Інформаційні технології

УДК 004.852

Кутовий Олександр Олександрович
бакалавр комп'ютерних наук
Національного технічного університету України
«Київський політехнічний інститут»
Кутовой Александр Александрович
бакалавр компьютерных наук
Национального технического университета Украины
«Киевский политехнический институт»
Kutoviy O.
Bachelor of computer science
The National Technical University of Ukraine
«Kyiv Polytechnic Institute»

РЕВЕРС-ІНЖЕНЕРИНГ МОБІЛЬНИХ ДОДАТКІВ
РЕВЕРС-ИНЖЕНЕРИНГ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ
REVERSE ENGINEERING OF MOBILE APPLICATIONS

Анотація: Розглянуто основні принципи то способи взлому мобільних додатків.

Ключові слова: APK, Android, маніфест, ресурси.

Аннотация: Рассмотрено основные принципы и способы взлома мобильных приложений.

Ключевые слова: APK, Android, манифест, ресурсы.

Abstract: Review of main principles and ways of cracking mobile applications.

Keywords: APK, Android, manifest, resources.

Ви втратили вихідні коди своєї програми і вам потрібно відновити код. Ви завантажили програму з вірусом і хочете дізнатися, що він робить.

Програми під Android поширюються в архівах. Ці архіви мають розширення ".apk". Такі файли не шифруються і є по суті файлами «zip». Можете перейменувати apk-файл в zip, щоб переконатися в цьому.

Вам необхідно покопатися в APK-файлі і отримати якісь дані. Можна потренуватися на кішках. Візьмемо свою програму "Hello world", знайдемо його apk-файл в папці проекту app \ build \ outputs \ apk і перемістимо в окрему папку для дослідів.

Розпакувавши архів, ви можете побачити структуру програми і зустріти знайомі файли. І навіть над деякими файли для перегляду. Наприклад, в папці res / drawable-hdpi-v4 я знайшов свою картинку world.png. Здавалося б, ось воно - щастя. Але стривайте радіти. Якщо з зображеннями проблем немає, то з читанням XML-файл вас чекає облом. Якісь рядки вам видно, але в цілому текст абсолютно нечитабельний. Тому спочатку підемо іншим шляхом.

Так як користувальницькі додатки для Android виконуються в java-машині, то APK-файли успадковують всі характерні риси JAR-файлів.
Вміст архіву зазвичай виглядає приблизно так:

Каталог META-INF містить:
CERT.RSA - сертифікат додатку
CERT.SF - контрольні суми файлів ресурсів (картинок, звуків і т.д.)
MANIFEST.MF - службова інформація, яка описувала сам apk-файл
Каталог res містить ресурси - значки в декількох розширеннях, опис розміщення елементів на формі в xml-файлі.

AndroidManifest.xml - службова інформація про програму. У цьому файлі містяться і так звані «permission» - дозволи, які потрібні для роботи програми (наприклад, доступ до мережі або доступ до телефонної книги).

classes.dex - виконуваний код програми. Саме цей файл цікавить нас в першу чергу.

resources.arsc - таблиця ресурсів. У цьому файлі зібрані xml-опису всіх ресурсів.

Ось і вся коротка інформація, яку потрібно знати, приступаючи до розбору шкідливих програм під Android.

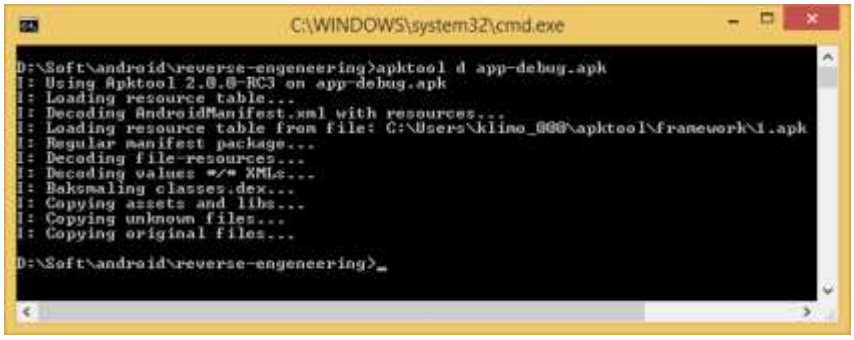
Тепер розглянемо популярні утиліти, що використовуються для вивчення програм.

Apktool

Для початку завантажуємо утиліту Apktool, який представляє собою jar-файл з номером версії. Для зручності перейменовуємо його в короткий вид **apktool.jar**, так як будемо працювати в командному рядку. Піддослідний файл розмістіть в тій же папці з утилітою.

Запускаємо у вікні командного рядка утиліту з прапором d:

```
>apktool d app-debug.apk
```



З'явиться окрема папка, ім'я якої буде збігатися з ім'ям вашого файлу. Зайдіть в неї і досліджуйте файли. Ви помітите, що XML-файли тепер доступні для читання в нормальному вигляді. Таким чином, ми можемо відкрити файл activity_main.xml і дізнатися розмітку своєї активності.

В папці ви також знайдете безліч системних файлів, які проект тягне з собою при створенні програми. На них не звертаємо уваги. Вам потрібно шукати тільки ті файли, які створювали програмісти, хакери, ви.

При вивченні своєї або чужої програми вам треба подивитися на файл маніфесту, щоб дізнатися використовувані дозволи, список активностей, сервісів і т.д. А в папці res вивчити всі ресурси, відносяться до програми.

Моя тестова програма була занадто проста. В інших прикладах можуть бути додаткові папки, наприклад, assets, яка може містити файли, картинки і т.д. Там можуть перебувати html-файли з сценаріями на Javascript, які ведуть на шкідливі сторінки.

В папці smali знаходяться вже файли класів з тим же розширенням smali. Код виглядає як в асемблері і при бажанні можна зрозуміти лістинг, але дуже незручно. Залишивши файли поки в спокої.

Першу частину завдання ми виконали.

dex2jar

Друга утиліта dex2jar, дозволяє перетворити файли dex в jar. Завантажуємо останню версію і розпаковуємо архів утиліти. Утиліта містить безліч файлів для різних ситуацій. Можете повивчати їх на дозвіллі.

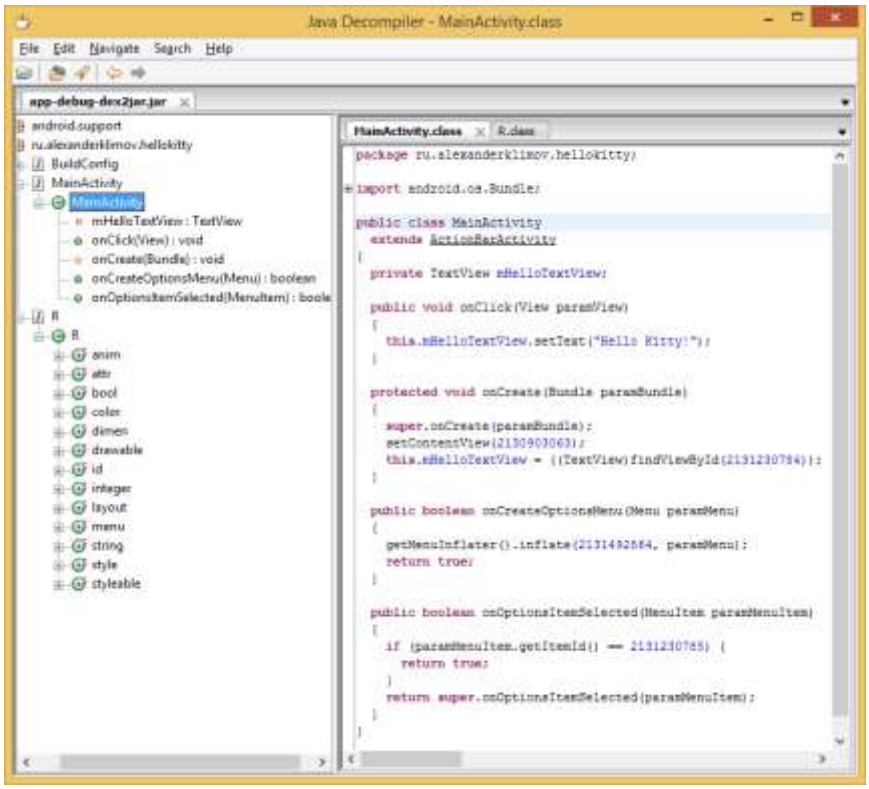
Запускаємо команду d**2j-dex2jar.bat app-debug.apk** і отримуємо на виході файл **app-debug-dex2jar.jar.** Це стандартний тип файлів для Java, але для нас поки не дуже корисний. Проте ми виконали другий крок і отримали проміжний файл.

JD-GUI

Утиліта, яка допоможе нам прочитати jar-файл, називається JD-GUI. На сторінці розробника можна знайти посилання на плагіни до середовищ розробки і навіть онлайн-версію.

Викачуємо останню версію і розпаковуємо архів. Там всього два файли - виконуємі exe-файл і readme.txt

Запускаємо програму і перетягуємо на нього jar-файл. І весь код на долоні.



Зверніть увагу, що код дещо відрізнятиметься. Наприклад, код в студії:

```
mHelloTextView = (TextView) findViewById(R.id.textView);
```

Порівняйте з кодом в утиліті.

```
this.mHelloTextView = ((TextView)findViewById(2131230784));
```

Іншими словами, замість констант з класу R підставляються їх реальні значення. Доведеться постаратися, щоб зіставити дані.

Burp Suite

Burp Suite дозволить вам переглядати HTTP-трафік на емуляторі. Скачайте останню версію.

Далі слід налаштувати проксі та інші параметри.

Література

1. Методы и технологии реинжиниринга ИС. – Режим доступу: http://citforum.ru/SE/project/isr/#_ftn1#_ftn1– Дата доступу: 14.05.2017
2. Юричев Д., Введение в reverse engineering для начинающих – (Питер). – (Бестселлеры O'Reilly), 2016-543 с.
3. "Reverse Engineering for Beginners" – Режим доступу: https://beginners.re/ /– Дата доступу: 18.04.2017.