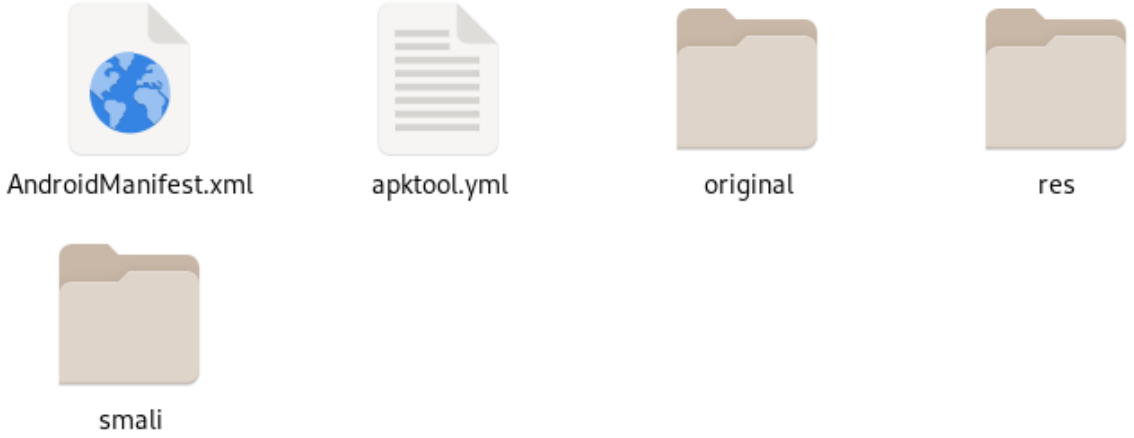
מטלת סיום מעברת התקפה
ת"ז: 314774159

תיאור התהליך:

1. בשלב הראשון חקרתי את האפליקציה שקיבלנו בעזרת apktool.



הבנתי שצריך להתמקד בתיקייה של ה smali כדי להבין איך הקוד שקיבלנו בנוי.
לאחר חקירה של הקבצים שם הבנתי שהקובץ שמעניין אותי הוא הקובץ:

2. בשלב השני חקרתי את הקובץ MagicDate.smali בכדי להבין את המבנה שלו

```
1 .class public Lcom/MagicDate/MagicDate;
2 .super Landroid/app/Activity;
3 .source "MagicDate.java"
4
5 # interfaces
6 .implements Landroid/view/View$OnClickListener;
```

לפי הקוד הנ"ל הבנתי שהמחלקה יורשת מ Activity וממשת את
ViewOnClickListener. מידע זה קריטי לבניית הקוד הזדוני שכן בניתי אותו במבנה זהה
בכדי שהאיחוד יהיה קל יותר.

3. איתור נקודה שבא ארצה להכניס את ההקוד הזדוני בשלב הזה גם הבנתי שבכל פונקציה של smali מצויינת כמות המשתנים לכן הבנתי שעדיף לשלב את הקוד כקריאה לפונקציה ואז לא אשנה את כמות המשתנים. חיפשתי את הפונקציה OnClick כי זה הגיוני שמשם תהיה קריאה לפונקציה של הRandom ואז מצאתי את הנקודה הבאה בקוד:

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

goto :goto_0
```

ובחרתי לשלב את הקריאה לקוד הזדוני כאן אחרי הקריאה לפונקציה הזו.
האפליקציה הזדונית תראה כך :

```
.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;->stealData()V
goto :goto_0
```

4. לאחר שהבנתי איפה עליי לשלב את הקוד הזדוני התחלתי בפיתוח של אפליקציה זדונית שם בחרתי בעצם מה לגנוב מהפלאפון ואיזה הרשאות לבקש
החלטתי לגנוב רשימה של אנשי הקשר שנמצאים במכשיר כלומר מספרי פלאפון ומיילים (חשוב בעיניי כדי שאוכל ליצור המשכיות בהפצת התוכנה הזדונית).
בנוסף הוצאתי רשימה של כל האפלקציות שמותקנות במכשיר ובנוסף מה המיקום שבו הן מותקנות מידע זה הוא בעל חשיבות רבה שכן הוא יכול לגלות הרבה על הבנאדם ובנוסף נדע אם יש כבר אפלקציות רגישות(כלומר בעלי חולשות ידועות) שכבר מותקנות אצלו ונוכל להשתמש בהן בעתיד.
ובנוסף הוצאתי מידע על סוג הפלאפון נתוני חומרה וכו.

5. לאחר שכתבתי את הקוד הזדוני והתאמתי אותו למבני של האפליקציה "התמימה" בניתי לו apk ואז חילצתי אותו בעזרת apktool d כדי להגיע ל smali קוד הזדוני.

6. פתיחה של האפלקצייה התמימה בעזרת apktool d ואז שילוב של הקוד smali הזדוני במיקום שצויין למעלה בחלק זה יש צורך לשנות את החתימות של הפונקציות שחילצתי מהapk של האפלקצייה הזדונית לדוגמא:

```
invoke-direct {p0}, Lcom/example/myapplication/maliciousActivity;->stealData()V
invoke-direct {p0}, Lcom/MagicDate/MagicDate;->stealData()V
```

בנוסף הוספת הרשאה לאנשי קשר לקובץ ה AndroidManifest.xml
7. בניית של ה apk מחדש עם apktool b ואז לחתום עליו עם מפתח שיצרתי
8. הרצה של האפלקצייה לאחר השינויים פלוס בדיקות שהיא לא קורסת.