

Android Malware Forensics

Mobile phone is our first need before "Food, Accommodation and Cloth". From last one decade smartphones are in vogue very fast. Nowadays smartphones have become so smart that all the necessary functions of our daily routine like as shopping, bill payment, food, hotel, flight booking, fees, fund transfers, etc. are done on the phone with the help of internet. Vendors have made their own mobile applications for each work and service.

- Ummed Meel

Introduction

Some criminals have started using this modern technology for criminal activities. Criminals steal the data, banking and personal information of consumers through malicious applications or malware. The common man does not recognize such a virus and duplicate applications and becomes a victim of criminal activities. Cyber criminals send these malware or viruses to users' phones in using distinct ways.



Android Malware

Android malware is an application or service that steals data, banking and other personal information from user's device without his permission and knowledge, and then uploads it to the remote servers. Once the malware or Trojan is installed on the android phone, they do not have any icon and neither can you uninstall them. An attacker or hacker can take complete access to your phone with the help of malware. Hackers can steal photos, videos, documents, call records, contact lists and GPS locations from your phone. Not only this, without doing any activity on the screen, hacker can click photos from your phone's camera and record audio from a microphone.

Hackers can infiltrate your phone in the following ways

- Hacker can bind malware or virus with legitimate mobile application
- Hacker can send an application with spoofed app name
- Through Social Engineering, hacker can also install malware directly from you
- Through exploitation, hacker can exploit latest vulnerabilities in android

Android Malware Forensics

There are many ways of android malware or Trojan analysis. You can also do android malware analysis through automated tools or manual. In the Android application forensics, live memory forensics, data retrieval, outgoing traffic monitoring and device behaviour are also included. But the scope of the forensic investigation officer in a malware application analysis should be as follows

- Remote host IP address or domain name
- Malicious functions of the malware
- List of permissions

Forensic analysts can easily trace and hold cyber criminals with the help of the above three information. In the following four main steps, you can easily locate the culprit's domain name or server IP address.

Step 01: Get Classes.dex file

To get classes.dex file, copy your malware application to the windows computer and rename the file extension from .apk to .ZIP. In this zip you will find all the files that were used while compilation of this application. When you unzip renamed file then you will find classes.dex file there as shown in snapshot.

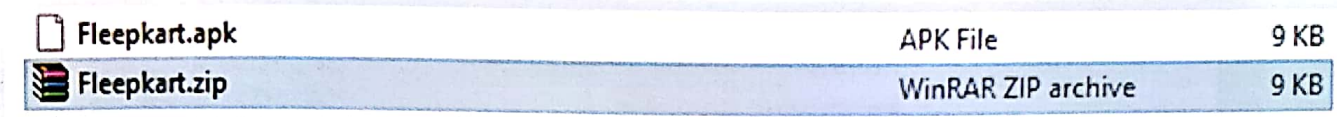


Fig 01: Rename .apk to .zip

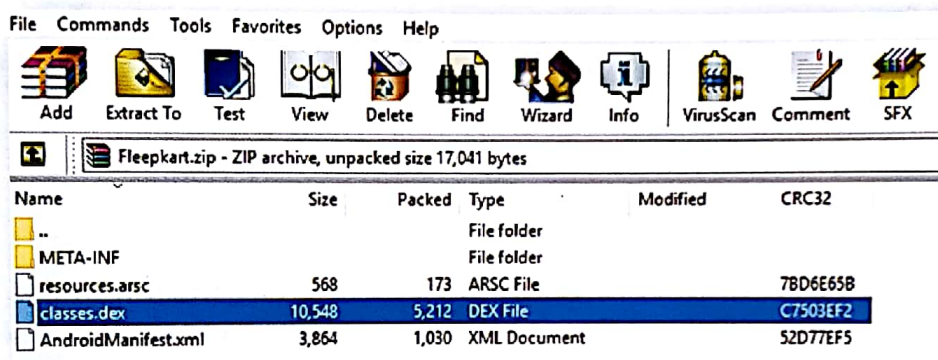


Fig 02: Get Classes.dex file

Step 02: Get classes.jar file

We use dex2jar tool to get classes.jar file from classes.dex. Copy classes.dex file (received from the previous step) to the dex2jar folder. Now open command prompt in windows and guide a path to your dex2jar folder. Now run "d2j-dex2jar.bat classes.dex" command through terminal. You can download dex2jar tool from internet. After the successful completion of command you will find classes-dex2jar.jar in the same folder as shown in snapshot.

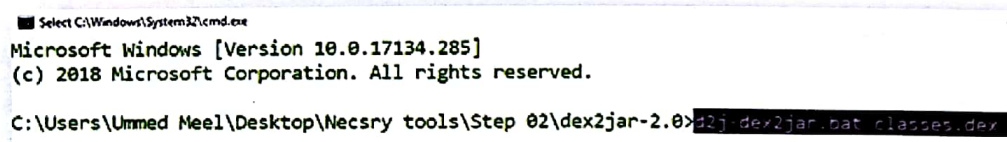


Fig 03: run command

lib	27-10-2014 17:32	File folder	
classes.dex		DEX File	11 KB
classes-dex2jar.jar	06-10-2018 11:33	Executable Jar File	8 KB
d2j_invoke.bat	27-10-2014 17:32	Windows Batch File	1 KB
d2j_invoke.sh	27-10-2014 17:32	SH File	2 KB
d2j-baksmali.bat	27-10-2014 17:32	Windows Batch File	1 KB
d2j-baksmali.sh	27-10-2014 17:32	SH File	2 KB
d2j-dex2jar.bat	27-10-2014 17:32	Windows Batch File	1 KB

Fig 04: Get classes-dex2jar.jar file

Step 03: Get JAVA files

To get all available classes file we use jd-gui (java de compiler) tool. Run jd-gui tool on your system and import classes-dex2jar.jar (received from the previous step). After complete de compilation you will find all .class file.

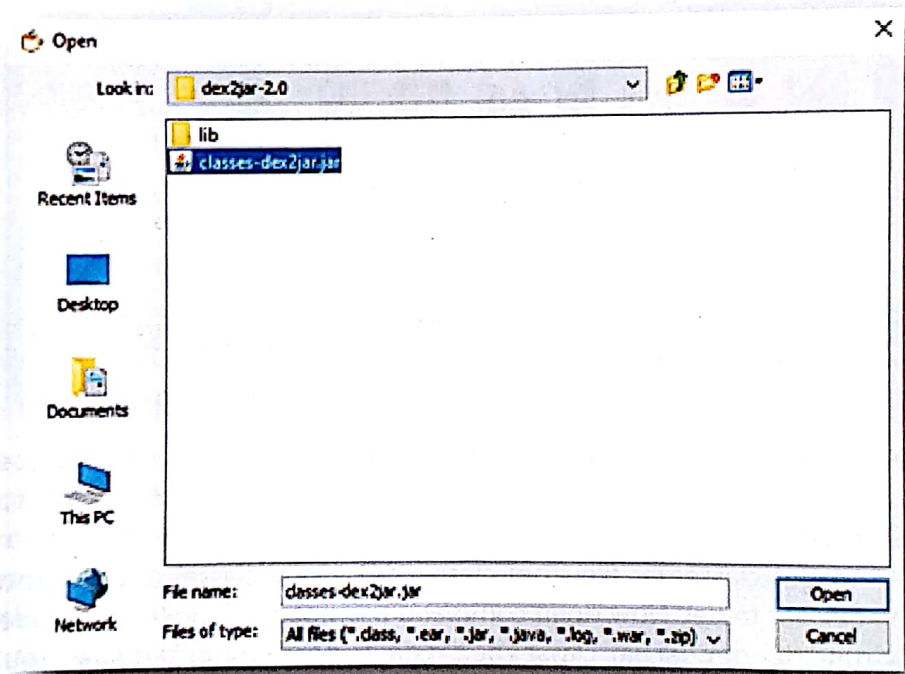


Fig 05: Import classes-dex2jar.jar file

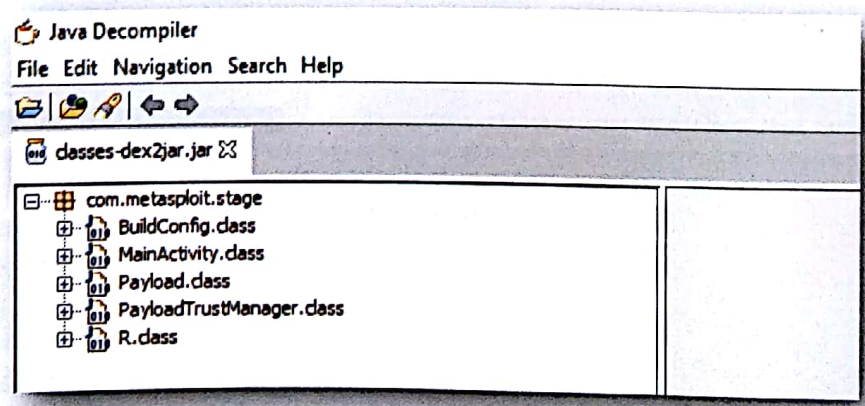


Fig 06: class files

Step 04: Remote IP or Domain name

As an investigation officer you should always look forward for remote host IP or domain name. Here we got a suspicious class named as payload.class. After getting deep into this class we found a specific class named as "payload". This class is designed to get command and send required data to the hacker. In this class we also found hacker's IP address on which he is uploading user's data.

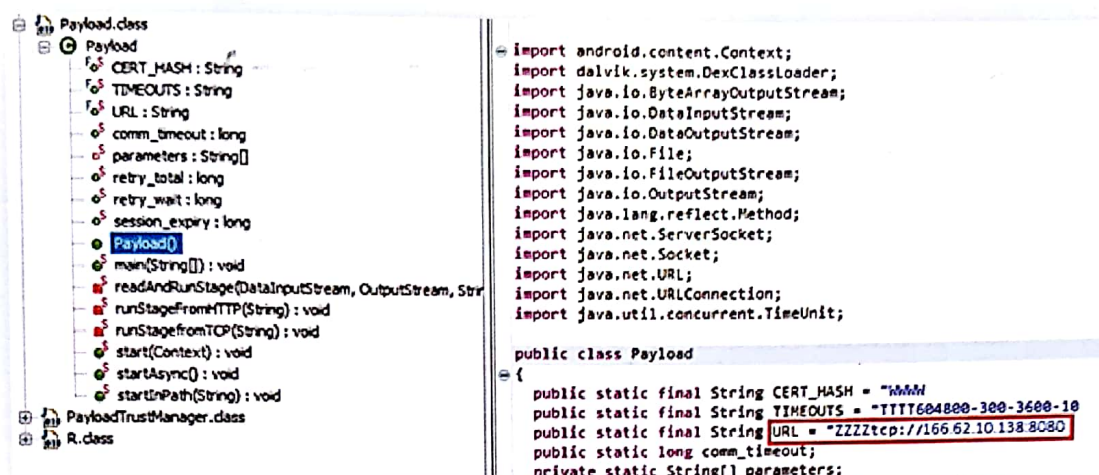


Fig 07: Hacker's server IP address

Note: It is not necessary that the hacker server's IP address or domain name will always be found in such a folder or file. We should check all files and folders to avoid duplicate IP and get the right result.

List of permissions

To see the list of permissions being used by any Android application, we use Apktool software. You can download Apktool from the internet. Copy malicious application into the Apktool folder. Use java -jar apktool_2.1.1.jar d yourappname.apk command in terminal.

```
Select C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17134.285]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Ummed Meel\Desktop\Necstry tools\permission>java -jar apktool_2.1.1.jar d Fleepkart.apk
I: Using Apktool 2.1.1 on Fleepkart.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\Ummed Meel\apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\Users\Ummed Meel\Desktop\Necstry tools\permission>
```

Fig 08: Apktool de compile command






Name	Date modified	Type	Size
 original	06-10-2018 12:27	File folder	
 res	06-10-2018 12:27	File folder	
 smali	06-10-2018 12:27	File folder	
 AndroidManifest.xml	06-10-2018 12:27	XML Document	2 KB
 apktool.yml	06-10-2018 12:27	YML File	1 KB

Fig 09: AndroidManifest.xml file

```

1 <?xml version="1.0" encoding="utf-8" standalone="no"?>
2 <manifest xmlns:android="http://schemas.android.com/apk/res/android" package="c
3   <uses-permission android:name="android.permission.INTERNET"/>
4   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
5   <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
6   <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
7   <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
8   <uses-permission android:name="android.permission.SEND_SMS"/>
9   <uses-permission android:name="android.permission.RECEIVE_SMS"/>
10  <uses-permission android:name="android.permission.RECORD_AUDIO"/>
11  <uses-permission android:name="android.permission.CALL_PHONE"/>
12  <uses-permission android:name="android.permission.READ_CONTACTS"/>
13  <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
14  <uses-permission android:name="android.permission.RECORD_AUDIO"/>
15  <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
16  <uses-permission android:name="android.permission.CAMERA"/>
17  <uses-permission android:name="android.permission.READ_SMS"/>
18  <application android:label="@string/app_name">

```

Fig 10: list of permission

After the compilation, a new folder is formed in which there will be a file named as AndroidManifest.xml. You can see the list of permissions by opening this file with any code editor. It is clear from the above analysis that cyber criminals are uploading personal information of the consumer on remote IP address using multiple malicious permissions.

Introduction of Author



UMMED MEEL, Designation: Cyber Expert (Police and Defense Trainer)

Education: B Tech (ECE), CEH (EC-Council), Diploma in Cyber Law, LLB (Pursuing)

Ummad is closely associated with police, Air Force, BSF, and higher defence authorities in India from last 5+ years. Ummad has conducted 50+ trainings and workshops for Indian Police of Delhi, Uttar Pradesh, Rajasthan, Haryana and Himachal police etc. and trained more than 8,000 police officers and other LEA's. He has also conducted 40+ seminars for government/non-government organizations, school, colleges and other law enforcement

agencies on Cybercrime awareness. He has 5+ years of experience in Cyber Security, Vulnerability Assessment and Penetration Testing, Cybercrime investigation, Digital Evidence seizure and Digital Forensics. He has been interviewed by several news channels, newspapers and magazines for Cyber Crime Safety and forensics.

Contact: +91 8010 6363 59, Email: ummadmeel@gmail.com

CONTENTS

Vol. 3. Issue 4 (2018)

1. Who Will Win The War Of Algorithms? Will It Be The Cyber Criminals? - Afrah Aamer	07
2. Digital Forensics And Information Security Of Art Objects In India - Dr.N.Kala	14
3. Network Forensics Analysis Using SIEM - Rashmi Joshi	24
4. CASB - Can Avoid Security Breach - Aman Chhikara	26
5. Need of Digital Forensic Proficiency - Dinesh N. Patil	28
6. Machine learning and AI in Cyber Security - Sainadh Jamalpur	33
7. Virtual Intelligence: The Ninth Family of Intelligences to be Added to Howard Gardner's List - Nadine Touzeau	35
8. Timeline Creation & Analysis using Plaso (Log2timeline) - Anshuman Sharma	43
9. Android Malware Forensics - Ummed Meel	48
10. LFI - Deepak S. Yadav	53
11. Open Source Intelligence (OSINT) - Aman	56
12. Blockchain Technology in Digital Forensic Investigation - Vinod Kumar Mishra	61
13. Detecting Digitally Edited Photos - Verifeyed - Yuwarn Ramachandren	64

INDIA'S 1ST DIGITAL FORENSIC JOURNAL

DIGITAL FORENSICS



f /d4n6j

@d4n6j

VOL 2 | ISSUE 4 | NOV 2018

Reg. No. DELEO/2017/73087

**Machine Learning &
AI in Cyber Security**

**Virtual
Intelligence**

ISSUE SPECIAL

**WAR OF
ALGORITHMS**

**NETWORK
FORENSIC
ANALYSIS
using SIEM**

**Digital Forensics &
Information Security of
ART Objects in India**

4N6

Rs. 250/-

www.digital4n6journal.com