

## דו"ח מטלת סיום מעבדת התקפה

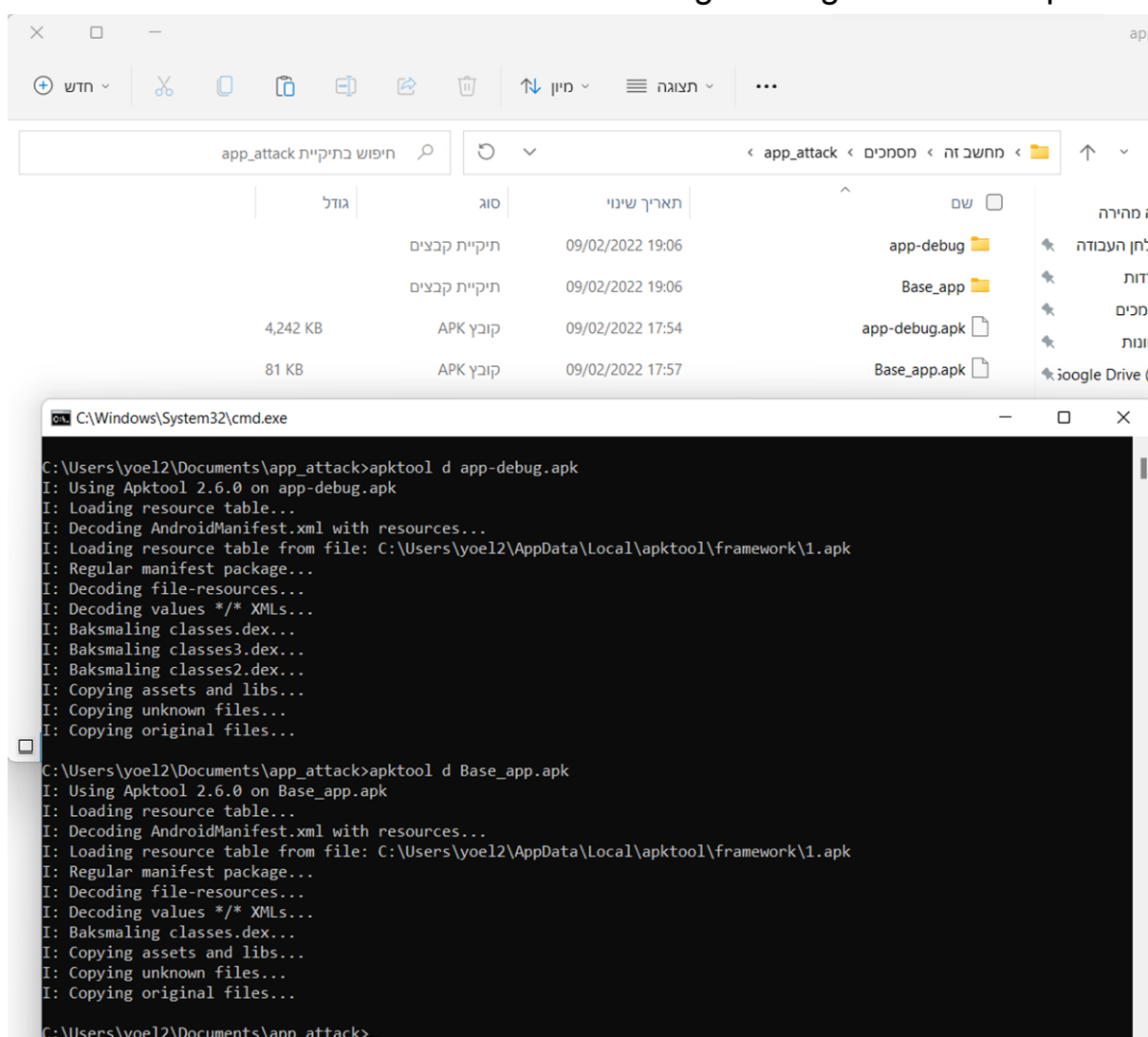
בדו"ח זה אני אתאר את התהליך שעשיתי כאשר הוספתי לאפליקציה שנתת לי קוד זדוני.

קודם כל כדי להתחיל את המטלה רציתי לרשום את הקוד הזדוני ב JAVA ואז להמיר אותו ל SMALI ואז לנסות להכניס את הקוד SMALI הזדוני לאפליקציה. כמובן שהיה ניתן גם לרשום את הקוד הזדוני ישירות ב SMALI אך הרגשתי שזה יקח לי זמן רב ולכן העדפתי לעשות בשיטה שהצגתי מקודם.

הערה: גם את הקוד הזדוני שרשמתי ב JAVA וגם את את הקוד SMALI עם הקוד הזדוני של האפליקציה Base\_app ניתן למצוא ב GitHub הבא:

<https://github.com/yoel2810/AttackLabCode.git>.

לאחר שבניתי את הקוד הזדוני ב JAVA השתמשתי ב APKTOOL כדי לעשות לו ולאפליקציה שנתת לי reverse engineering.



הפעולה הראשונה שעשיתי הייתה להעתיק את הבקשת הרשאות של הקוד הזדוני מה- Manifest ל Manifest של Base\_app (אפילו לאחר הפעלת APKTOOL הקובץ manifest נראה כמעט זהה כמו לקובץ manifest המקורי).

זה נראה כך:

```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
2
3     <uses-permission android:name="android.permission.READ_CONTACTS"/>
4     <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
5     <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
6     <uses-permission android:name="android.permission.INTERNET"/>
7     <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
8     <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
9     <uses-permission android:name="android.permission.READ_SMS"/>
10    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
11    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
12
13    <application android:icon="@drawable/icon" android:label="@string/app_name">
14        <activity android:label="@string/app_name" android:name=".MagicDate" android:screenOrientation="portrait">
15            <intent-filter>
16                <action android:name="android.intent.action.MAIN"/>
17                <category android:name="android.intent.category.LAUNCHER"/>
18            </intent-filter>
19        </activity>
20    </application>
21</manifest>
```

כעת, מתחיל החלק הקשה והוא לשלב את הקוד הזדוני בקוד של Base\_app ובפרט בלחיצת כפתור של random. קודם כל הייתי צריך למצוא איפה בכלל לשלב את הקוד. ראיתי שקיימת פונקציה getRandom אשר מפעילים אותה בתוך onclick, ולכן מכאן הבנתי מיד שאחרי זימון הפונקציה אני אמור לשים את הקוד הזדוני שלי.

```
2519
2520     .line 136
2521     :cond_0
2522     invoke-static {v0}, Ljava/lang/Integer;-->parseInt(Ljava/lang/String;)I
2523
2524     move-result v1
2525
2526     invoke-direct {p0, v1}, Lcom/MagicDate/MagicDate;-->calc(I)V
2527
2528     goto :goto_0
2529
2530     .line 137
2531     .end local v0      # "tmpAnzahl":Ljava/lang/String;
2532     :pswitch_1
2533     invoke-direct {p0}, Lcom/MagicDate/MagicDate;-->getRandom()V
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
```

Normal text file      length: 80,253    lines: 2,792    Ln: 2,541    Col: 5    Pos: 74,044    Windows (CR LF)    UTF-8    INS

עכשיו שמצאנו איפה לשים את הקוד הזדוני, צריך להעתיק אותו מהקבצי SMALI האחרים ולהדביק אותו בקבצי SMALI של האפליקציה "התמימה". חלק זה לקח לי זמן רב, ניסיתי לעשות זאת בכמה שיטות שונות ולבסוף הצלחתי. עיקר הסיבוכים והבעיות שלי נבעו מ 2 הגורמים הבאים:

- כל אזכור של "Lcom/example/malware/MainActivity" היה צריך לשנות ל "Lcom/MagicDate/MagicDate".
- היה צריך לשנות בפונקציה את locals. (כלומר לשנות את מספר האוגרים non-parameter בפונקציה)

לאחר שהבנתי את הבעיות המרכזיות הצלחתי לשים את הקוד הזדוני באפליקציה "התמימה", וכאשר לחצו על הכפתור random, הקוד הזדוני פעל ונוצר קובץ טקסט

(כמו שתואר בסרטון).

עכשיו נשאר רק להחזיר את האפליקציה קק Base\_app חזרה לקובץ APK, עושים זאת גם ע"י APKTOOL.

```
Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yoel2\Documents\app_attack4>apktool b Base_app
I: Using Apktool 2.6.0
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...

C:\Users\yoel2\Documents\app_attack4>
```

יש לנו עכשיו קובץ APK של האפליקציה עם הקוד הזדוני שלי, מה שנשאר רק לעשות הוא לחתום דיגיטלית על הקובץ APK ולהריץ באימולטור לראות שהכל עובד. ניצור קודם כל מפתח:

```
Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yoel2\Documents\app_attack\Base_app\dist>keytool -alias yoel -genKey -v -keystore mykey.keystore -keyalg RSA
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Yoel Hartman
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]:  Holon
What is the name of your State or Province?
  [Unknown]:  Israel
What is the two-letter country code for this unit?
  [Unknown]:  972
Is CN=Yoel Hartman, OU=Ariel, O=Ariel, L=Holon, ST=Israel, C=972 correct?
  [no]:  y

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 90 days
for: CN=Yoel Hartman, OU=Ariel, O=Ariel, L=Holon, ST=Israel, C=972
[Storing mykey.keystore]

C:\Users\yoel2\Documents\app_attack\Base_app\dist>
```

ולאחר מכן נחתום ע"י jarsigner:

```

Microsoft Windows [Version 10.0.22000.434]
(c) Microsoft Corporation. All rights reserved.

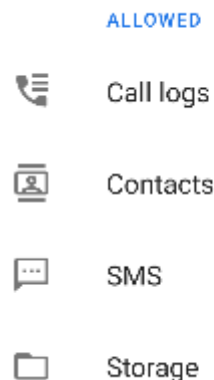
C:\Users\yoel2\Documents\app_attack4\Base_app\dist>jarsigner -keystore mykey.keystore Base_app.apk yoel
Enter Passphrase for keystore:
jar signed.

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

C:\Users\yoel2\Documents\app_attack4\Base_app\dist>_

```

הכל אמור להיות מוכן, בשלב זה בדקתי שהכל עובד (ואכן באמת הכל עובד כפי שניתן לראות בסרטון).  
 מה שכן, ניתן לראות שהרבה מידע שאני מוציא אינו מופיע (כמו הודעות SMS, אנשי קשר, שיחות), זאת מכיוון שהרצתי את האפליקציה על אילומטור ולכן הגיוני שלא יהיו לו את הדברים שיש לטלפון רגיל.  
 ההרשאות שביקשתי הן:



והמידע שלקחתי מוצג בקובץ `information.txt`.

הערה: לאחר צילום הסרטון גיליתי ששכחתי להדפיס כמה נתונים לקובץ טקסט, חוץ מכמה הבדלים של הדפסות אין שום הבדל בין מה שמוצג בסרטון לבין מה שמוצג בקובץ טקסט. ניתן גם להריץ את הקובץ `apk.212330898` ולראות שאכן האפליקציה פולטת את אותו קובץ טקסט עם כל הנתונים כמו שמוצג ב `GitHub` ושלא הוספתי דברים ידנית.