

## דו"ח מטלת סיום מעבדת התקפה

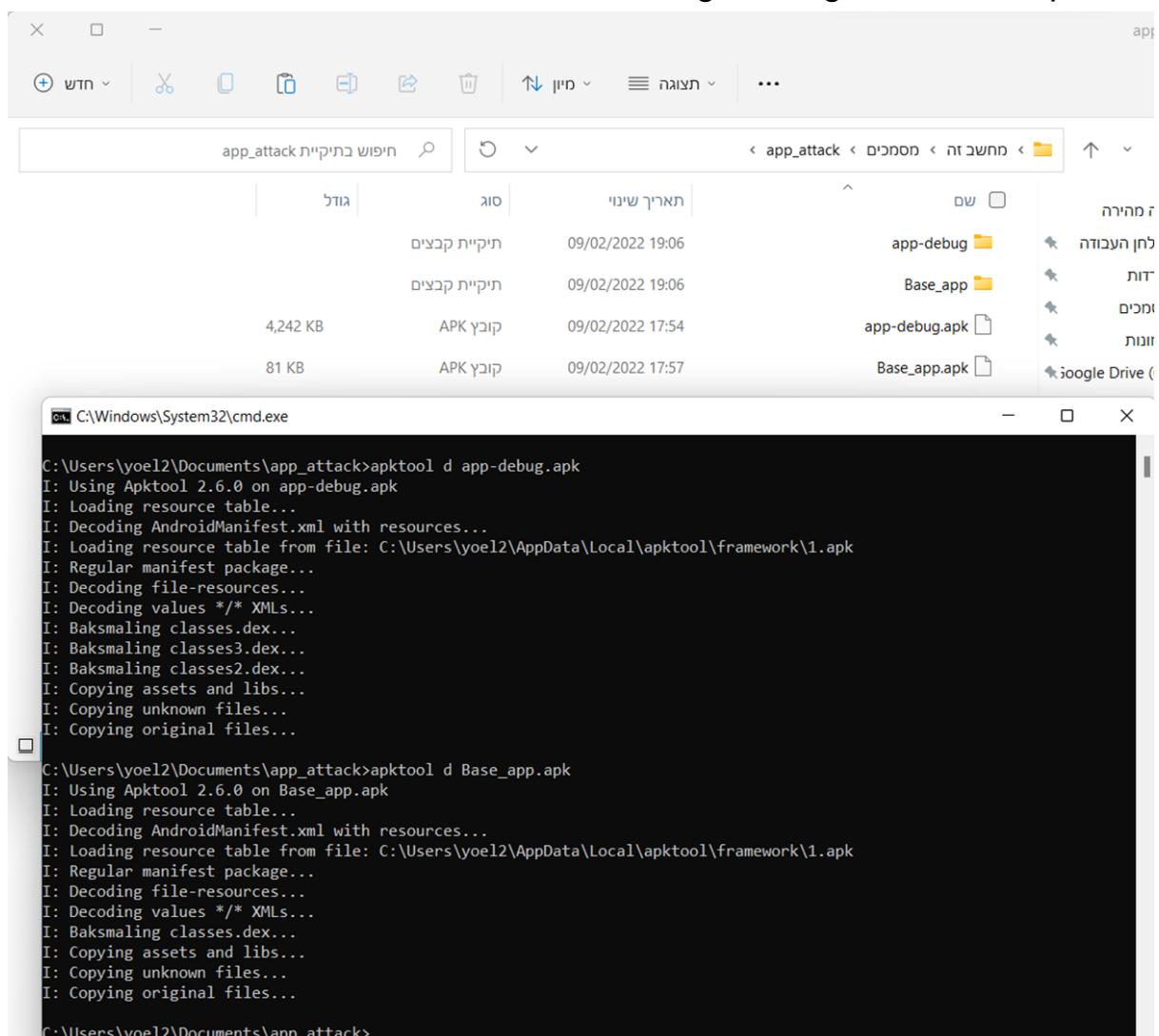
בדוח זה אני אתאר את התהליך שעשית ל애�ליקציה שנთמם לי קוד זדוני.

קודם כל כדי להתחיל את המטלה רציתי לרשום את הקוד הזרוני בJAVA ואז להמיר אותו ל-SMALI ואז לנסות להכניס את הקוד SMALI הזרוני לאפליקציה. כמובן שהיה ניתן גם לרשום את הקוד הזרוני ישירות ב-SMALI אך הרגשתי שהוא יקח לי זמן רב וכן העדפתה לעשות בשיטה שהציגי מקודם.

הערה: גם את הקוד הזרוני שרשמתי בJAVA וגם את הקוד SMALI עם הקוד הזרוני של האפליקציה Base\_app ניתן למצוא ב-GitHub הבא:

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

לאחר שבניתי את הקוד הזרוני בJAVA השתמשתי ב-APKTOOL כדי לעשות לו ואפליקציה שנתמם לי reverse engineering.



הפעולה הראשונה שעשית הייתה להעתק את הבקשת הרשאות של הקוד הזרוני מה- Manifest של Base\_app (איפילו לאחר הפעלת APKTOOL הקובץ manifest נראה כמו לקובץ 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     <uses-permission android:name="android.permission.READ_CONTACTS"/>
3     <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
4     <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
5     <uses-permission android:name="android.permission.INTERNET"/>
6     <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
7     <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
8     <uses-permission android:name="android.permission.READ_SMS"/>
9     <uses-permission android:name="android.permission.READ_CALL_LOG"/>
10    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
11
12    <application android:icon="@drawable/icon" android:label="@string/app_name">
13        <activity android:label="@string/app_name" android:name=".MagicDate" android:screenOrientation="portrait">
14            <intent-filter>
15                <action android:name="android.intent.action.MAIN"/>
16                <category android:name="android.intent.category.LAUNCHER"/>
17            </intent-filter>
18        </activity>
19    </application>
20
21</manifest>
```

כעת, מתחילה החלק הקשה והוא לשלב את הקוד הדזוני בקוד של `Base_app` ובפרט בלחיצת כפתור של `random`. קודם כל הימי צריך למצאו איפה בכלל לשלב את הקוד. ראייתי שקיימת פונקציה `getrandom` כאשר מפעילים אותה בתוך `onclick`, ולכן מכאן הבנתי מיד שאחרי דימון הפונקציה אני אמור לשים את הקוד הדזוני שלי.

```
2519
2520     .line 136
2521     :cond_0
2522     invoke-static {v0}, Lcom/MagicDate/MagicDate;->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
```

עכשו שמצאנו איפה לשים את הקוד הדזוני, צריך להעתיק אותו מהקובץ **SMALI** الآخרים ולהדביק אותו בקובץ **SMALI** של האפליקציה "התמייה". חלק זה לוקח 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 `-parameter` וחסוך בפונקציה)

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

(כמו שתואר בסרטון).

עכשו נשאר רק להחזיר את האפליקציה חוזרת 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 הזרוני שלי, מה שנשאר רק לעשות הוא לחתום דיגיטלי 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>
```

ולآخر 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 אמר ליהו מוכן, בשלב זה בדקתי שהכל עובד (ואכן באמת הכל עובד כפ' שנייתן לראות בסרטון).

מה שכך, ניתן לראות שהרבה מידע שאינו 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.

הרשאות שביקשתי הן:

ALLOWED	
	Call logs
	Contacts
	SMS
	Storage

והמידע שלקחת 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 הסרטון לבין מה שモוצג בקובץ טקסט. ניתן גם להריץ את הקובץ 212330898.apk ולראות שאכן האפליקציה פולטת את אותו קובץ טקסט עם כל הנתונים כמו שמוצג בGitHub ושלא הוספה דברים ידנית.