запросов разрешений.....	184
Глава 14. Пишем вредоносную программу для Android	185
Каркас	185
Информация о местоположении.....	187
Список установленных приложений.....	189
Дамп SMS	190
Запись аудио.....	191
Съемка	192
Складываем все вместе	198
Задания по расписанию.....	198
Снимок при включении экрана	199
Запуск при загрузке	199
Запись аудио по команде	200
Отправка данных на сервер	201
Выводы	201
Глава 15. Используем возможности Android в личных целях	203
IPC.....	203
Интенды.....	204
Широковещательные сообщения	205
Логирование звонков	207
Скрытые API	208
Оригинальный фреймворк.....	210
Рефлексия.....	211
Какие еще скрытые API существуют?	211
Запрет рефлексии в Android 9	211

Системный API	212
Немного теории	212
Уровень доступа privileged	213
Уровень доступа signature	215
Уровень доступа development	215
Права администратора и сервис Accessibility	216
Нажимаем кнопки смартфона	217
Извлекаем текст из полей ввода	219
Блокируем устройство и защищаемся от удаления	221
Перехватываем и смахиваем уведомления	224
Права root	226
Запускаем команды	226
Получаем права суперпользователя	228
Несколько примеров	230
Сторонние библиотеки	233
Расширение функциональности	233
Плагины	233
API	234
Простейший плагин	234
Поиск плагинов	235
Запуск функций плагина	236
Динамическая загрузка кода	238
Простейший пример	238
Долой рефлексю	240
Когда модулей много	241
Берем модули с собой	242
Глава 16. Скрываем и запутываем код	245
Обфускация	245
Собственный словарь	246
Скрытие строк	247
Сохраняем строки в strings.xml	247
Разбиваем строки на части	248
Кодируем помощью XOR	248
Шифруем строки	250
Советы по использованию шифрования	252
Храним данные в нативном коде	253
«Крашим» измененное приложение	254
Сверяем цифровую подпись	255
Проверяем источник установки	257
Защита от реверса и отладки	257
Root	257
Эмулятор	259
Отладчик	261
Xposed	263
Frida	264
Клонирование	267
Предметный указатель	268