

DIGITAL FORENSIC PROJECTS



DISCLAIMER



This document does not promote or encourage any illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.



MALWARE ANALYSIS & THREAT IDENTIFICATION

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



MALWARE ANALYSIS & THREAT IDENTIFICATION

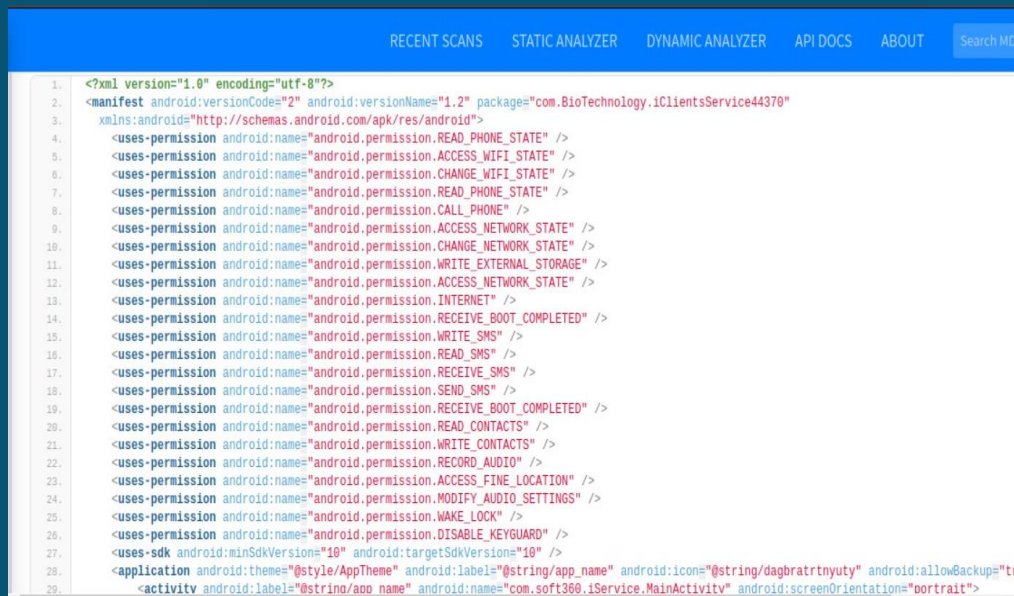
Project Name: Malware Analysis & Threat Identification

Tool Used: **Static Analysis:** Dex2Jar | JD-GUI | APKTool | **Dynamic Analysis:** Any.Run | IDA Pro | Cookoo SandBox

Platform: Windows

Implementation timeline: 20 Days

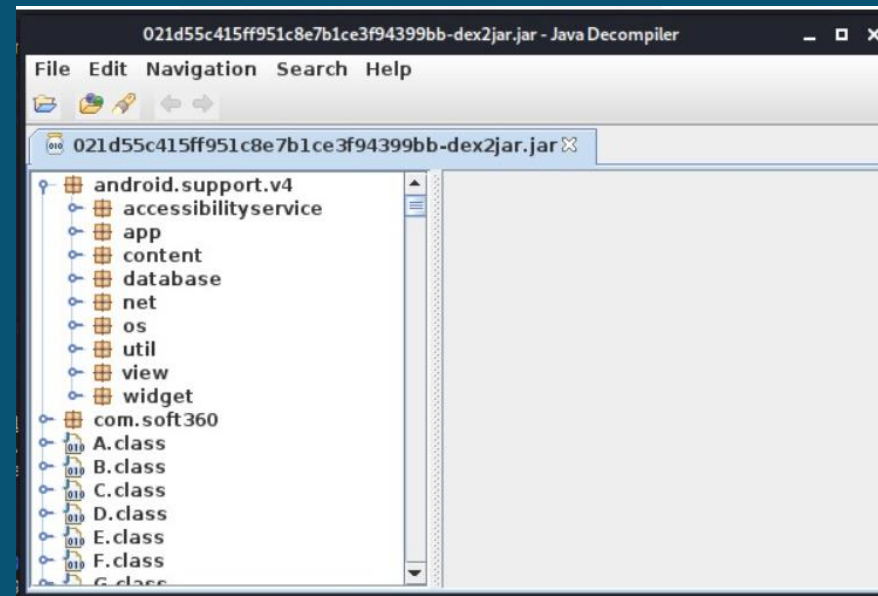
Work Around Existence: Any.run | Cookoo sandBox



```

1. <?xml version="1.0" encoding="utf-8"?>
2. <manifest android:versionCode="2" android:versionName="1.2" package="com.BioTechnology.iClientsService44370"
3.     xmlns:android="http://schemas.android.com/apk/res/android">
4.     <uses-permission android:name="android.permission.READ_PHONE_STATE" />
5.     <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
6.     <uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
7.     <uses-permission android:name="android.permission.READ_PHONE_STATE" />
8.     <uses-permission android:name="android.permission.CALL_PHONE" />
9.     <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
10.    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
11.    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
12.    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
13.    <uses-permission android:name="android.permission.INTERNET" />
14.    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
15.    <uses-permission android:name="android.permission.WRITE_SMS" />
16.    <uses-permission android:name="android.permission.READ_SMS" />
17.    <uses-permission android:name="android.permission.RECEIVE_SMS" />
18.    <uses-permission android:name="android.permission.SEND_SMS" />
19.    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
20.    <uses-permission android:name="android.permission.READ_CONTACTS" />
21.    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
22.    <uses-permission android:name="android.permission.RECORD_AUDIO" />
23.    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
24.    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS" />
25.    <uses-permission android:name="android.permission.WAKE_LOCK" />
26.    <uses-permission android:name="android.permission.DISABLE_KEYGUARD" />
27.    <uses-sdk android:minSdkVersion="10" android:targetSdkVersion="10" />
28.    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@string/dagbratrnuty" android:allowBackup="true"
29.        <activity android:label="@string/app_name" android:name="com.soft360.iService.MainActivity" android:screenOrientation="portrait">

```



021d55c415ff951c8e7b1ce3f94399bb-dex2jar.jar - Java Decompiler

File Edit Navigation Search Help

021d55c415ff951c8e7b1ce3f94399bb-dex2jar.jar

- android.support.v4
 - accessibilityservice
 - app
 - content
 - database
 - net
 - os
 - util
 - view
 - widget
- com.soft360
 - A.class
 - B.class
 - C.class
 - D.class
 - E.class
 - F.class

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



MALWARE ANALYSIS

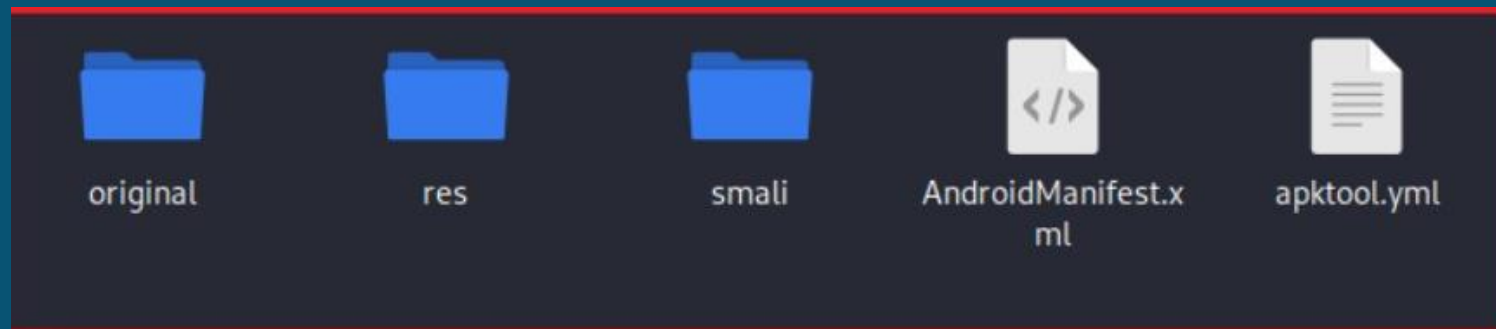
& THREAT IDENTIFICATION | PROJECT WORK FLOW (1/3)

Static Analysis:

Two approaches for static analysis i.e. is using tools like Apktool, Dex2jar and JD-GUI.

1. Apktool is used to decompile the APK.

```
(kali@kali)=[~/Downloads]
└─$ apktool d 021d55c415ff951c8e7b1ce3f94399bb.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty on 021d55c415ff951c8e7b1ce3f94399bb.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/kali/.local/share/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 ...
```



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



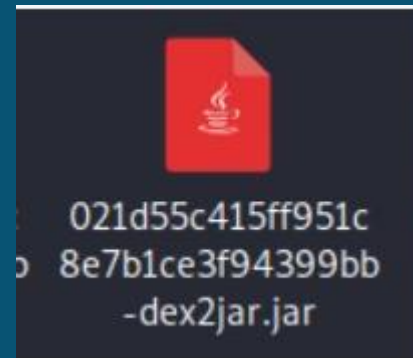
MALWARE ANALYSIS

& THREAT IDENTIFICATION | PROJECT WORK FLOW (2/3)

Static Analysis:

2. Dex2Jar used to convert APK to .jar format .

```
(kali@kali) - [~/Downloads]
└─$ d2j-dex2jar 021d55c415ff951c8e7b1ce3f94399bb.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
dex2jar 021d55c415ff951c8e7b1ce3f94399bb.apk → ./021d55c415ff951c8e7b1ce3f94399bb-dex2jar.jar
```

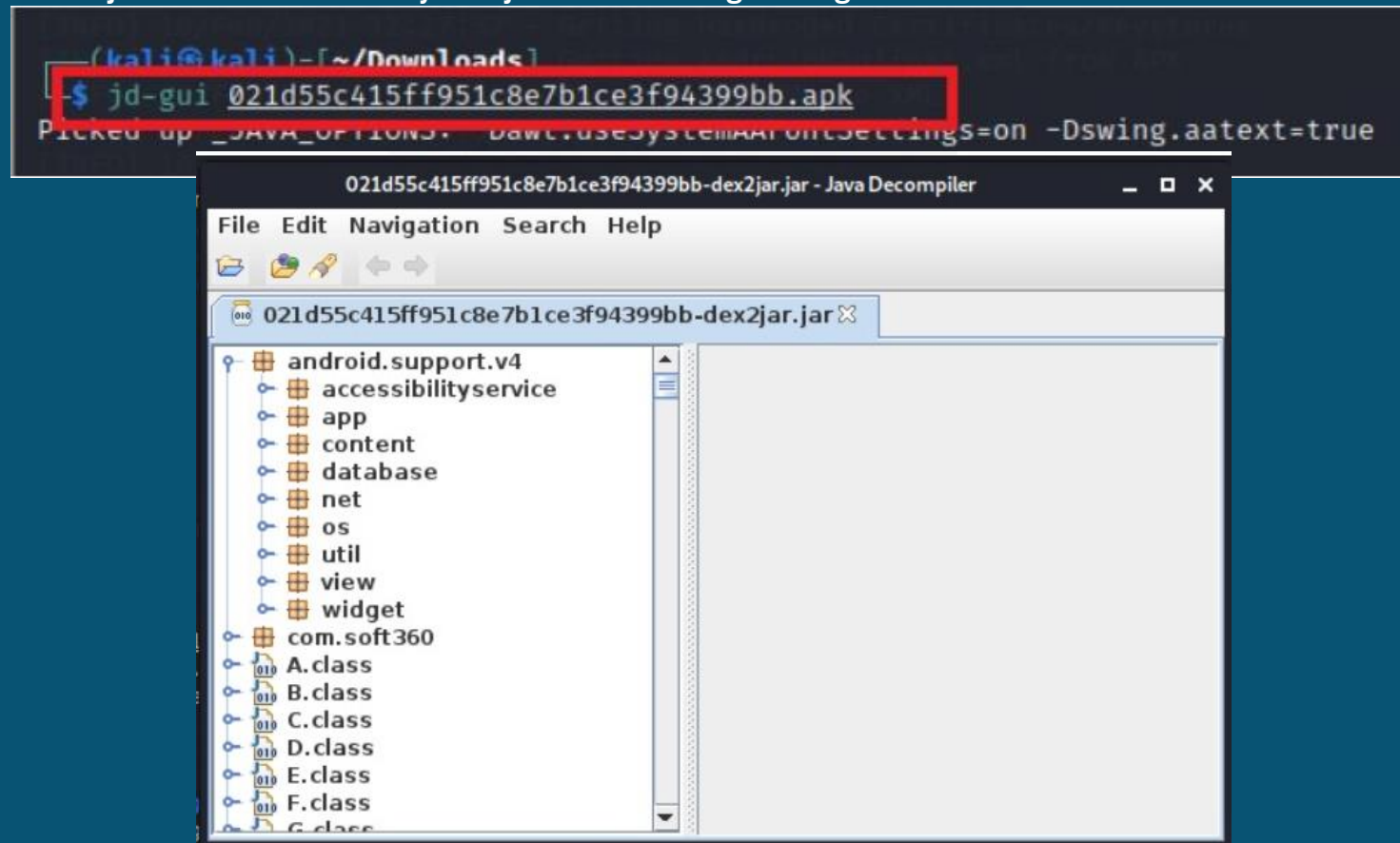


MALWARE ANALYSIS

& THREAT IDENTIFICATION | PROJECT WORK FLOW (3/3)

Static Analysis:

3. Using Jd-GUI to load the .jar format file created by dex2jar for reverse engineering.



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

