Malicious APK File Analysis
No. 5

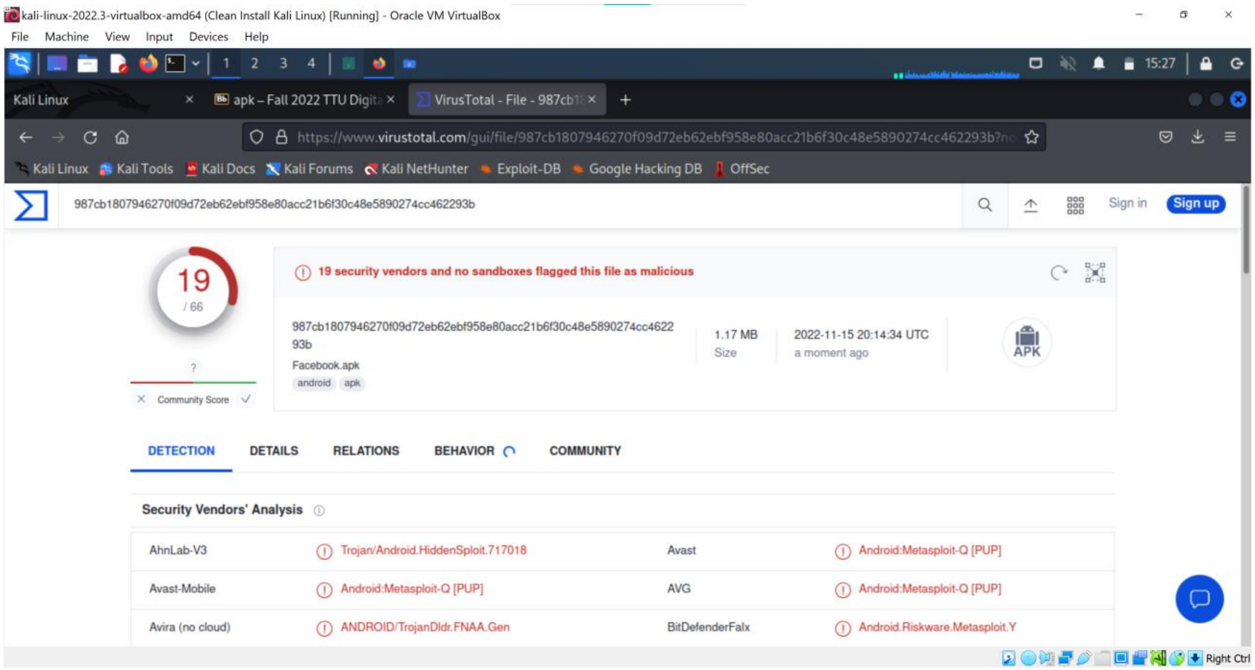
In this Assignment 2 phase 2, we did 3 distinct tasks. The first task was running the APK file through virus total to see what was detected and by how many different security vendors.

The second task was decompiling the APK file and looking at the code looking at the code to investigate the malicious content and discover our secret key. Finally, we performed some analysis using a sandbox.

A) Virus Total Screening

When running the APK through virus total, we got a score of 19/66 which indicates the presence of malware. When looking at why it was flagged. When can notice that Android Trojan, Android Backdoor are used to describe why it was flagged as malicious.

Thus, we think that this malware might result in some process injection, giving remote access to a specific IP address on the infected device as soon as the apk file is opened.



https://www.virustotal.com/gui/file/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b?n

987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b

19 / 66

19 security vendors and no sandboxes flagged this file as malicious

987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
93b
Facebook.apk
android apk

1.17 MB
Size

2022-11-15 20:14:34 UTC
a moment ago

APK

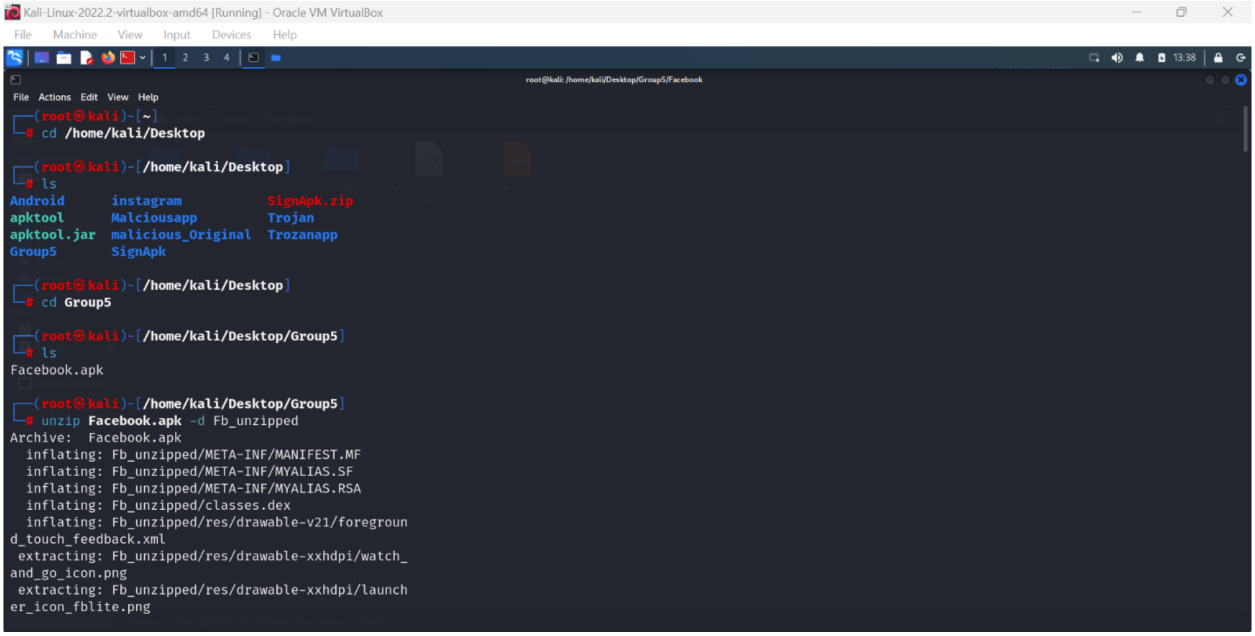
Security Vendors' Analysis

AhnLab-V3	Trojan/Android.HiddenSploit.717018	Avast	Android:Metasploit-Q [PUP]
Avast-Mobile	Android:Metasploit-Q [PUP]	AVG	Android:Metasploit-Q [PUP]
Avira (no cloud)	ANDROID/TrojanDldr.FNAA.Gen	BitDefenderFalx	Android.Riskware.Metasploit.Y

Figure 1: Virus total scan

B) Investigating the code

The Facebook.apk file is unzipped using the command : unzip Facebook.apk -d Fb_unzipped.

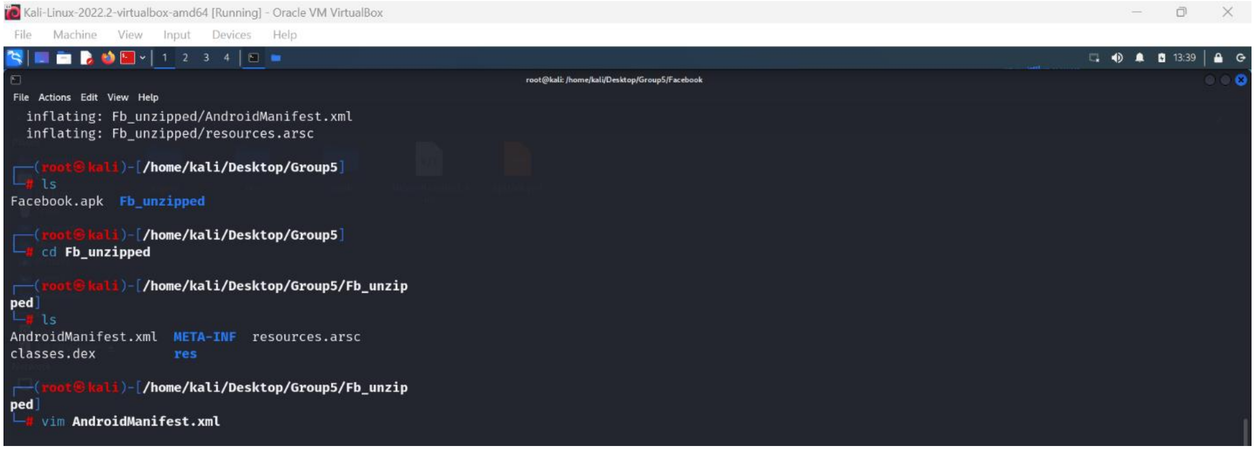


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Group5/Facebook
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# cd /home/kali/Desktop

┌──(root㉿kali)-[/home/kali/Desktop]
└─# ls
Android      instagram          SignApk.zip
apktool      Malciousapp        Trojan
apktool.jar  malicious_Original Trozanapp
Group5       SignApk

┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd Group5

┌──(root㉿kali)-[/home/kali/Desktop/Group5]
└─# ls
Facebook.apk

┌──(root㉿kali)-[/home/kali/Desktop/Group5]
└─# unzip Facebook.apk -d Fb_unzipped
Archive:  Facebook.apk
  inflating: Fb_unzipped/META-INF/MANIFEST.MF
  inflating: Fb_unzipped/META-INF/MYALIAS.SF
  inflating: Fb_unzipped/META-INF/MYALIAS.RSA
  inflating: Fb_unzipped/classes.dex
  inflating: Fb_unzipped/res/drawable-v21/foregroun
d_touch_feedback.xml
 extracting: Fb_unzipped/res/drawable-xxhdpi/watch_
and_go_icon.png
 extracting: Fb_unzipped/res/drawable-xxhdpi/launch
er_icon_fblite.png
```

Figure 2: Unzip the APK file

After the file unzip the xml file,resources.arsc,res,classes.dex,META-INF are created.

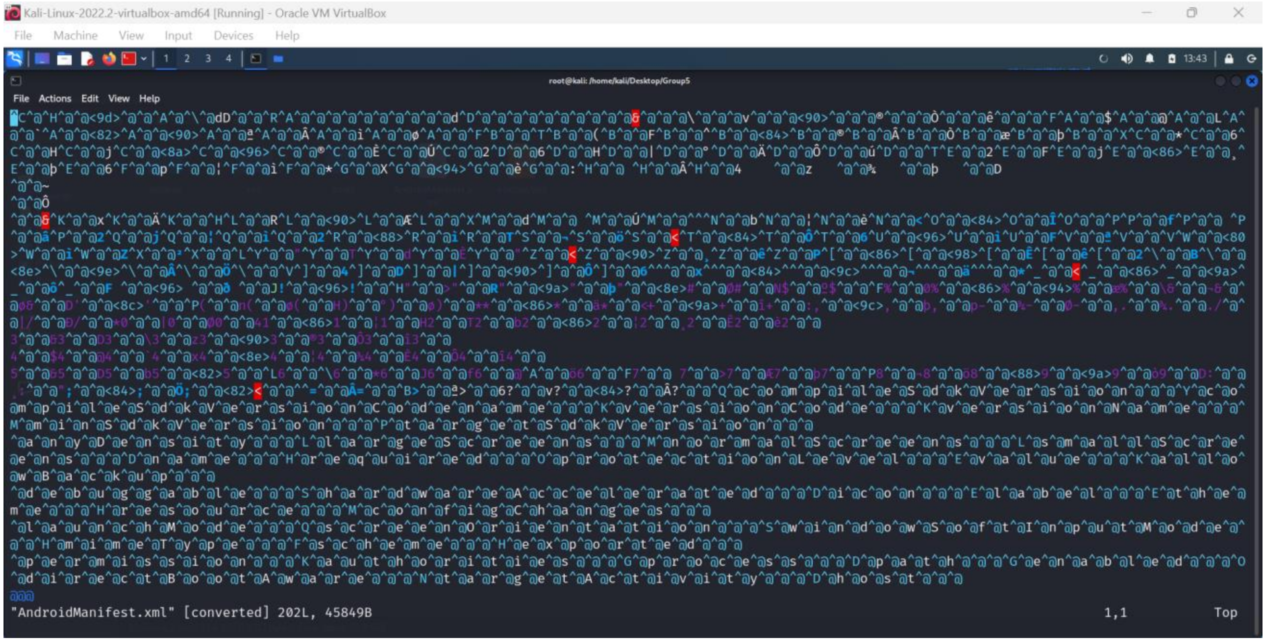


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Group5/Facebook
File Actions Edit View Help

```
  inflating: Fb_unzipped/AndroidManifest.xml
  inflating: Fb_unzipped/resources.arsc

┌──(root㉿kali)-[/home/kali/Desktop/Group5]
└─# ls
Facebook.apk  Fb_unzipped

┌──(root㉿kali)-[/home/kali/Desktop/Group5]
└─# cd Fb_unzipped

┌──(root㉿kali)-[/home/kali/Desktop/Group5/Fb_unzip
ped]
└─# ls
AndroidManifest.xml  META-INF  resources.arsc
classes.dex          res

┌──(root㉿kali)-[/home/kali/Desktop/Group5/Fb_unzip
ped]
└─# vim AndroidManifest.xml
```

Figure 3: Components in the unzipped file

When the AndroidManifest.xml file is opened it is in an unreadable format.

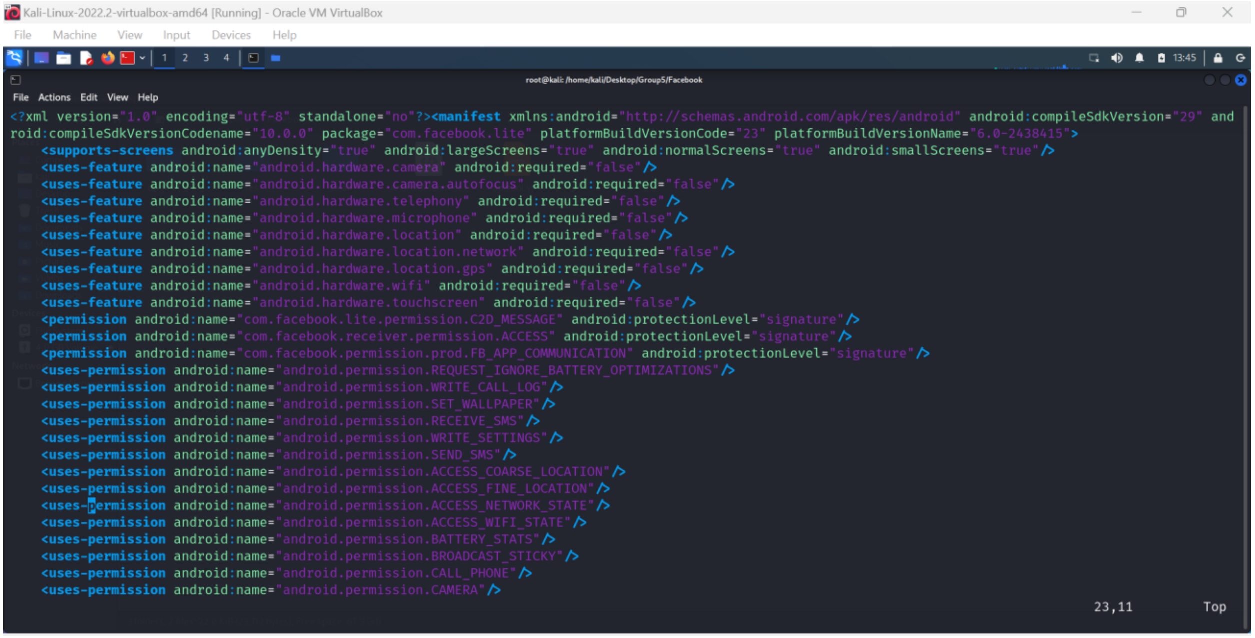


Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Group5
File Actions Edit View Help

```
"AndroidManifest.xml" [converted] 202L, 45849B                                              1,1           Top
```

Figure 4: Android Manifest.xml

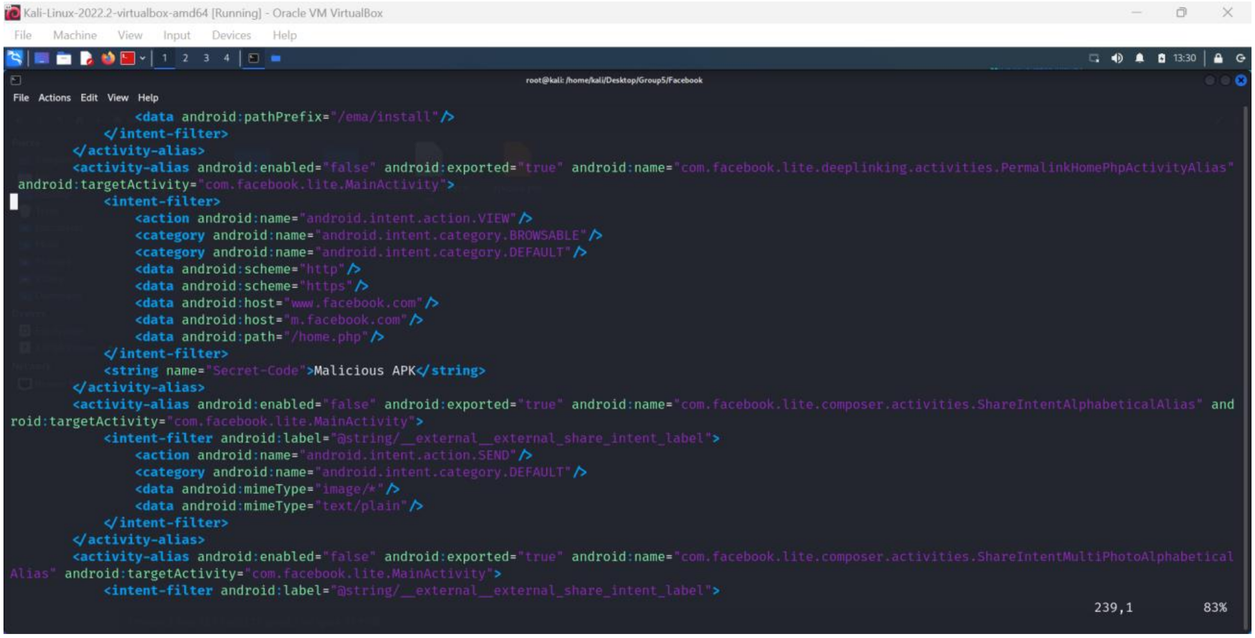
We use the command: java -jar apktool.jar d /home/kali/Desktop/Group5/Facebook.apk -f and path name of apk file to decompile and deobfuscate our APK.



Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Group5/Facebook
File Actions Edit View Help

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="29" and
roid:compileSdkVersionCodename="10.0.0" package="com.facebook.lite" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
    <supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true" android:smallScreens="true"/>
    <uses-feature android:name="android.hardware.camera" android:required="false"/>
    <uses-feature android:name="android.hardware.camera.autofocus" android:required="false"/>
    <uses-feature android:name="android.hardware.telephony" android:required="false"/>
    <uses-feature android:name="android.hardware.microphone" android:required="false"/>
    <uses-feature android:name="android.hardware.location" android:required="false"/>
    <uses-feature android:name="android.hardware.location.network" android:required="false"/>
    <uses-feature android:name="android.hardware.location.gps" android:required="false"/>
    <uses-feature android:name="android.hardware.wifi" android:required="false"/>
    <uses-feature android:name="android.hardware.touchscreen" android:required="false"/>
    <permission android:name="com.facebook.lite.permission.C2D_MESSAGE" android:protectionLevel="signature"/>
    <permission android:name="com.facebook.receiver.permission.ACCESS" android:protectionLevel="signature"/>
    <permission android:name="com.facebook.permission.prod.FB_APP_COMMUNICATION" android:protectionLevel="signature"/>
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
    <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.BATTERY_STATS"/>
    <uses-permission android:name="android.permission.BROADCAST_STICKY"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.CAMERA"/>
                                                                                                 23,11         Top
```

Figure 5: Android Manifest.xml and its permissions



Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Desktop/Group5/Facebook
File Actions Edit View Help

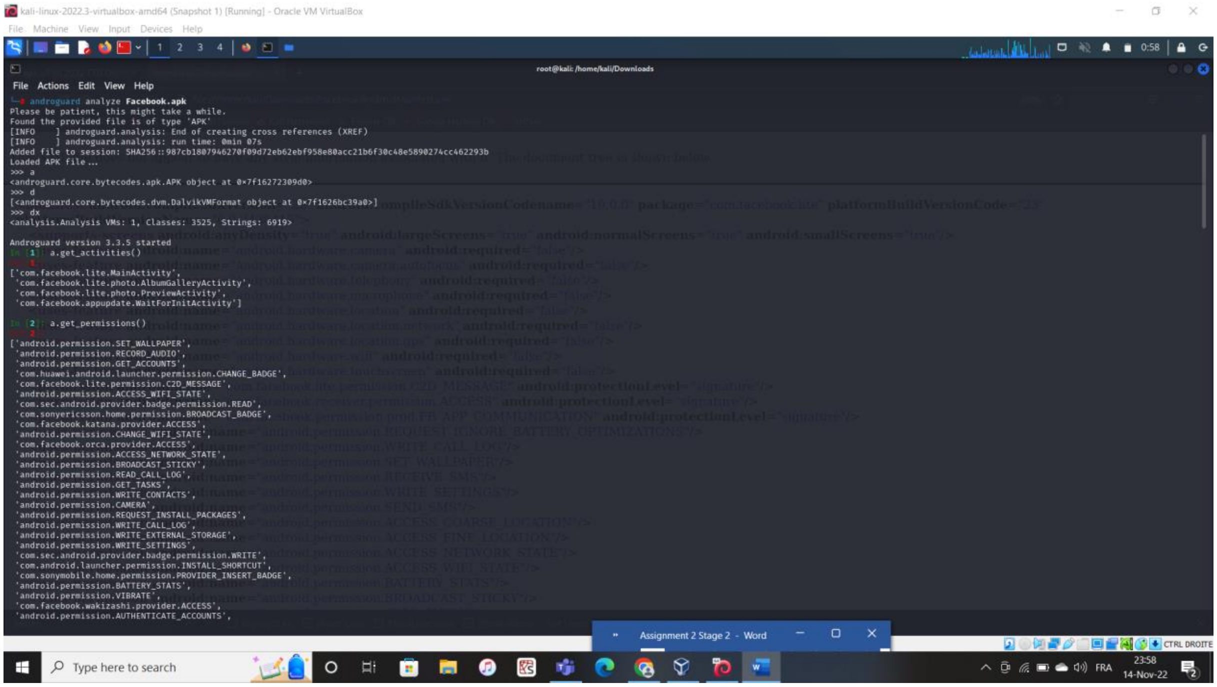
```
                <data android:pathPrefix="/ema/install"/>
            </intent-filter>
        </activity-alias>
        <activity-alias android:enabled="false" android:exported="true" android:name="com.facebook.lite.deeplinking.activities.PermalinkHomePhpActivityAlias"
 android:targetActivity="com.facebook.lite.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <data android:scheme="http"/>
                <data android:scheme="https"/>
                <data android:host="www.facebook.com"/>
                <data android:host="m.facebook.com"/>
                <data android:path="/home.php"/>
            </intent-filter>
            <string name="Secret-Code">Malicious APK</string>
        </activity-alias>
        <activity-alias android:enabled="false" android:exported="true" android:name="com.facebook.lite.composer.activities.ShareIntentAlphabeticalAlias" and
roid:targetActivity="com.facebook.lite.MainActivity">
            <intent-filter android:label="@string/__external__external_share_intent_label">
                <action android:name="android.intent.action.SEND"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <data android:mimeType="image/*"/>
                <data android:mimeType="text/plain"/>
            </intent-filter>
        </activity-alias>
        <activity-alias android:enabled="false" android:exported="true" android:name="com.facebook.lite.composer.activities.ShareIntentMultiPhotoAlphabetical
Alias" android:targetActivity="com.facebook.lite.MainActivity">
            <intent-filter android:label="@string/__external__external_share_intent_label">
                                                                                          239,1         83%
```

Figure 6: Secret Code found!

The secret code: Malicious APK

C) Sandbox Analysis

Using Androguard, let's analyze these permissions and view their individual risk levels.



kali-linux-2022.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Downloads
File Actions Edit View Help
Assignment 2 Stage 2 - Word
Type here to search
CTRL DROITE
FRA
23:58
14-Nov-22

```
└─$ androguard analyze Facebook.apk
Please be patient, this might take a while.
Found the provided file is of type 'APK'
[INFO    ] androguard.analysis: End of creating cross references (XREF)
[INFO    ] androguard.analysis: run time: 0min 07s
Added file to session: SHA256::987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b
Loaded APK file...
>>> a
<androguard.core.bytecodes.apk.APK object at 0×7f16272309d0>
>>> d
[<androguard.core.bytecodes.dvm.DalvikVMFormat object at 0×7f1626bc39a0>]
>>> dx
<analysis.Analysis VMs: 1, Classes: 3525, Strings: 6919>

Androguard version 3.3.5 started
In [1]: a.get_activities()
Out[1]:
['com.facebook.lite.MainActivity',
 'com.facebook.lite.photo.AlbumGalleryActivity',
 'com.facebook.lite.photo.PreviewActivity',
 'com.facebook.appupdate.WaitForInitActivity']

In [2]: a.get_permissions()
Out[2]:
['android.permission.SET_WALLPAPER',
 'android.permission.RECORD_AUDIO',
 'android.permission.GET_ACCOUNTS',
 'com.huawei.android.launcher.permission.CHANGE_BADGE',
 'com.facebook.lite.permission.C2D_MESSAGE',
 'android.permission.ACCESS_WIFI_STATE',
 'com.sec.android.provider.badge.permission.READ',
 'com.sonyericsson.home.permission.BROADCAST_BADGE',
 'com.facebook.katana.provider.ACCESS',
 'android.permission.CHANGE_WIFI_STATE',
 'com.facebook.orca.provider.ACCESS',
 'android.permission.ACCESS_NETWORK_STATE',
 'android.permission.BROADCAST_STICKY',
 'android.permission.READ_CALL_LOG',
 'android.permission.GET_TASKS',
 'android.permission.WRITE_CONTACTS',
 'android.permission.CAMERA',
 'android.permission.REQUEST_INSTALL_PACKAGES',
 'android.permission.WRITE_CALL_LOG',
 'android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.WRITE_SETTINGS',
 'com.sec.android.provider.badge.permission.WRITE',
 'com.android.launcher.permission.INSTALL_SHORTCUT',
 'com.sonymobile.home.permission.PROVIDER_INSERT_BADGE',
 'android.permission.BATTERY_STATS',
 'android.permission.VIBRATE',
 'com.facebook.wakizashi.provider.ACCESS',
 'android.permission.AUTHENTICATE_ACCOUNTS',
```

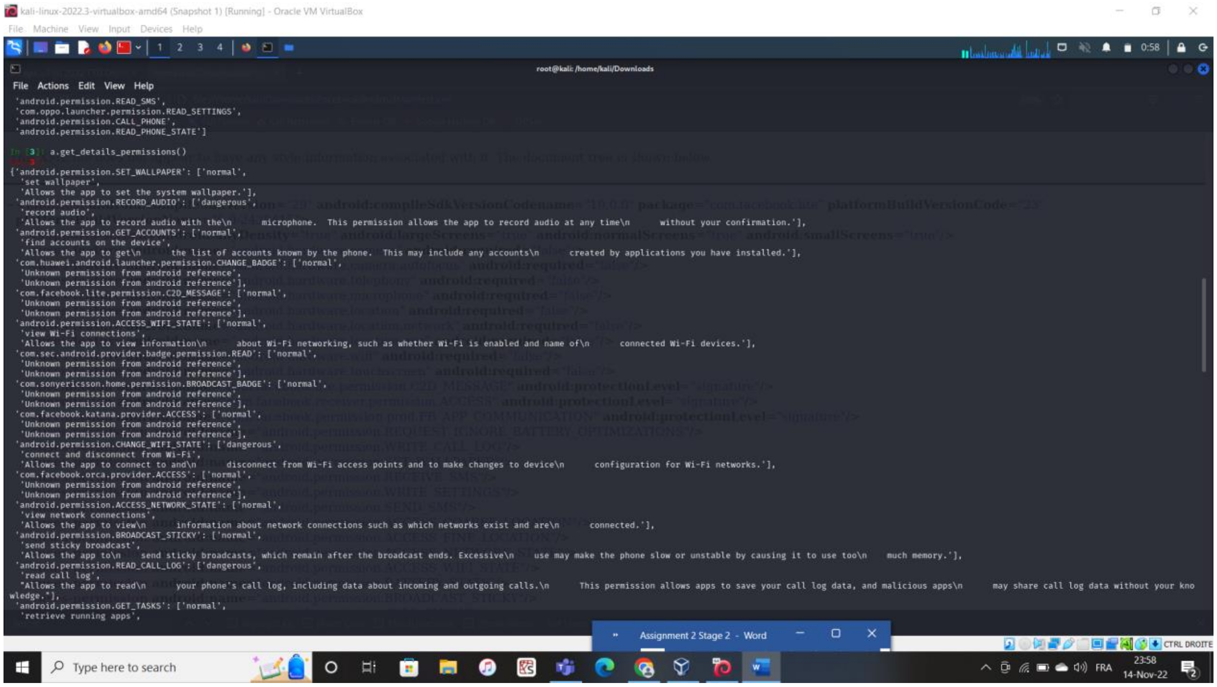
Figure 7: Analyze APK with Androguard

The APK file has 3525 classes and 4 activities:

- Main
- AlbumGalleryActivity
- PreviewActivity
- WaitforInitActivity

The WaitforInit activity seems a bit vague.

Let’s review the permissions with Androguard.



kali-linux-2022.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Downloads
File Actions Edit View Help
Assignment 2 Stage 2 - Word
Type here to search
FRA
23:58
14-Nov-22

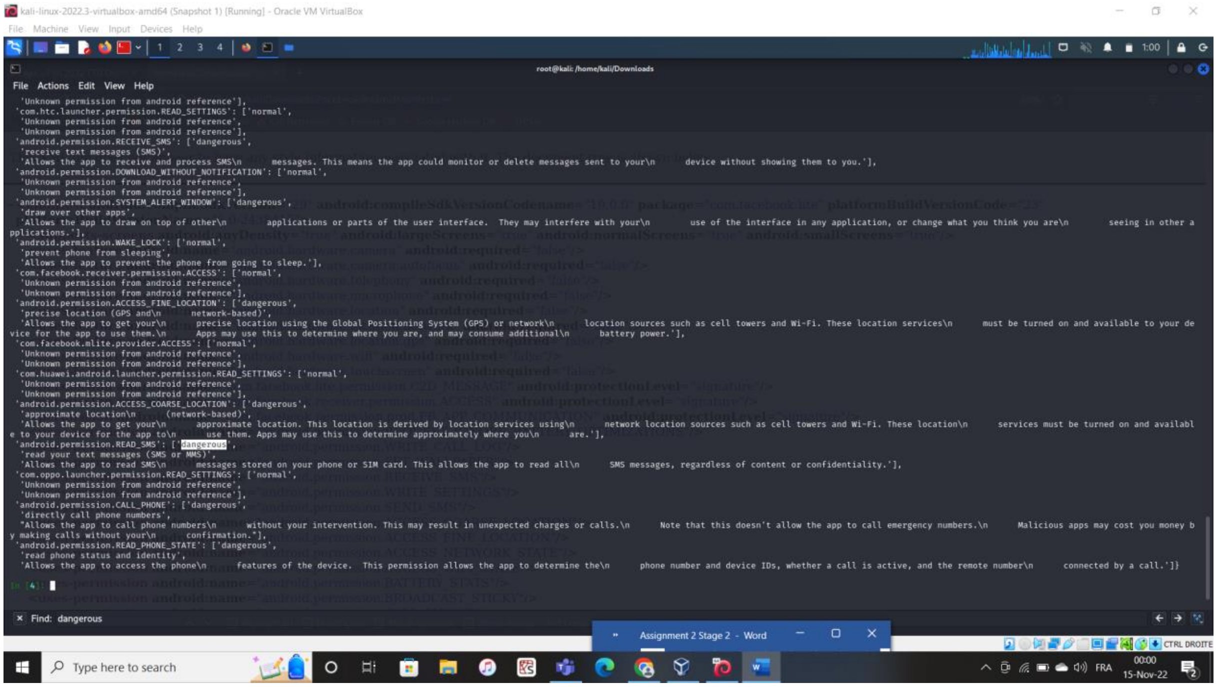
```
 'android.permission.READ_SMS',
 'com.oppo.launcher.permission.READ_SETTINGS',
 'android.permission.CALL_PHONE',
 'android.permission.READ_PHONE_STATE']

In [3]: a.get_details_permissions()
Out[3]:
{'android.permission.SET_WALLPAPER': ['normal',
  'set wallpaper',
  'Allows the app to set the system wallpaper.'],
 'android.permission.RECORD_AUDIO': ['dangerous',
  'record audio',
  'Allows the app to record audio with the\n      microphone.  This permission allows the app to record audio at any time\n      without your confirmation.'],
 'android.permission.GET_ACCOUNTS': ['normal',
  'find accounts on the device',
  'Allows the app to get\n      the list of accounts known by the phone.  This may include any accounts\n      created by applications you have installed.'],
 'com.huawei.android.launcher.permission.CHANGE_BADGE': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'com.facebook.lite.permission.C2D_MESSAGE': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.ACCESS_WIFI_STATE': ['normal',
  'view Wi-Fi connections',
  'Allows the app to view information\n      about Wi-Fi networking, such as whether Wi-Fi is enabled and name of\n      connected Wi-Fi devices.'],
 'com.sec.android.provider.badge.permission.READ': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'com.sonyericsson.home.permission.BROADCAST_BADGE': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'com.facebook.katana.provider.ACCESS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.CHANGE_WIFI_STATE': ['dangerous',
  'connect and disconnect from Wi-Fi',
  'Allows the app to connect to and\n      disconnect from Wi-Fi access points and to make changes to device\n      configuration for Wi-Fi networks.'],
 'com.facebook.orca.provider.ACCESS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.ACCESS_NETWORK_STATE': ['normal',
  'view network connections',
  'Allows the app to view\n      information about network connections such as which networks exist and are\n      connected.'],
 'android.permission.BROADCAST_STICKY': ['normal',
  'send sticky broadcast',
  'Allows the app to\n    send sticky broadcasts, which remain after the broadcast ends. Excessive\n    use may make the phone slow or unstable by causing it to use too\n    much memory.'],
 'android.permission.READ_CALL_LOG': ['dangerous',
  'read call log',
  "Allows the app to read\n      your phone's call log, including data about incoming and outgoing calls.\n      This permission allows apps to save your call log data, and malicious apps\n      may share call log data without your kno
wledge."],
 'android.permission.GET_TASKS': ['normal',
  'retrieve running apps',
```

Figure 8: Get permission details

Some of these permissions have been flagged as dangerous:

- The malicious app can record audio without permission, this is a dangerous permission
- It can also change the WiFi state at will, an attacker would take advantage of this.
- It can also read the call log
- The app can monitor and change or delete messages that come into the phone without showing them to the user.
- The app can also access your precise location
- It can access the phone features of the device.

These are all features that are unnecessary to a Social Media application.

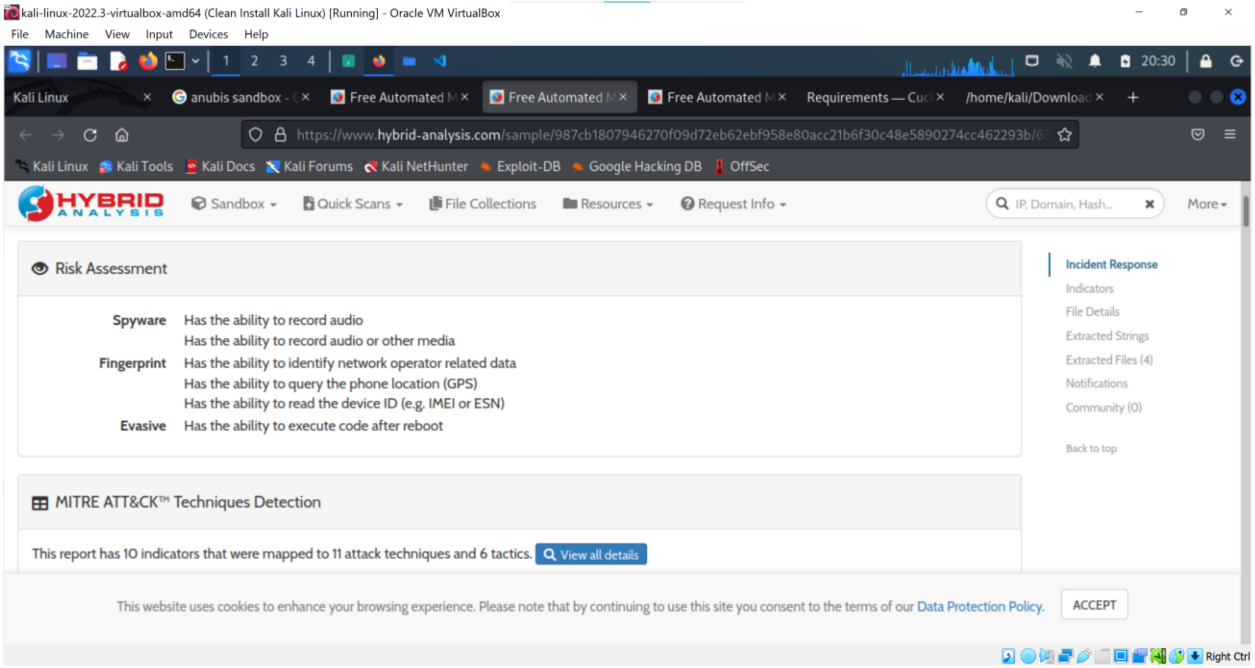

kali-linux-2022.3-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/Downloads
File Actions Edit View Help
Find: dangerous
Assignment 2 Stage 2 - Word
Type here to search
FRA
00:00
15-Nov-22

```
  'Unknown permission from android reference'],
 'com.htc.launcher.permission.READ_SETTINGS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.RECEIVE_SMS': ['dangerous',
  'receive text messages (SMS)',
  'Allows the app to receive and process SMS\n       messages. This means the app could monitor or delete messages sent to your\n       device without showing them to you.'],
 'android.permission.DOWNLOAD_WITHOUT_NOTIFICATION': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.SYSTEM_ALERT_WINDOW': ['dangerous',
  'draw over other apps',
  'Allows the app to draw on top of other\n        applications or parts of the user interface.  They may interfere with your\n        use of the interface in any application, or change what you think you are\n        seeing in other a
pplications.'],
 'android.permission.WAKE_LOCK': ['normal',
  'prevent phone from sleeping',
  'Allows the app to prevent the phone from going to sleep.'],
 'com.facebook.receiver.permission.ACCESS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.ACCESS_FINE_LOCATION': ['dangerous',
  'precise location (GPS and\n      network-based)',
  'Allows the app to get your\n      precise location using the Global Positioning System (GPS) or network\n      location sources such as cell towers and Wi-Fi. These location services\n      must be turned on and available to your de
vice for the app to use them.\n      Apps may use this to determine where you are, and may consume additional\n      battery power.'],
 'com.facebook.mlite.provider.ACCESS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'com.huawei.android.launcher.permission.READ_SETTINGS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.ACCESS_COARSE_LOCATION': ['dangerous',
  'approximate location\n      (network-based)',
  'Allows the app to get your\n      approximate location. This location is derived by location services using\n      network location sources such as cell towers and Wi-Fi. These location\n      services must be turned on and availabl
e to your device for the app to\n      use them. Apps may use this to determine approximately where you\n      are.'],
 'android.permission.READ_SMS': ['dangerous',
  'read your text messages (SMS or MMS)',
  'Allows the app to read SMS\n      messages stored on your phone or SIM card. This allows the app to read all\n      SMS messages, regardless of content or confidentiality.'],
 'com.oppo.launcher.permission.READ_SETTINGS': ['normal',
  'Unknown permission from android reference',
  'Unknown permission from android reference'],
 'android.permission.CALL_PHONE': ['dangerous',
  'directly call phone numbers',
  "Allows the app to call phone numbers\n      without your intervention. This may result in unexpected charges or calls.\n      Note that this doesn't allow the app to call emergency numbers.\n      Malicious apps may cost you money b
y making calls without your\n      confirmation."],
 'android.permission.READ_PHONE_STATE': ['dangerous',
  'read phone status and identity',
  'Allows the app to access the phone\n      features of the device.  This permission allows the app to determine the\n      phone number and device IDs, whether a call is active, and the remote number\n      connected by a call.']}

In [4]: 
```

Figure 9: Get Permission Details

For a more in-depth analysis, let's analyze this file using a sandbox.

Just as we identified, we see that the APK has the permissions listed in the image below:


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
anubis sandbox -
Free Automated M
Free Automated M
Free Automated M
Requirements — Cuc
/home/kali/Download
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b/6
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID ANALYSIS
Sandbox Quick Scans File Collections Resources Request Info
IP, Domain, Hash...
More
Incident Response
Indicators
File Details
Extracted Strings
Extracted Files (4)
Notifications
Community (0)
Back to top
View all details
ACCEPT
20:30
Right Ctrl

Risk Assessment

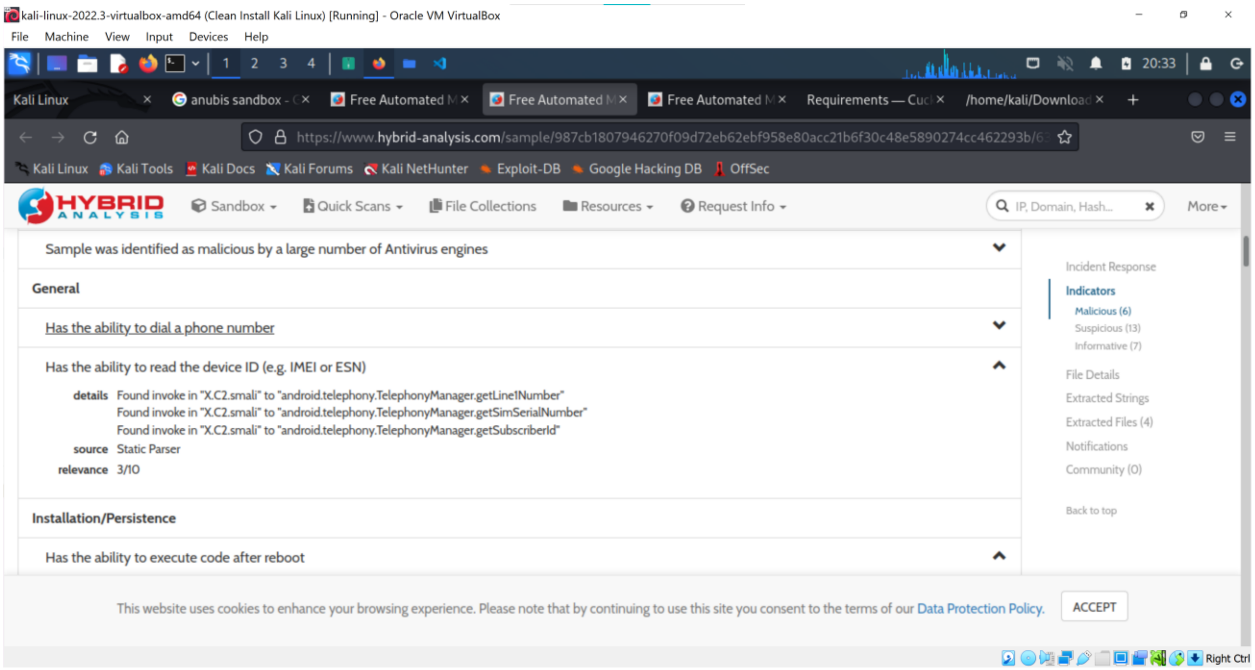
Spyware	Has the ability to record audio Has the ability to record audio or other media
Fingerprint	Has the ability to identify network operator related data Has the ability to query the phone location (GPS) Has the ability to read the device ID (e.g. IMEI or ESN)
Evasive	Has the ability to execute code after reboot

MITRE ATT&CK™ Techniques Detection

This report has 10 indicators that were mapped to 11 attack techniques and 6 tactics.

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Policy.

Figure 10: Sandbox Analysis - Malicious indicators



kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b/6
Sandbox
Quick Scans
File Collections
Resources
Request Info
More
Incident Response
Indicators
Malicious (6)
Suspicious (13)
Informative (7)
File Details
Extracted Strings
Extracted Files (4)
Notifications
Community (0)
Back to top
ACCEPT

Sample was identified as malicious by a large number of Antivirus engines

General

Has the ability to dial a phone number

Has the ability to read the device ID (e.g. IMEI or ESN)

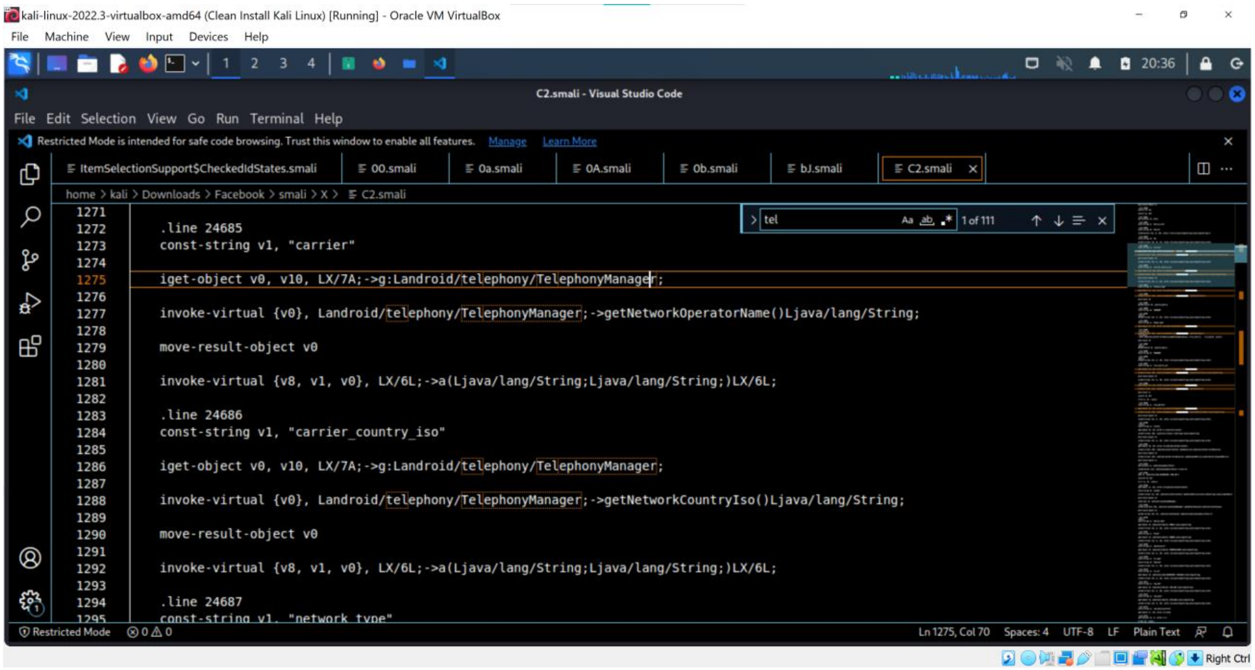
details Found invoke in "X.C2.smali" to "android.telephony.TelephonyManager.getLine1Number"
Found invoke in "X.C2.smali" to "android.telephony.TelephonyManager.getSimSerialNumber"
Found invoke in "X.C2.smali" to "android.telephony.TelephonyManager.getSubscriberId"
source Static Parser
relevance 3/10

Installation/Persistence

Has the ability to execute code after reboot

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Policy.

Figure 11: The APK can dial a phone number, this is dangerous

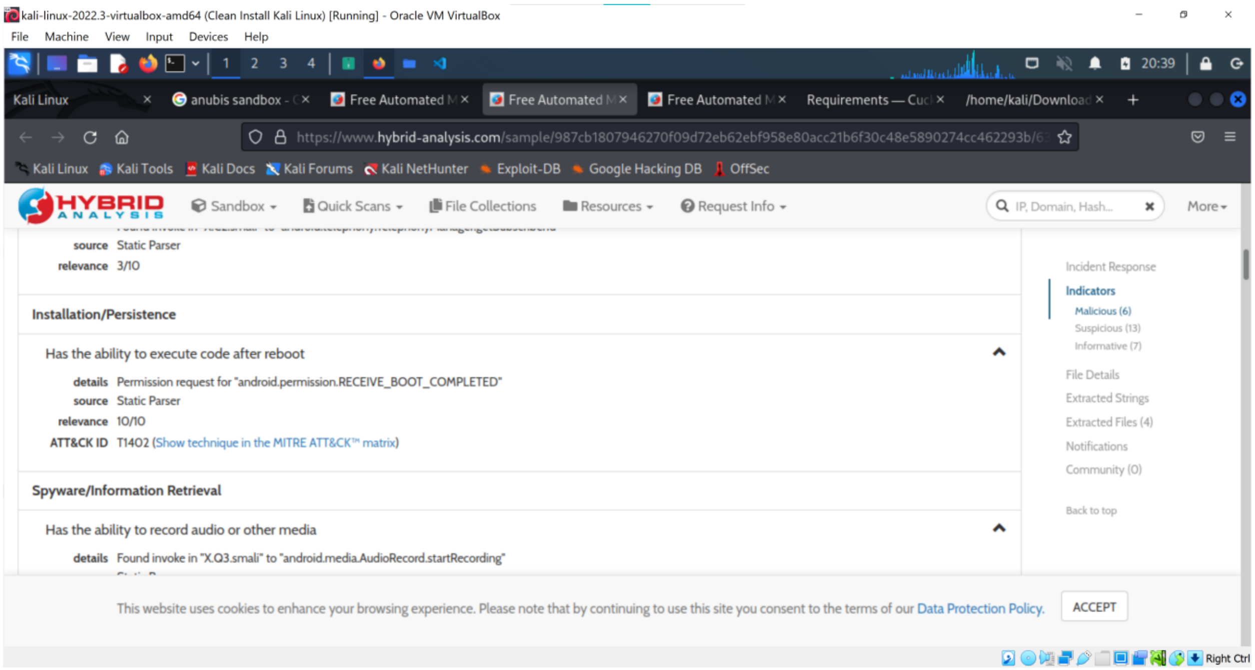


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
C2.smali - Visual Studio Code
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
ItemSelectionSupport$CheckedIdStates.smali
00.smali
0a.smali
0A.smali
0b.smali
bJ.smali
C2.smali
home > kali > Downloads > Facebook > smali > X > C2.smali
tel
1 of 111
Restricted Mode
Ln 1275, Col 70 Spaces: 4 UTF-8 LF Plain Text

```

    .line 24685
    const-string v1, "carrier"

    iget-object v0, v10, LX/7A;->g:Landroid/telephony/TelephonyManager;

    invoke-virtual {v0}, Landroid/telephony/TelephonyManager;->getNetworkOperatorName()Ljava/lang/String;

    move-result-object v0

    invoke-virtual {v8, v1, v0}, LX/6L;->a(Ljava/lang/String;Ljava/lang/String;)LX/6L;

    .line 24686
    const-string v1, "carrier_country_iso"

    iget-object v0, v10, LX/7A;->g:Landroid/telephony/TelephonyManager;

    invoke-virtual {v0}, Landroid/telephony/TelephonyManager;->getNetworkCountryIso()Ljava/lang/String;

    move-result-object v0

    invoke-virtual {v8, v1, v0}, LX/6L;->a(Ljava/lang/String;Ljava/lang/String;)LX/6L;

    .line 24687
    const-string v1, "network_type"
```

Figure 12: X.C2.smali file

This permission is added discreetly and the APK can then dial phone numbers without permission. This is very dangerous and beyond the necessities for a social media application.



source Static Parser
relevance 3/10

Installation/Persistence

Has the ability to execute code after reboot

details Permission request for "android.permission.RECEIVE_BOOT_COMPLETED"
source Static Parser
relevance 10/10
ATT&CK ID T1402 (Show technique in the MITRE ATT&CK™ matrix)

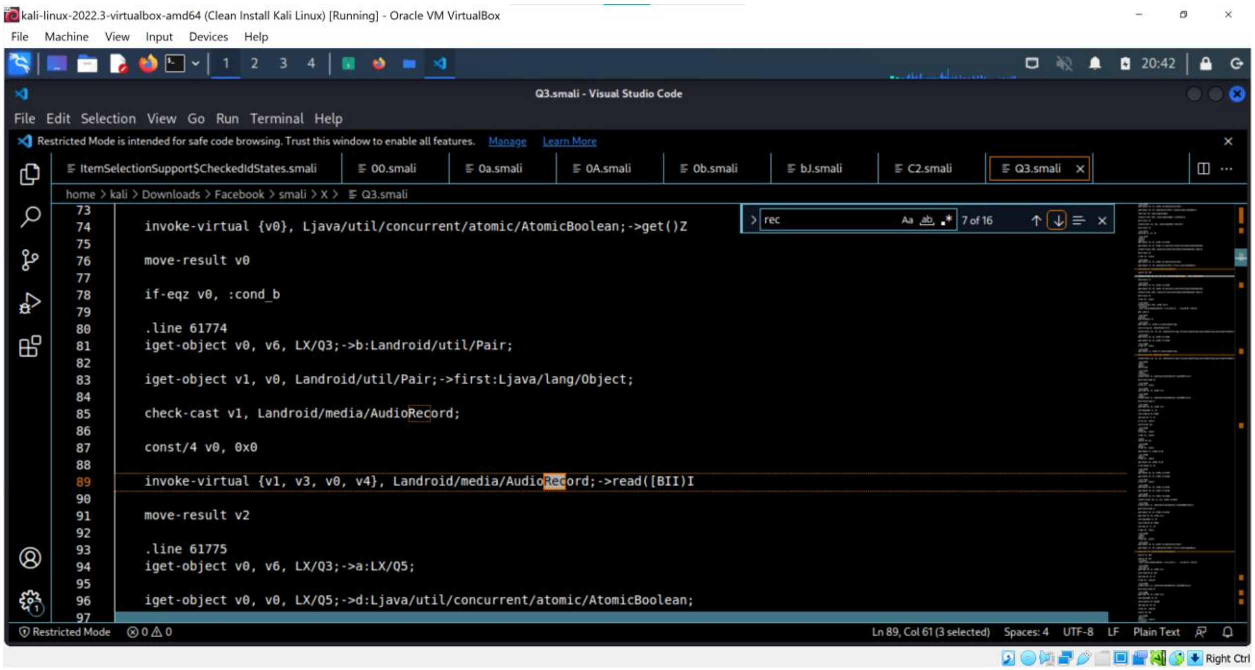
Spyware/Information Retrieval

Has the ability to record audio or other media

details Found invoke in "X.Q3.smali" to "android.media.AudioRecord.startRecording"

This website uses cookies to enhance your browsing experience. Please note that by continuing to use this site you consent to the terms of our Data Protection Policy.

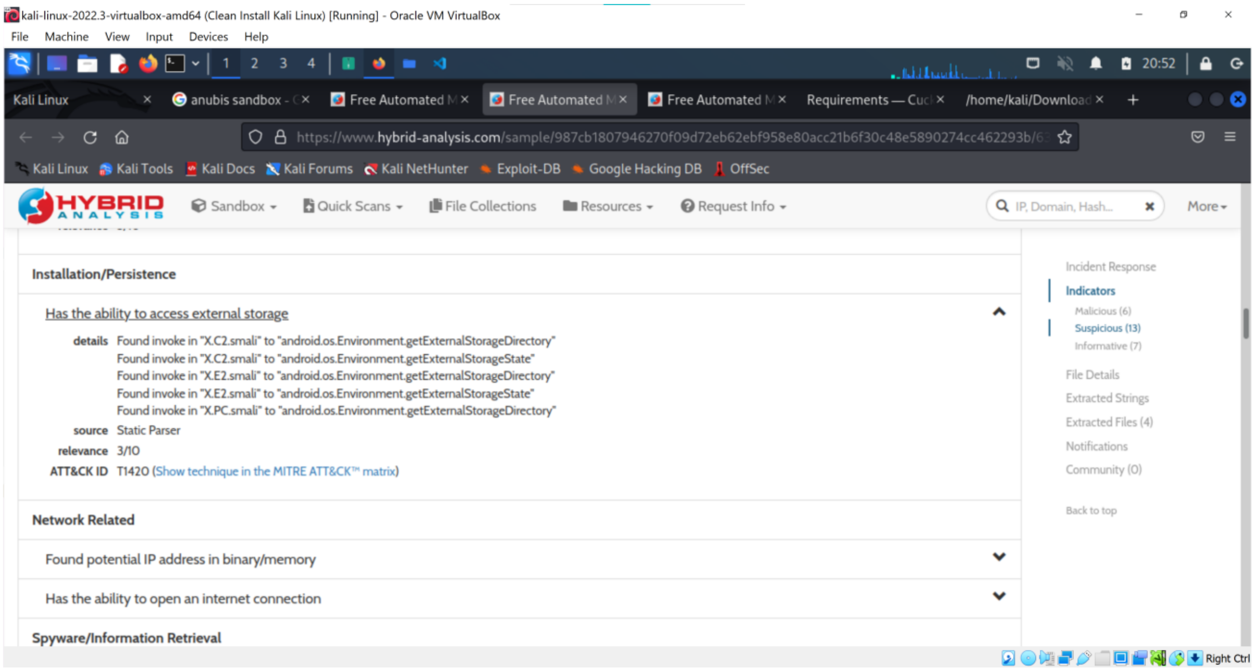
Figure 13: The APK can also execute code upon reboot and record media - malicious


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
20:42
Q3.smali - Visual Studio Code
File Edit Selection View Go Run Terminal Help
Manage
Learn More
ItemSelectionSupport$CheckedIdStates.smali
00.smali
0a.smali
0A.smali
0b.smali
bJ.smali
C2.smali
Q3.smali
home > kali > Downloads > Facebook > smali > X > Q3.smali
rec
7 of 16
Restricted Mode
0 0
Ln 89, Col 61 (3 selected)
Spaces: 4
UTF-8
LF
Plain Text
Right Ctrl

Restricted Mode is intended for safe code browsing. Trust this window to enable all features.

```

    invoke-virtual {v0}, Ljava/util/concurrent/atomic/AtomicBoolean;->get()Z

    move-result v0

    if-eqz v0, :cond_b

    .line 61774
    iget-object v0, v6, LX/Q3;->b:Landroid/util/Pair;

    iget-object v1, v0, Landroid/util/Pair;->first:Ljava/lang/Object;

    check-cast v1, Landroid/media/AudioRecord;

    const/4 v0, 0x0

    invoke-virtual {v1, v3, v0, v4}, Landroid/media/AudioRecord;->read([BII)I

    move-result v2

    .line 61775
    iget-object v0, v6, LX/Q3;->a:LX/Q5;

    iget-object v0, v0, LX/Q5;->d:Ljava/util/concurrent/atomic/AtomicBoolean;

```

Figure 14: X.Q3.smali file



Installation/Persistence

Has the ability to access external storage

details Found invoke in "X.C2.smali" to "android.os.Environment.getExternalStorageDirectory"
Found invoke in "X.C2.smali" to "android.os.Environment.getExternalStorageState"
Found invoke in "X.E2.smali" to "android.os.Environment.getExternalStorageDirectory"
Found invoke in "X.E2.smali" to "android.os.Environment.getExternalStorageState"
Found invoke in "X.PC.smali" to "android.os.Environment.getExternalStorageDirectory"
source Static Parser
relevance 3/10
ATT&CK ID T1420 (Show technique in the MITRE ATT&CK™ matrix)

Network Related

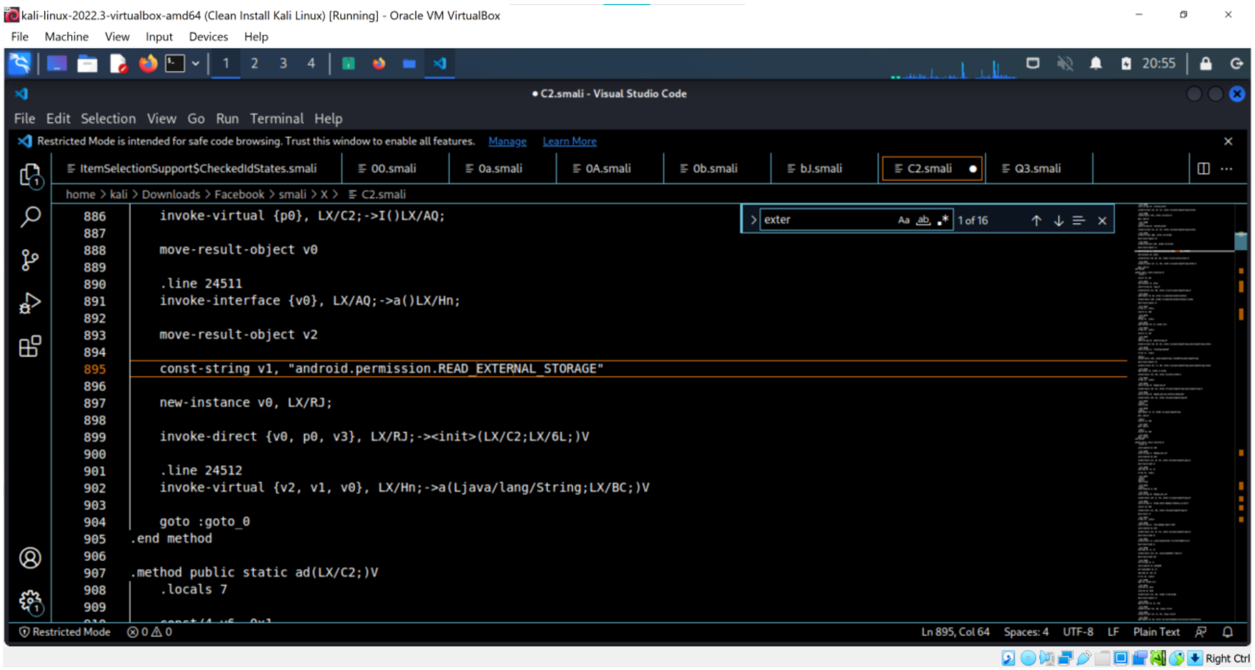
Found potential IP address in binary/memory

Has the ability to open an internet connection

Spyware/Information Retrieval

kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc462293b/
HYBRID ANALYSIS
Sandbox
Quick Scans
File Collections
Resources
Request Info
More
Incident Response
Indicators
Malicious (6)
Suspicious (13)
Informative (7)
File Details
Extracted Strings
Extracted Files (4)
Notifications
Community (0)
Back to top

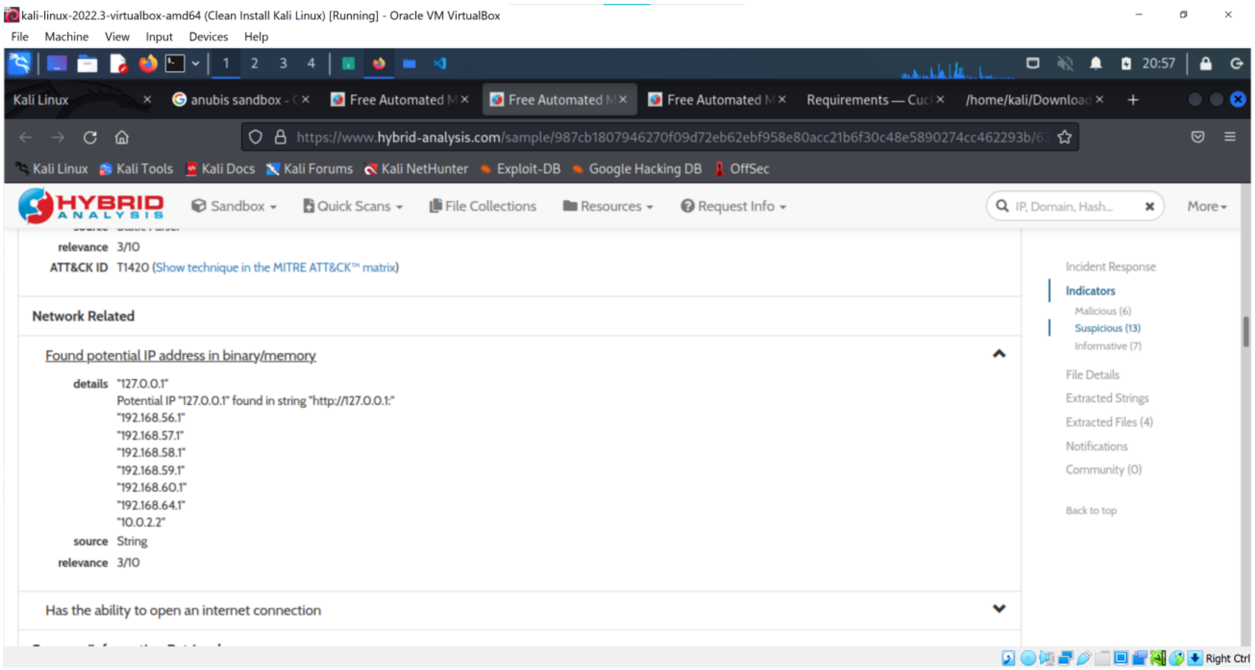
Figure 15: The APK can access external storage



```
    invoke-virtual {p0}, LX/C2;->I()LX/AQ;

    move-result-object v0

    .line 24511
    invoke-interface {v0}, LX/AQ;->a()LX/Hn;

    move-result-object v2

    const-string v1, "android.permission.READ_EXTERNAL_STORAGE"

    new-instance v0, LX/RJ;

    invoke-direct {v0, p0, v3}, LX/RJ;-><init>(LX/C2;LX/6L;)V

    .line 24512
    invoke-virtual {v2, v1, v0}, LX/Hn;->a(Ljava/lang/String;LX/BC;)V

    goto :goto_0
.end method

.method public static ad(LX/C2;)V
    .locals 7
```

kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
● C2.smali - Visual Studio Code
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
ItemSelectionSupport$CheckedIdStates.smali
00.smali
0a.smali
0A.smali
0b.smali
bJ.smali
C2.smali
Q3.smali
home > kali > Downloads > Facebook > smali > X > C2.smali
exter
1 of 16
Restricted Mode
Ln 895, Col 64 Spaces: 4 UTF-8 LF Plain Text

Figure 16: X.C2.smali – Malicious Code



relevance 3/10
ATT&CK ID T1420 (Show technique in the MITRE ATT&CK™ matrix)

Network Related

Found potential IP address in binary/memory

```
details   "127.0.0.1"
          Potential IP "127.0.0.1" found in string "http://127.0.0.1:"
          "192.168.56.1"
          "192.168.57.1"
          "192.168.58.1"
          "192.168.59.1"
          "192.168.60.1"
          "192.168.64.1"
          "10.0.2.2"
source    String
relevance 3/10
```

Has the ability to open an internet connection

Figure 17: IP Addresses Found! - Malicious

Just like the popular meterpreter reverse-shell exploit, it seems this application allows a remote attacker at the IP address listed in Figure 17 access into the victims' phone once the application is installed.

Summary:

In conclusion, the Facebook.apk android application is malicious and opens a backdoor into the user personal files, audio, contacts, sms, call history once installed. It also can execute code upon installation. After decompiling, we noticed a folder marked “X” in the smali folder. The name alone did not match other, and common folder nomenclature within android applications. The folder contains several other similarly named smali files, which from our Sandbox Analysis contains a lot of the malicious code for this app.

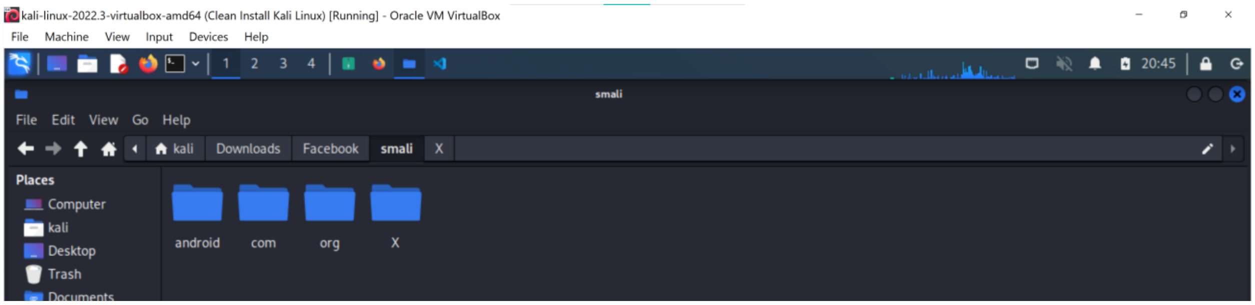
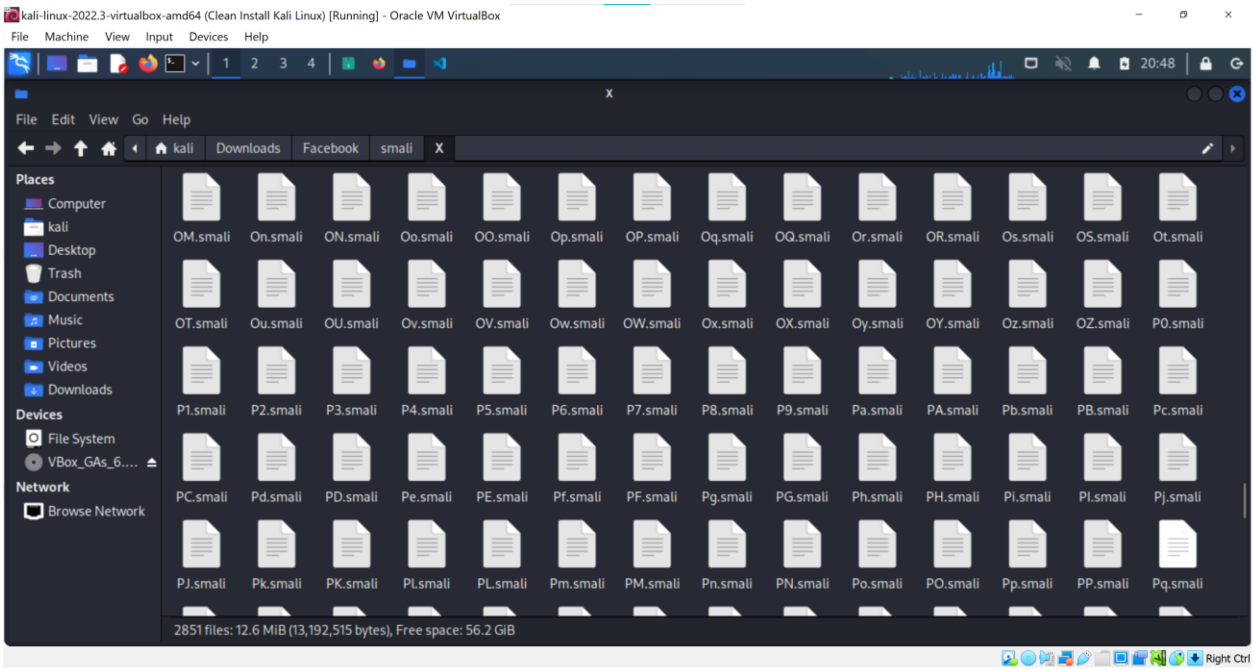

kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
20:45
smali
File Edit View Go Help
kali Downloads Facebook smali X
Places
Computer
kali
Desktop
Trash
Documents
android
com
org
X

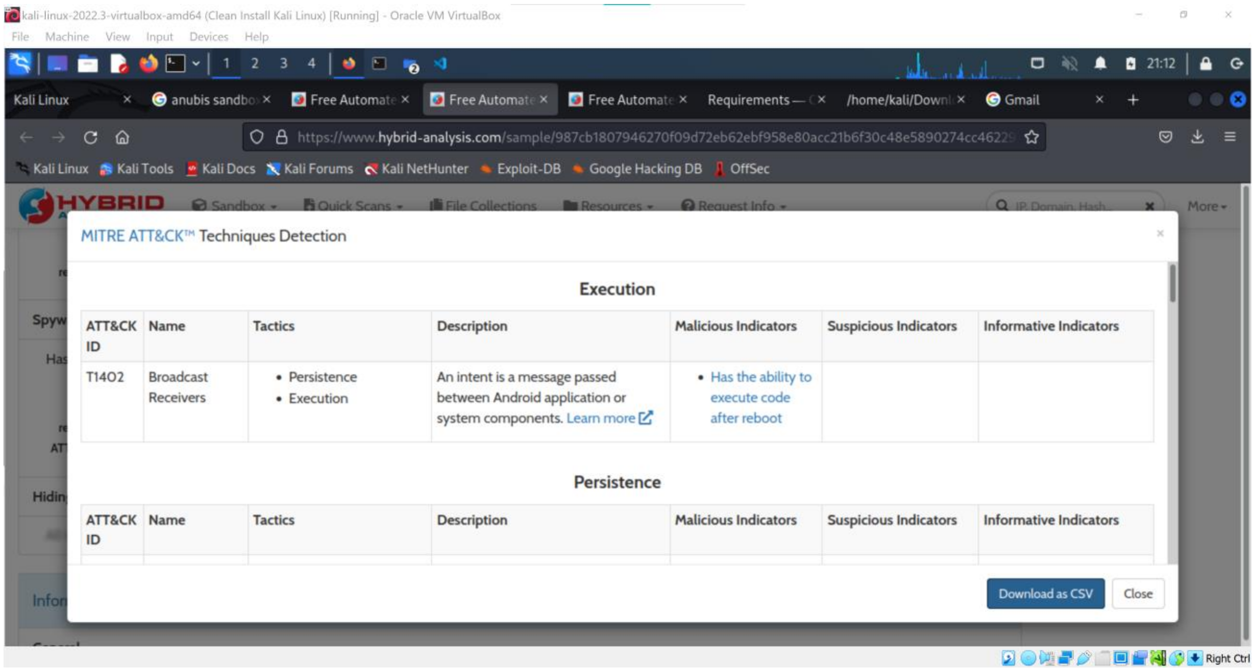
Figure 18: Folder X in Facebook.apk decompiled


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
20:48
X
File Edit View Go Help
kali Downloads Facebook smali X
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
VBox_GAs_6....
Network
Browse Network
OM.smali On.smali ON.smali Oo.smali OO.smali Op.smali OP.smali Oq.smali OQ.smali Or.smali OR.smali Os.smali OS.smali Ot.smali
OT.smali Ou.smali OU.smali Ov.smali OV.smali Ow.smali OW.smali Ox.smali OX.smali Oy.smali OY.smali Oz.smali OZ.smali P0.smali
P1.smali P2.smali P3.smali P4.smali P5.smali P6.smali P7.smali P8.smali P9.smali Pa.smali PA.smali Pb.smali PB.smali Pc.smali
PC.smali Pd.smali PD.smali Pe.smali PE.smali Pf.smali PF.smali Pg.smali PG.smali Ph.smali PH.smali Pi.smali PI.smali Pj.smali
PJ.smali Pk.smali PK.smali Pl.smali PL.smali Pm.smali PM.smali Pn.smali PN.smali Po.smali PO.smali Pp.smali PP.smali Pq.smali
Right Ctrl

2851 files: 12.6 MiB (13,192,515 bytes), Free space: 56.2 GiB

Figure 19: Folder X contents

All the malicious techniques used in this APK, their description and indicators are identified in Figures 20 – 26.


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:12
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
More
Download as CSV
Close
Right Ctrl

MITRE ATT&CK™ Techniques Detection

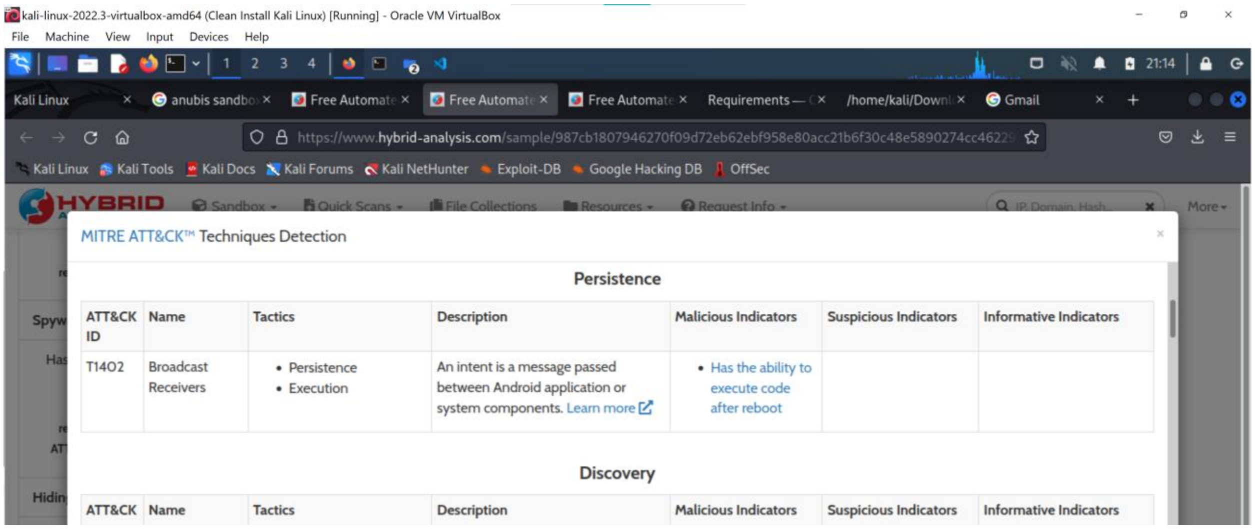
Execution

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	• Persistence • Execution	An intent is a message passed between Android application or system components. Learn more	• Has the ability to execute code after reboot		

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators

Figure 20


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:14
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
More

MITRE ATT&CK™ Techniques Detection

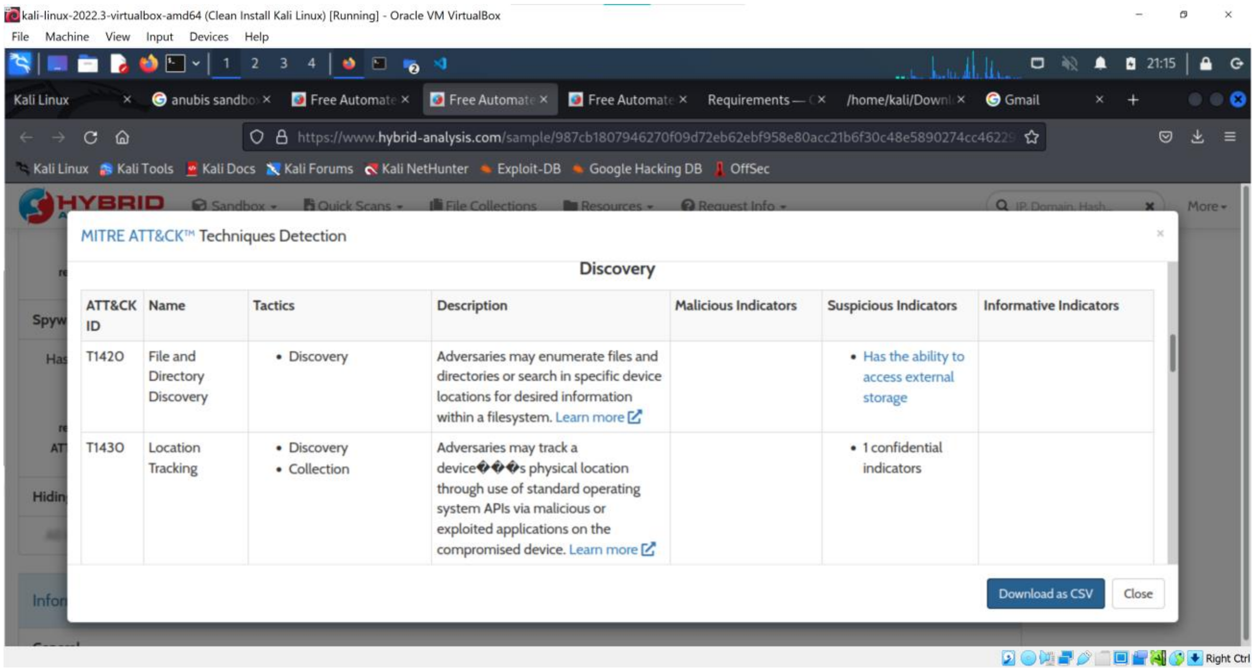
Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1402	Broadcast Receivers	• Persistence • Execution	An intent is a message passed between Android application or system components. Learn more	• Has the ability to execute code after reboot		

Discovery

ATT&CK	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators

Figure 21

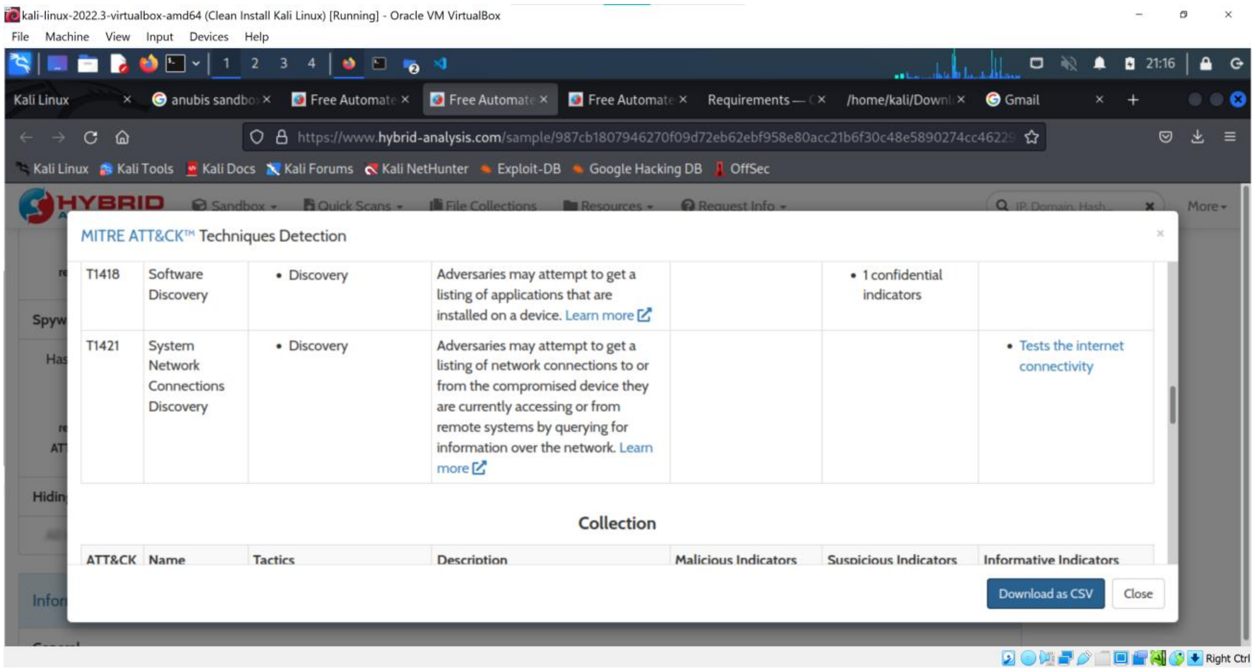

kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:15
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
IP, Domain, Hash...
More
Download as CSV
Close
Right Ctrl

MITRE ATT&CK™ Techniques Detection

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1420	File and Directory Discovery	• Discovery	Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Learn more		• Has the ability to access external storage	
T1430	Location Tracking	• Discovery • Collection	Adversaries may track a device���s physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. Learn more		• 1 confidential indicators	

Figure 22


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:16
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
IP, Domain, Hash...
More
Download as CSV
Close
Right Ctrl

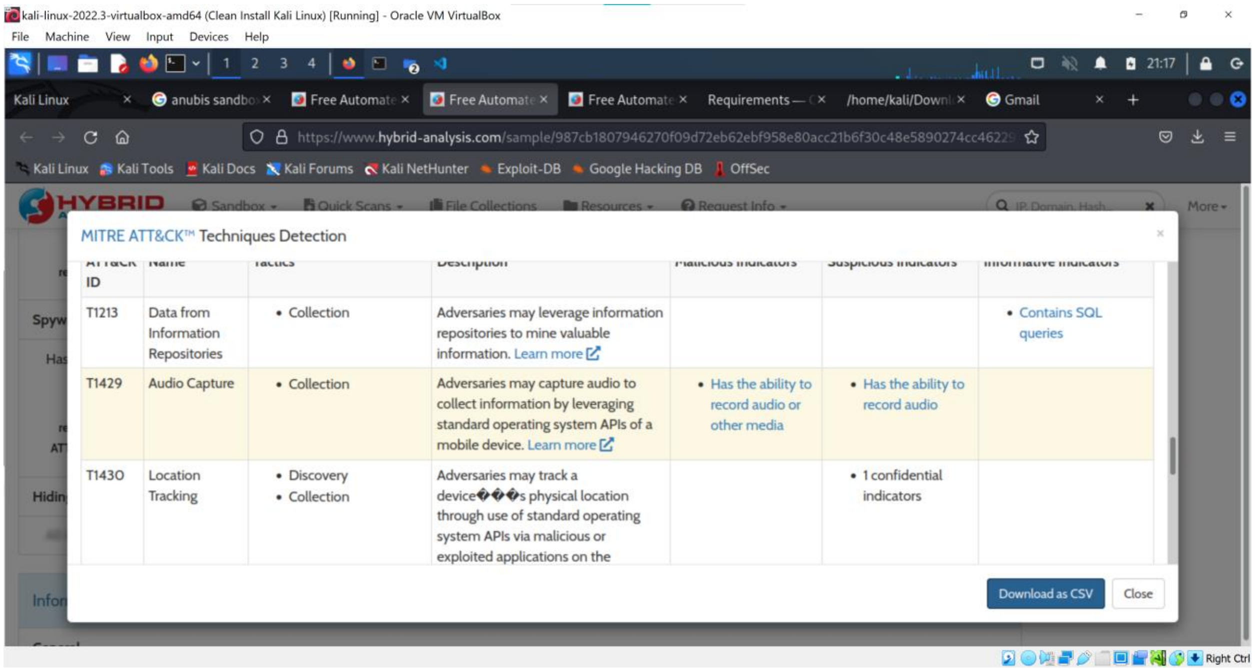
MITRE ATT&CK™ Techniques Detection

T1418	Software Discovery	• Discovery	Adversaries may attempt to get a listing of applications that are installed on a device. Learn more		• 1 confidential indicators	
T1421	System Network Connections Discovery	• Discovery	Adversaries may attempt to get a listing of network connections to or from the compromised device they are currently accessing or from remote systems by querying for information over the network. Learn more			• Tests the internet connectivity

Collection

ATT&CK	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators

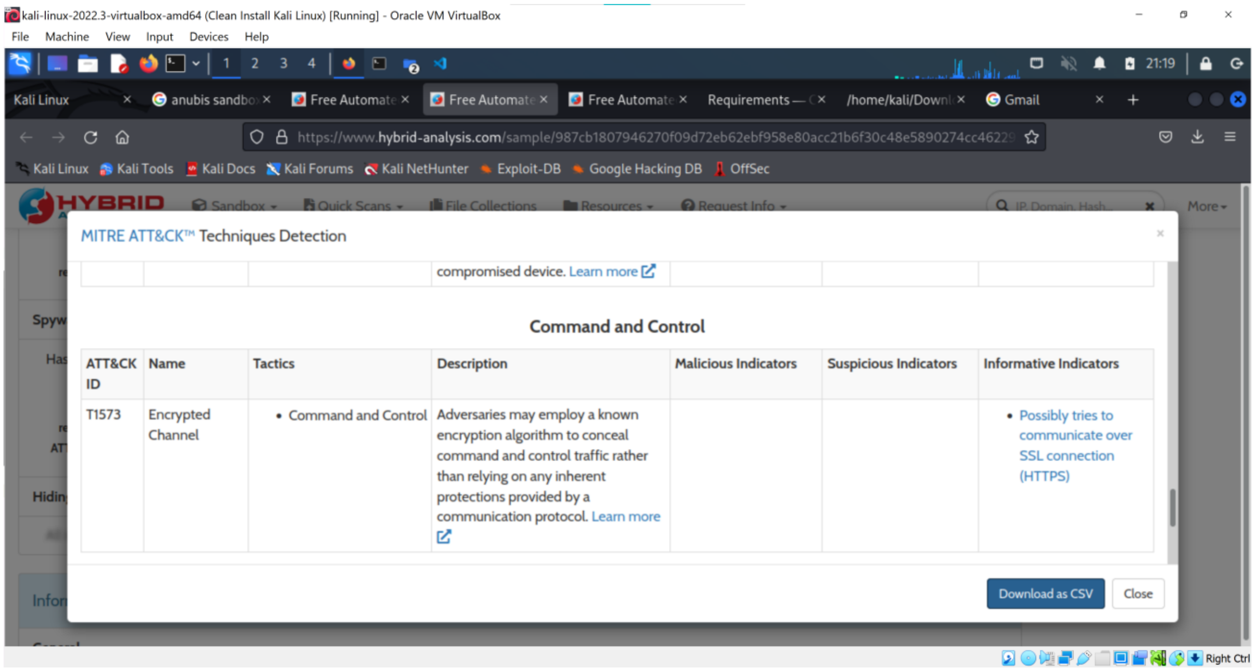
Figure 23


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:17
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
IP, Domain, Hash...
More
Download as CSV
Close
Right Ctrl

MITRE ATT&CK™ Techniques Detection

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1213	Data from Information Repositories	• Collection	Adversaries may leverage information repositories to mine valuable information. Learn more			• Contains SQL queries
T1429	Audio Capture	• Collection	Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Learn more	• Has the ability to record audio or other media	• Has the ability to record audio	
T1430	Location Tracking	• Discovery • Collection	Adversaries may track a device���s physical location through use of standard operating system APIs via malicious or exploited applications on the		• 1 confidential indicators	

Figure 24


kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
21:19
Kali Linux
anubis sandbo
Free Automate
Free Automate
Free Automate
Requirements —
/home/kali/Downl
Gmail
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HYBRID
Sandbox Quick Scans File Collections Resources Request Info
IP, Domain, Hash...
More
Download as CSV
Close
Right Ctrl

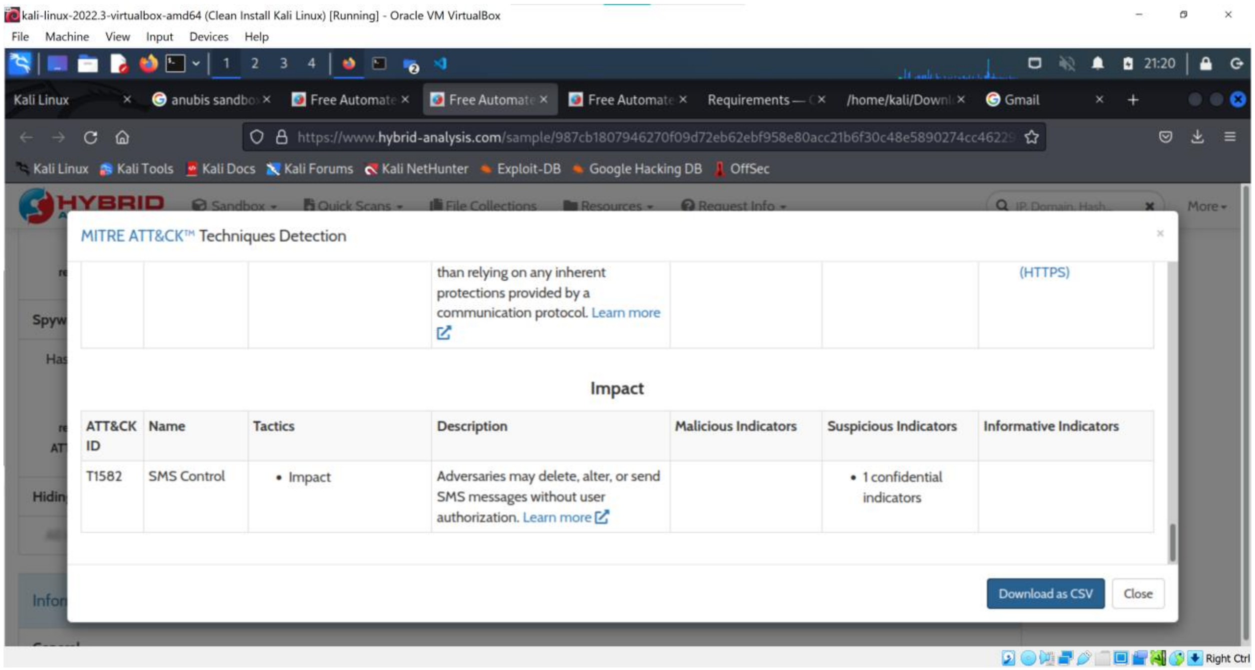
MITRE ATT&CK™ Techniques Detection

compromised device. Learn more

Command and Control

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1573	Encrypted Channel	• Command and Control	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Learn more			• Possibly tries to communicate over SSL connection (HTTPS)

Figure 25



kali-linux-2022.3-virtualbox-amd64 (Clean Install Kali Linux) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
https://www.hybrid-analysis.com/sample/987cb1807946270f09d72eb62ebf958e80acc21b6f30c48e5890274cc4622
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Download as CSV
Close

MITRE ATT&CK™ Techniques Detection

			than relying on any inherent protections provided by a communication protocol. Learn more			(HTTPS)

Impact

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1582	SMS Control	• Impact	Adversaries may delete, alter, or send SMS messages without user authorization. Learn more		• 1 confidential indicators	

Figure 26