Final Task

במטלה זו התבקשתי לבצע החדרת קוד זדוני לאפליקציה אשר סופקה בשם MagicDate.

קיבלתי קובץ מסוג apk עם שם האפליקציה והמרנו אותו לקוד smali ע"י הכלי apktool.

לאחר מכן בניתי אפליקציה זדונית משלי אשר מבקשת הרשאות לאנשי הקשר הודעות קבצים בזיכרון החיצוני של המערכת וליומן השיחות אשר כותבת לקובץ בשם information.txt את כל המידע אשר הוצאתי מהמכשיר.

information.txt
7:31 AM 207 kB TXT document

את האפליקציה הזדונית המרתי גם כן לקוד smali ומשם לקחתי את הקוד הרצוי כגון משתנים פונקציות וכולי , הקוד בנוי מפונקציה ראשית ואובייקט כתיבה מסוג OutputStreamWritert אשר בהתאמה קוראים לפונקציות וכותבים לקובץ הInformation .

```
# instance fields
.field private anzahl:Landroid/widget/EditText;
.field streamWriter:Ljava/io/OutputStreamWriter;
```

מצאתי את מיקום כפתור הרנדום ע"י חיפוש בקוד ה smali של אפליקציית המקור ונתקלתי בפונקציה בשם GetRandom אשר מופעלת בעת לחיצה על הכפתור.

```
.method private getRandom()V
    .locals 8
```

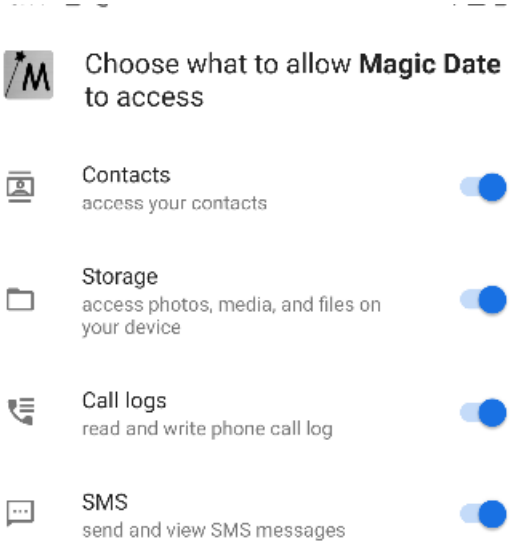
לאחר הוספת הפונקציות לרשימת הפונקציות בקוד ה smali ושינוי שם הספרייה לשם הספרייה של האפליקציה והוספת ההרשאות לקובץ ה manifest.xml , הוספתי קריאה לפונקציה הזדונית בהפעלת הפונקציה ()getRandom אשר מופעלת בלחיצה על הכפתור .

```
invoke-virtual {p0}, Lcom/MagicDate/MagicDate;->start_to_hack()V
```

בעזרת Apktool בניתי את האפליקציה בחזרה מקוד ה smali ולאחר מכן חתמתי אותה בעזרת הכלי jarsigner , לאחר החתימה אפשר להתקין את האפליקציה על המכשיר ללחוץ על כפתור ה Random והקוד הזדוני יתחיל לרוץ ולרשום את כל המידע אל תוך הקובץ .

רשימת הרשאות :

```
"android.permission.READ_CONTACTS",
"android.permission.READ_EXTERNAL_STORAGE",
"android.permission.READ_CALL_LOG",
"android.permission.READ_SMS"
```



בחירת ההרשאות התבצעה מהרצון להבין כמה שיותר על הסביבה של המשתמש ואיזה תוכן הוא צורך , בגלל שבקשת כל ההרשאות מתבצעת במקביל הנחתי שקיימים משתמשים אשר לא ישימו לב להרשאות הניתנות \ ידלגו על חלון ההרשאות ללא התייחסות.

במהלך התהליך הצלחתי גם להוציא מיקום של המשתמש ופרטים על ממשק הרשת בו הוא משתמש והרשת עצמה אך העדפתי לא להשתמש בהרשאות אלה. בהתייחסות למה שנאמר בתרגיל.