CSEC 502 Network Security, Term Project

VIZYON

**Purpose**

Our project Vizyon is an application that provides Android users to view movies in [theaters](http://tureng.com/tr/turkce-ingilizce/movies%20in%20theaters) easily.

At first, Vizyon is not different from other normal applications. However, it is an Android malware application at background. Only the parsed information on the screen is shown while the application sends data to a remote server without the awareness of the user. When Vizyon is installed, it collects such sensible informations: SMS messages, call logs, contacts, GPS location and phone number belong to device.

**Project Parts**

Our project is composed of two main parts:

* Android Application (java)
* Server Side (java, tomcat)

**1) Android Application**

***Getting movies****:* Application gets a DOM object from “http://www.beyazperde.com/filmler/vizyondakiler/sinema-sayisi/” by Jsoup Java Library. By parsing the DOM according to tags, Images and movies’ detail are listed on screen. This list is updated in each

***Collecting Infos:*** When application works, get all infos as JsonObject itself and sent it to server. After that, it remains in listening mode by opening a socket. Whenever server sends a command to get infos, application collects the related details from device and sends them to remote server. These commands are:

*String getCommandAll =* ***"all"****; (collect all infos)  
String getCommandUtils =* ***"utils"****; (get Android Id, IMEI, IMSI, phone number)  
String getCommandGps =* ***"gps"****;  
String getCommandContacts =* ***"contacts"***

*String getCommandCallLogs =* ***"callLogs"****;*

*String getpCommandMessages =* ***"messages"****;  
String attackCommand =* ***"attack"****;  
String stopCommand =* ***"stop"****;*

Application needs permissions to reach sensitive information. These permissions are added to AndroidManifest.xml:

*<uses-permission android:name="android.permission.INTERNET" />*

*<uses-permission android:name="android.permission.READ\_CONTACTS" />*

*<uses-permission android:name="android.permission.READ\_PHONE\_STATE"/>*

*<uses-permission android:name="android.permission.READ\_SMS"/>*

*<uses-permission android:name="android.permission.RECEIVE\_SMS"/>*

*<uses-permission android:name="android.permission.SEND\_SMS"/>*

*<uses-permission android:name="android.permission.ACCESS\_FINE\_LOCATION" />*

*<uses-permission android:name="android.permission.READ\_CALL\_LOG" />*

The permissions listed above, works for android versions lower than 6.0 marshmallow. By marshmallow, android devices prevent to access sensitive data without user’s permissions. Therefore, application checks permissions firstly. If device cannot give permission then ask to user to reach messages, contacts, callLogs, gps, and device id separately. You cannot access the data if user does not allow to application.

***Dos Attack:*** When application gets *“attack command”* from server, it creates a timer. Timer send http-post request to given url continuously. The url and time interval are provided as parameter with *“attack command”*. Server also stops the attack by *“stop command”.*

**2) Server Side**

***Store Infos:*** Server gets data sent from clients as json object and stores them according to data received date and client ip information.

***Commands:*** Server can send request to client machine with the help of client ip info and a dedicated port for send command such as 8080. “Attack command” is implemented both client and server side which can be used for DDos attack. The application is written in generic format and can be extensible for further commands such as adclicker etc.