

BITS 3453 MALWARE ANALYSIS AND DIGITAL INVESTIGATION

FINAL REPORT

GROUP KEEPALIVE

GROUP MEMBERS:

|  |  |
| --- | --- |
| NAME | MATRICS NO. |
| MUHAMMAD IZHAM BIN NORHAMADI | B032020039 |
| AHMAD SHA HERIZAM BIN TAHIR | B032020009 |
| AFFENDY ELYAS BIN AZHARI SHARIDAN | B032020024 |
| MUHAMMAD RIFQI BIN RAMLAN | B032020028 |

Table of Content

[1.0 Introduction 3](#_Toc1647053014)

[2.0 Background of the sample (.apk file) 3](#_Toc936223630)

[3.0 The process flow of the investigation and the tool used. 4](#_Toc362674349)

[3.1 Process 4](#_Toc774890227)

[3.2 Tools used 6](#_Toc966590339)

[4.0 Summarization of report gain from the online analysis. 6](#_Toc884523568)

[5.0 Finding of the group analysis. (Should include snapshot of the finding) 10](#_Toc696655365)

[6.0 Similarity of the online analysis and the group analysis. 19](#_Toc693353867)

[7.0 Conclusion 21](#_Toc1432682929)

1.0 Introduction

Mobile malware just like the name itself is a malicious software that specifically targets the operating system on mobile phones. There are many types of mobile malware variants and different methods of infection. For example, spyware, viruses, trojans and mobile phishing. All this malware can damage and gain access to private data in the mobile devices.

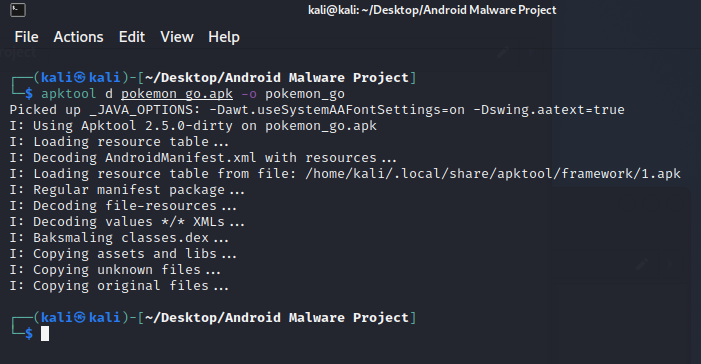
# **2.0 Background of the sample (.apk file)**

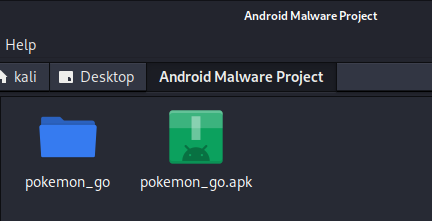
This APK is a modified version of the original application that is Pokémon Go game. When the game had not been officially released globally at the same time, many gamers wishing to access the game before it was released in their region resorted to downloading the APK from third parties. Additionally, many large media outlets provided instructions on how to download the game from a third party. Some even went further and described how to install the APK downloaded from a third party. This is an extremely risky practice and can easily lead users to installing malicious modified apps on their own mobile devices. This modified version of APK is a dangerous one that can gain access of the mobile devices by infected it with a backdoor.

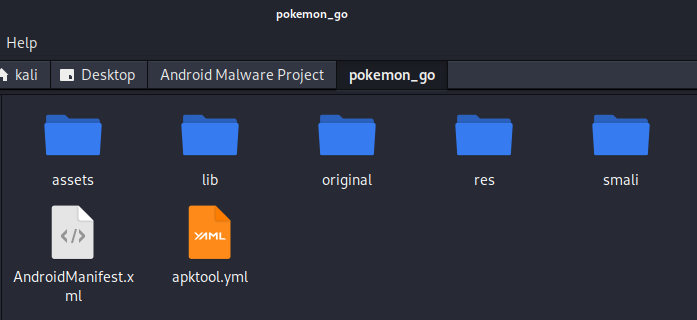
# **3.0 The process flow of the investigation and the tool used.**

## **3.1 Process**

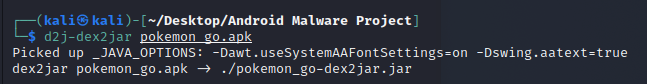
1.First, we decompile the apk file using apktool so that we can explore the contents of the apk

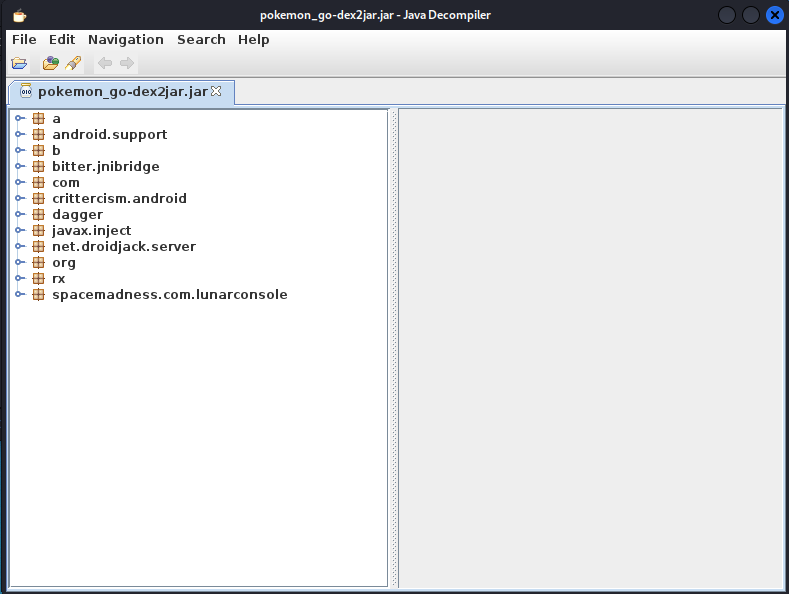




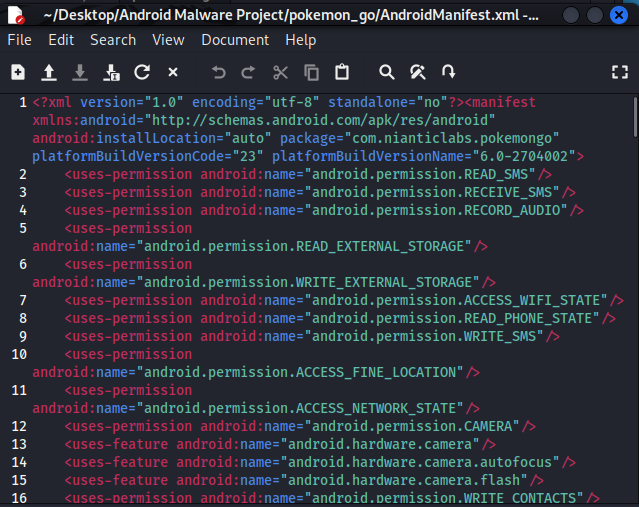


2. Then we convert the apk’s dex file to jar file and view the java classes using jd-gui





3. Before looking for malicious code in java classes, we first look into the app’s AndroidManifest.xml file as we can find key permissions and services listed there using note software

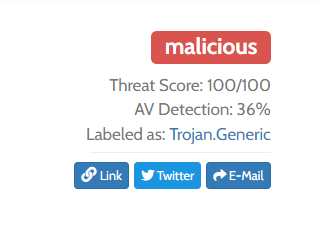


## **3.2 Tools used**

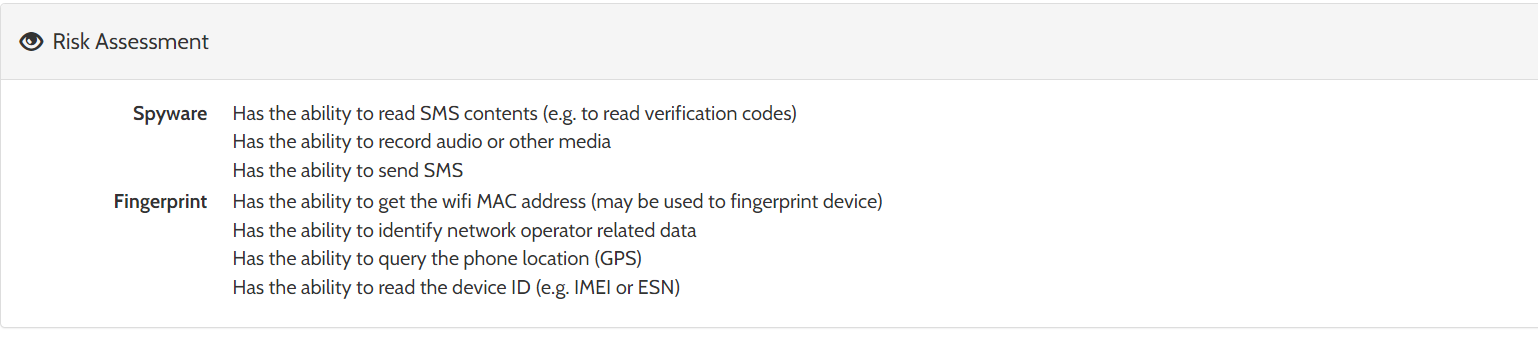
* dex2jar
* jd-gui
* apktool
* jadx-gui

# **4.0 Summarization of report gain from the online analysis.**

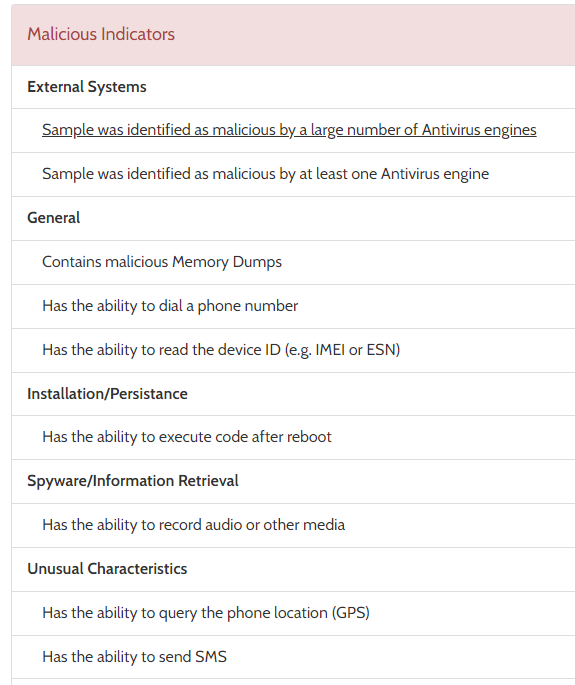
By using Hybrid-Analysis.com to do online analysis of the Pokémon Go APK, it is crystal clear that the APK is 100% malicious based on the status state by the Hybrid Analysis. Hybrid Analysis states that the APK is malicious and given extreme threat score of 100/100. Hybrid Analysis also identifies the APK resides in a dangerous malware in Trojan category.

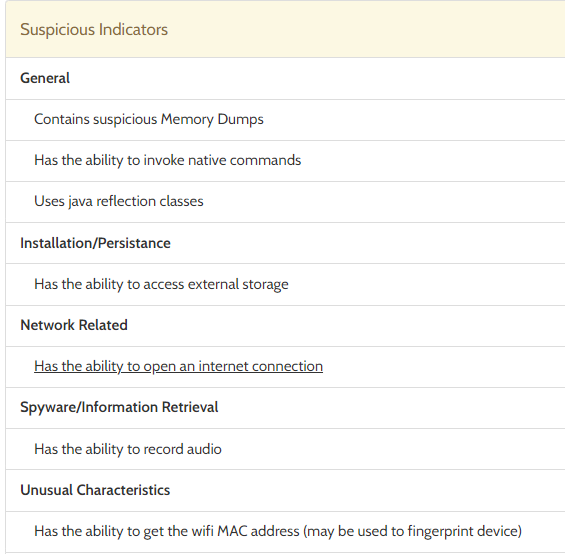


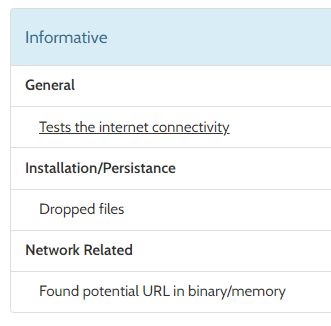
Hybrid Analysis provides risk assessment which the APK intends to do maliciously towards a user. For example, the apk can read SMS content specifically to read verification codes, record audio and even send a SMS.



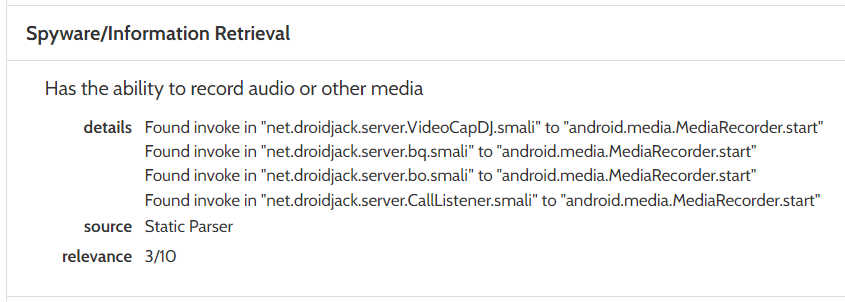
Hybrid Analysis categorized indicators which are found in the APK in three parts, Malicious, Suspicious and Informative. Malicious is indicators which can harm the mobile system, Suspicious is process that most likely can harm the mobile system that will lead to malware infection meanwhile informative is general processes which any application can do.



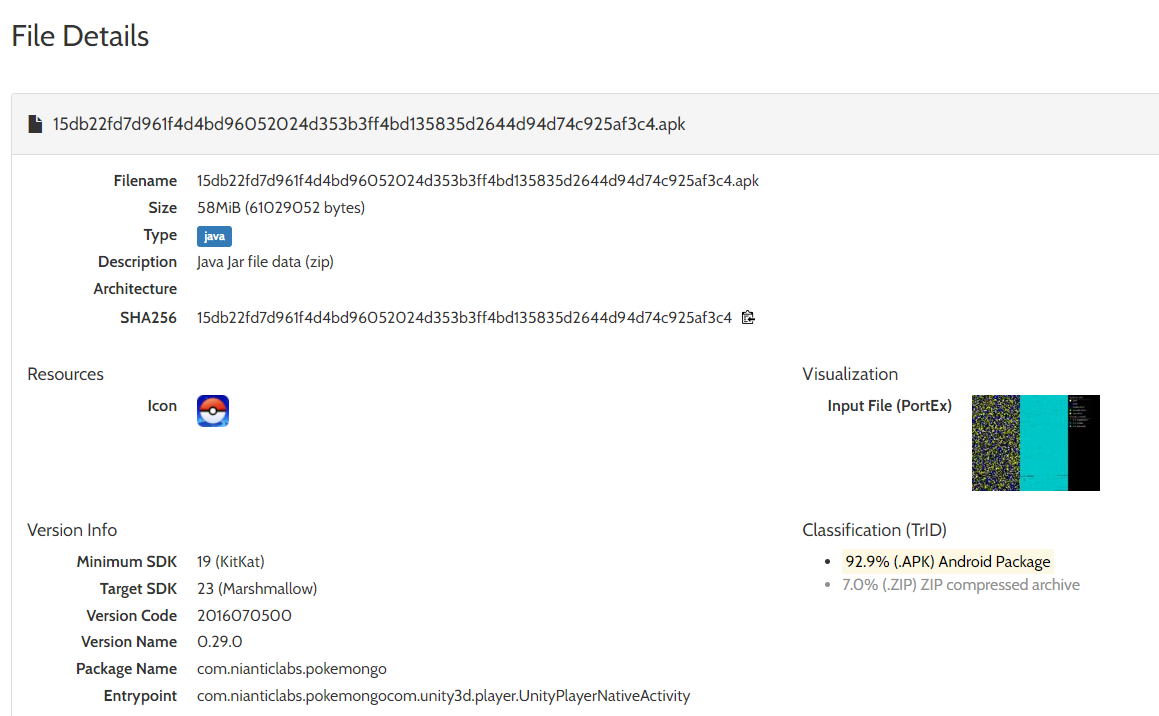




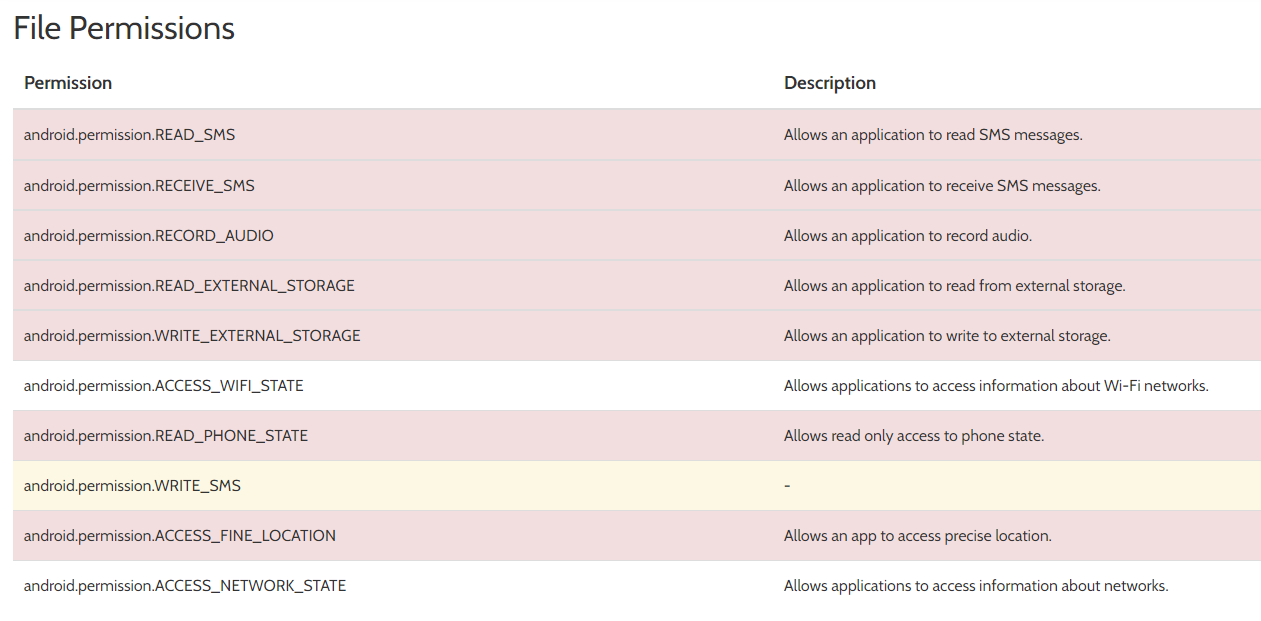
All the indicators above will have its file process shown by the Hybrid Analysis, for example, one of the indicators in Malicious category which is ‘Has the ability to record audio or other media' shows the process that can be found inside the APK.



The detailed information of the APK will display in the Hybrid Analysis such as hash function of SHA256, file size and apk version.



File permission will be listed out by Hybrid Analysis with red-colored as the malicious, yellow-colored is suspicious, and the white is generally informative based on the indicator stated above. These permissions can be found inside the apk.



# **5.0 Finding of the group analysis. (Should include snapshot of the finding)**

1. The name of the malware

* DroidJack

1. What is the application true nature

* A game that uses augmented reality for players to see their game model in real life through a screen.

1. The malicious behavior of the app

* Automatically include a backdoor malware that is DroidJack when installing the modified apk. It can gain access to many permissions in the mobile device and then steal many private data on it.

1. The intent

* With permission gained by the attacker, it can gain control of the mobile devices such as SMS so that when the attacker requesting an OTP, they can get the OTP code and gain access to the victim’s account such as bank account or any other social account.

1. The malicious permissions

* **Read user’s SMS** - Access SMS, intercept SMS, SMS on your behalf (this can be used to log into account through password recovery), (important message such as OTP is exposed).
* **Receive user’s phone GPS location** - Can be used to spy on the user’s location
* **Read and write to the phone external storage** - More malicious app can be install on the user’s phone.
* **Access the camera app and record the audio** - The exploiter can spy on the users by accessing the camera and recording the audio.
* **Read, write contacts list and call logs also call phone -** Identity theft (exploiter can pretend to be the user of the phone and perform malicious activity).

1. List of API/Function in the binary that you think malicious

* CallListener.class
* CamSnapDJ.class
* Connector.class
* Controller.class
* GPSLocation.class
* VideoCapDJ.class

1. Other necessary information that can be the traces of malicious behavior of the app.

* The app requests a lot of information such as Wi-Fi information, phone model, manufacturer, version, and has various odd strings of texts printed out in the app

Findings

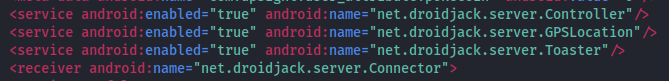
AndroidManifest.xml

* Contains multiple and dangerous permission that can breach user’s privacy such as READ\_SMS, READ\_CONTACTS, READ\_CALL\_LOG, and ACCESS\_FINE\_LOCATION

Text

Description automatically generated

* Contains droidjack services which is a software service that monitors and controls android devices with a GUI



Java Libraries

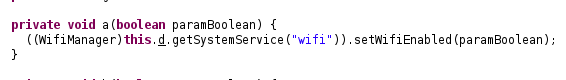
* Contains classes and functions for droidjack malware in net.droidjack.server library

Text

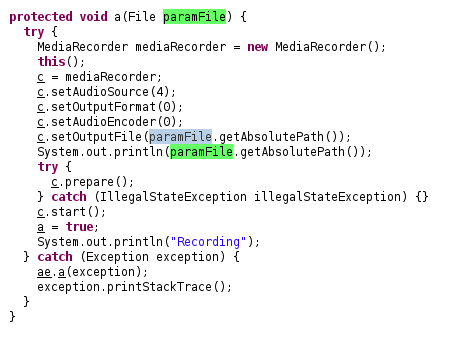
Description automatically generated

CallListener.class

* Turning on Wi-Fi for the user



* Have audio recorder and encoder function



* Uses Telephony Manager service to get device’s information such as the service provider, intercepts SMS, records call, and logs call.



* Function to spy on calls and the incoming call number

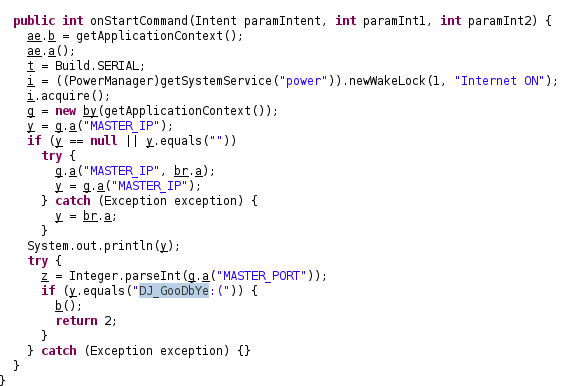


Controller.class

* Center function that calls the function that records and intercepts calls and SMS then logs them.



* Calls function that sends the information to an external IP address



CamSnapDJ.class

* Function that extracts camera status and information



VideoCapDJ.class

* Function that utilizes MediaRecorder to record video in varying quality with timer and schedule



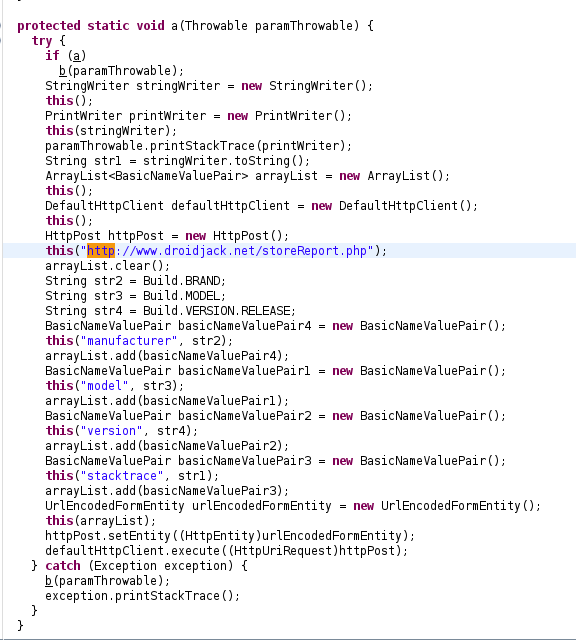
GPSLocation.class

* Allows function that tracks the user’s location to run on threads asynchronously, which allows the tracking to run separately from the primary application thread



ae.class

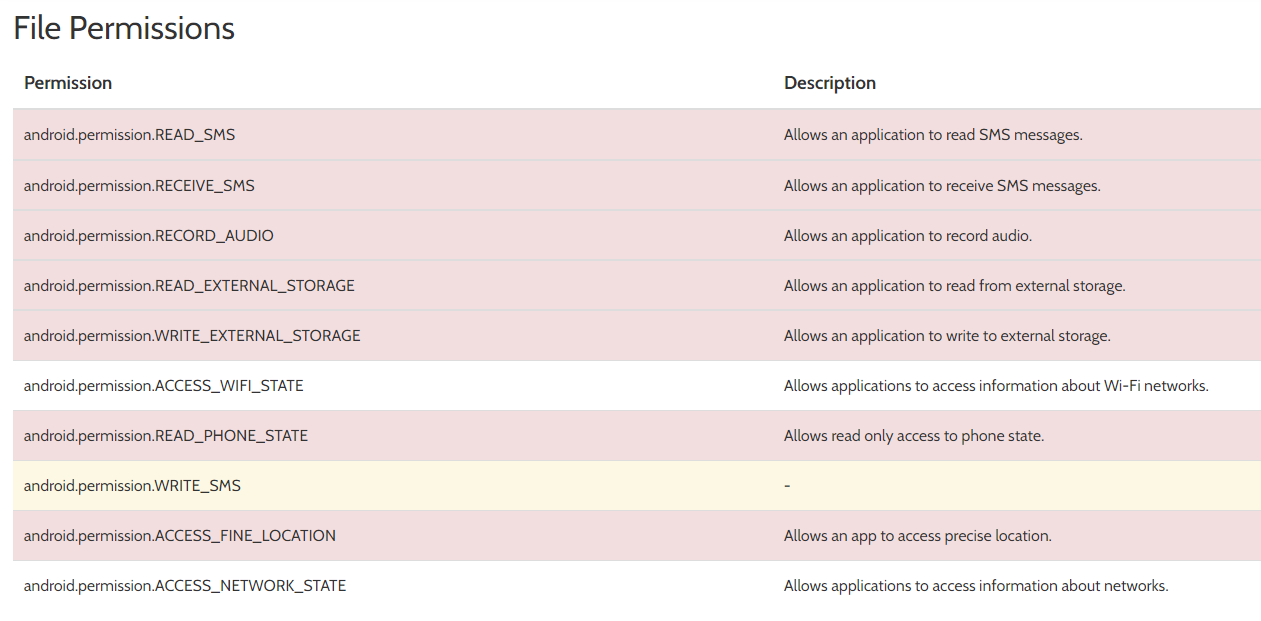
* Function that collects all the extracted information as well as device information such as the manufacturer, model and version and send them to www.droidjack.net/ storeReport.php



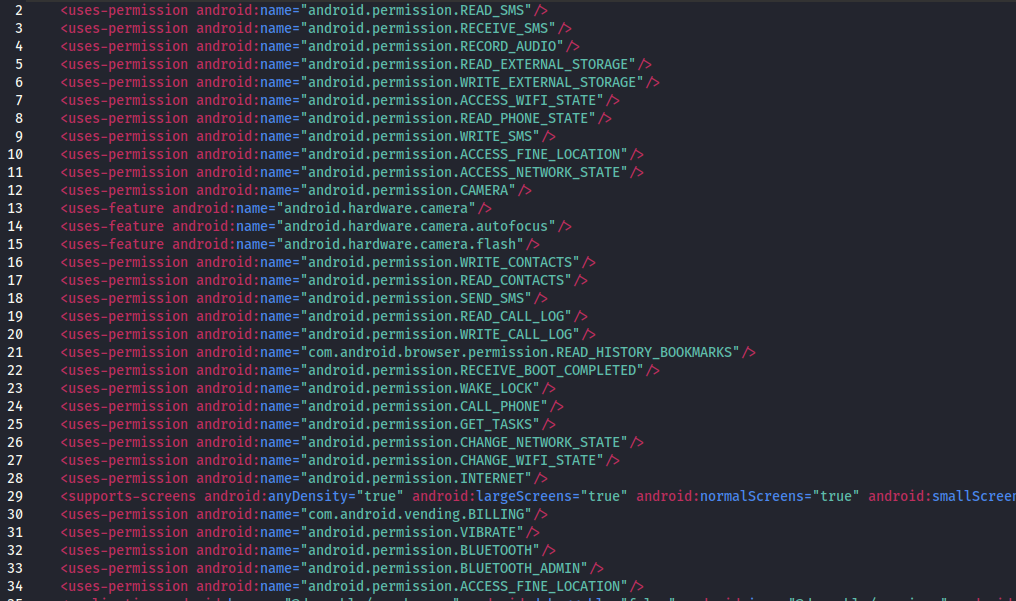
# **6.0 Similarity of the online analysis and the group analysis.**

1. APK permissions whether it is malicious, suspicious or common permission can be found in both analyses.

Online analysis:



Group analysis:



2. Both analysis found the use of droidjack which is Remote Access Tool (RAT) android trojan

Application

Description automatically generated

3. Both analysis found the use of android services to spy on the device, logs them and send the information externally

Graphical user interface, text, application

Description automatically generated

# **7.0 Conclusion**

The idea of computer virus was in 1949 and back then only computers could be infected. Nowadays, the revolution of computer viruses, especially malware, has advanced so that now it can even attack and manipulate mobile devices such as smartphones and tablets. Every layer of people in this modern era nowadays should know the general basic knowledge of mobile malware analysis. Even in our daily lives, we sometimes install applications APK on the internet which will risk our mobile devices. So, having a basic knowledge of using simple online analysis such as hybrid-analysis.com or virustotal.com is sufficient to have a general status whether the APK is malicious or not. For an individual with vast knowledge of mobile security they should make a thorough analysis of the APK to have a better understanding on how the APK works to gain more knowledge or discover new malware mobile threats. Security analyzer today are provided with plenty of tools that were created for reverse engineering to identify the malicious aspect of an android application.