

Содержание

ВВЕДЕНИЕ.....	9
ГЛАВА 1. СТЕК ТЕХНОЛОГИЙ ANDROID	13
1.1. JAVA	14
1.2. МНОГОЗАДАЧНОСТЬ	17
1.3. ПЕСОЧНИЦА	20
1.4. СЕРВИСЫ GOOGLE.....	22
1.5. LINUX	23
1.6. ANDROID GO	24
ГЛАВА 2. ИНСТРУМЕНТЫ БЕЗОПАСНОСТИ ANDROID ..	27
2.1. ОБЗОР КОМПОНЕНТОВ БЕЗОПАСНОСТИ	28
2.2. СИСТЕМА ПОЛНОМОЧИЙ	30
2.3. СИСТЕМА ОГРАНИЧЕНИЙ	32
2.4. ШИФРОВАНИЕ ДАННЫХ	35
2.5. ДОВЕРИТЕЛЬНЫЕ ОТНОШЕНИЯ	36
2.6. SELINUX	37
2.7. ТЕХНОЛОГИЯ SECCOMP-BPF	38
2.8. ТЕМНАЯ ЛОШАДКА GOOGLE PLAY PROTECT	38
2.9. УМНАЯ БЛОКИРОВКА С ПОМОЩЬЮ SMARTLOCK	39
2.10. ЗАЩИТА WEBVIEW.....	40
2.11. ЦИФРОВЫЕ ПОДПИСИ APK.....	41
2.12. УДАЛЕННЫЙ СБРОС И ЗАЩИТА ОТ СБРОСА.....	41
ГЛАВА 3. ПРОЦЕСС ЗАГРУЗКИ СИСТЕМЫ	43
3.1. ЗАПУСК ЗАГРУЗЧИКА ОПЕРАЦИОННОЙ СИСТЕМЫ	44

3.2. ЗАГРУЗОЧНЫЙ РАЗДЕЛ	48
3.3. ИНИЦИАЛИЗАЦИИ СИСТЕМЫ	50
3.4. СЛУЖБА ZYGOTE	51
ГЛАВА 4. БЕСШОВНЫЕ ОБНОВЛЕНИЯ	53
4.1. БОЛЬ ANDROID.....	54
4.2. ИНТЕРФЕЙС TREBLE	55
4.3. А/В-РАЗМЕТКА.....	57
4.4. ДИНАМИЧЕСКИЕ ОБНОВЛЕНИЯ	61
ГЛАВА 5. КАК МОЖНО ВЗЛОМАТЬ ANDROID.....	65
5.1. ПРИБОРЫ И МАТЕРИАЛЫ.....	66
5.2. ВСКРЫВАЕМ APK.....	70
5.3. ВНОСИМ ИЗМЕНЕНИЯ В ПРОГРАММУ.....	75
5.4. УСТАНОВКА ANDROID STUDIO В LINUX	77
ГЛАВА 6. ВНЕДРЕНИЕ В ПРИЛОЖЕНИЕ	83
6.1. ПОДГОТОВИТЕЛЬНЫЕ МЕРОПРИЯТИЯ	85
6.2. ПИШЕМ ВРЕДОНОСНЫЙ КОД. ПОПЫТКА 1	86
6.3. ПИШЕМ ВРЕДОНОСНЫЙ КОД. ПОПЫТКА 2	89
ГЛАВА 7. ПРАВИЛЬНОЕ ИСПОЛЬЗОВАНИЕ ОТЛАДЧИКА	95
7.1. ЗАЧЕМ НАМ НУЖЕН ОТЛАДЧИК	96
7.2. ПРОГОНКА КОДА ЧЕРЕЗ JADX	98
7.3. ИМПОРТ ПРОЕКТА В ANDROID STUDIO И ЗАПУСК ОТЛАДЧИКА	100
ГЛАВА 8. ЗАПУТЫВАЕМ КОД	105
8.1. ЧТО ТАКОЕ ОБФУСКАЦИЯ КОДА	106

8.2. ДЕОБФУСКАТОРЫ	111
8.3. УПАКОВЩИКИ	113

ГЛАВА 9. ИНСТРУМЕНТ DROZER И ДРУГИЕ ПОЛЕЗНЫЕ ИНСТРУМЕНТЫ 115

9.1. ЗНАКОМСТВО С DROZER И ЕГО УСТАНОВКА	116
9.2. ИСПОЛЬЗОВАНИЕ DROZER.....	121
9.3. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ	129

ГЛАВА 10. ПАКЕТ DYNAMIC INSTRUMENTATION TOOLKIT 131

10.1. ПОДГОТОВКА К РАБОТЕ	132
10.2. ОСНОВЫ FRIDA.....	135
10.2.1. Вызов Frida из командной строки	136
10.2.2. Python-сценарий для выполнения произвольного JavaScript-кода	136
10.3. ВНЕДРЯЕМ КОД.....	137
10.4. ОБХОД PIN-КОДА.....	144
10.5. БРУТФОРС PIN-КОДА.....	145
10.6. ЧТО ДЕЛАТЬ ДАЛЬШЕ?.....	147

ГЛАВА 11. ВИРУСОЛОГИЯ. ПИШЕМ ВИРУС ДЛЯ ANDROID 149

11.1. ОТ ПЕРВОГО ВИРУСА ДО НАШИХ ДНЕЙ	150
11.2. ВИРУС GEINIMI	156
11.3. DROIDDREAM	157
11.4. ТОТ САМЫЙ ЗЕВС	158
11.5. ВИРУС OP.FAKE	158
11.6. BACKDOOR.ANDROIDOS.OBAD.A	159
11.7. SIMPLE LOCKER	159

11.8. ПИШЕМ СОБСТВЕННЫЙ ВИРУС	161
11.8.1. Прежде, чем начать.....	161
11.8.2. Манифест	162
11.8.3. Реализация функционала.....	164
Список установленных приложений	164
Получение списка SMS	165
Получение информации о местоположении устройства	166
Прослушка	168
Съемка камерами	169
Используем код	175

ГЛАВА 12. ПРИМЕРЫ СОВРЕМЕННЫХ ВИРУСОВ ДЛЯ ANDROID 179

12.1. ANDROID/BANKER.GT!TR.SPY – КРАЖА БАНКОВСКОЙ ИНФОРМАЦИИ	180
12.2. CHRYSAOR (ХРИСАОР) – САМОЛИКВИДИРУЮЩИЙСЯ ВИРУС	184
12.3. MAILLOCKER - ВЫМОГАТЕЛЬ	186
12.4. JOCKER - ДОЛГОЖИТЕЛЬ	186
12.5. MANDRAKE - ТРЕКОМПОНЕНТНЫЙ	187
12.6. ROOTNIK – ПРОДВИНУТЫЙ ВИРУС	188
12.7. VULTUR – КРАЖА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.....	189
12.8. GRIFTHORSE – ПОДПИСКА НА ПЛАТНЫЕ СЕРВИСЫ	189
12.9. ROGUE	190
12.10. ADWARE.NEWDICH – УГРОЗА МЕСЯЦА.....	191

ГЛАВА 13. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ANDROID 193

13.1. МЕЖПРОЦЕССНОЕ ВЗАИМОДЕЙСТВИЕ BINDER	194
13.2. ИСПОЛЬЗОВАНИЕ СКРЫТЫХ API	198
13.3. УРОВНИ ПОЛНОМОЧИЙ	200
13.3.1. Привилегированные приложения.....	201
13.3.2. Системные приложения.....	202

13.3.3. Права администратора	202
13.4. НАПИСАНИЕ ПРИЛОЖЕНИЙ С ПРАВАМИ ROOT.....	205
13.5. ПРОЕКТ ANDROID KEYLOGGER.....	206
ГЛАВА 14. СОКРЫТИЕ КОДА	211
14.1. ОБФУСКАЦИЯ. PROGUARD, R8 И ДРУГИЕ	213
14.1.1. Введение в обфускацию	213
14.1.2. Место ProGuard в процессе сборки приложения	215
14.1.3. Алгоритм работы ProGuard	216
14.1.4. R8	223
14.2. СОКРЫТИЕ СТРОК.....	224
14.3. ХОР-КОДИРОВАНИЕ	226
14.4. ДАННЫЕ В НАТИВНОМ КОДЕ	227
14.5. ЦИФРОВЫЕ ПОДПИСИ.....	229
14.6. ОПРЕДЕЛЯЕМ ЭМУЛЯТОР	230
14.7. ЗАЩИТА ОТ ОТЛАДКИ	231
ПРИЛОЖЕНИЕ ШВЕЙЦАРСКИЙ НОЖ ХАКЕРА	233
П.1. КАК ВОССТАНОВИТЬ ПАРОЛЬ TOTAL COMMANDER	233
П.2. БЕСПЛАТНАЯ ОТПРАВКА SMS ПО ВСЕМУ МИРУ	234
П.3. ЗАПУТЫВАЕМ СЛЕДЫ В ЛОГАХ СЕРВЕРА.....	235
П.4. ВОРУЕМ WINRAR	236
П.5. ПРИВАТНАЯ ОПЕРАЦИОННАЯ СИСТЕМА KODACHI	237
П.6. ПЛАГИН PRIVACY POSSUM ДЛЯ FIREFOX	237
П.7. ПОЛУЧАЕМ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ О ПОЛЬЗОВАТЕЛЕ FACEBOOK	238
П.8. УЗНАЕМ МЕСТОНАХОЖДЕНИЕ ПОЛЬЗОВАТЕЛЯ GMAIL	238
П.9. ОБХОД АВТОРИЗАЦИИ WI-FI С ГОСТЕВЫМ ДОСТУПОМ. ЛОМАЕМ ПЛАТНЫЙ WI-FI В ОТЕЛЕ	239
П.10. САЙТ ДЛЯ ИЗМЕНЕНИЯ ГОЛОСА.....	240

П.11. СПАМИМ ДРУГА В TELEGRAM С ПОМОЩЬЮ TERMUX	240
П.12. УЗНАЕМ IP-АДРЕС ЧЕРЕЗ TELEGRAM	241
П.13. КАК УБИТЬ ANDROID-ДЕВАЙС ВРАГА	241
П.14. ШИФРУЕМ ВИРУС ДЛЯ ANDROID	242
П.15. МСТИМ НЕДРУГУ С ПОМОЩЬЮ CALLSPAM	243
П.16. ЕЩЕ ОДНА БОМБА-СПАММЕР ТВОМВ	244
П.17. ВЗЛОМ INSTAGRAM.....	247
П.18. DDOS-АТАКА РОУТЕРА	248
П.19. SPLOITUS – ПОИСКОВИК СВЕЖИХ УЯЗВИМОСТЕЙ.....	249
П.20. УГОН TELEGRAM-АККАУНТА	250
П.21. КАК ПОЛОЖИТЬ WIFI СОСЕДА ИЛИ КОНКУРЕНТА	251