

Malicious APK File Analysis

No. 17

We use androguard to analyse given Horoscope.apk from group 17.

```
root@kali: /home/manisha/Downloads
File Actions Edit View Help
-rw-r--r-- 1 manisha manisha 10235 Nov 3 23:54 fb.apk
drwxr-xr-x 2 manisha manisha 4096 Nov 9 22:43 'Final '
-rw-r--r-- 1 manisha manisha 11427 Nov 10 10:39 'Final_apk.zip
-rw-r--r-- 1 manisha manisha 17476151 Nov 3 22:35 Horoscope.apk
-rw-r--r-- 1 manisha manisha 16155164 Nov 14 21:47 Horoscope.zip
-rwxr-xr-x 1 root root 19981711 Nov 3 21:02 usrlocalbin

(root@kali)-[/home/manisha/Downloads]
# androguard analyze mal.apk
Usage: androguard analyze [OPTIONS] [APK]
Try 'androguard analyze --help' for help.

Error: Invalid value for '[APK]': Path 'mal.apk' does not exist.

(root@kali)-[/home/manisha/Downloads]
# androguard analyze Horoscope.apk
Please be patient, this might take a while.
Found the provided file is of type 'APK'
[WARNING ] androguard.core.api_specific_resources: Requested API level 33 is larger than maximum we have, returning API level 28 instead.
[INFO ] androguard.analysis: End of creating cross references (XREF)
[INFO ] androguard.analysis: run time: 0min 00s
[INFO ] androguard.analysis: End of creating cross references (XREF)
[INFO ] androguard.analysis: run time: 0min 08s
[INFO ] androguard.analysis: End of creating cross references (XREF)
[INFO ] androguard.analysis: run time: 0min 11s
Added file to session: SHA256::06d9b96f7aaa5ba97ff4d4518b27d9c71d9de68faf3fb28ef7ab8ce651715c15
Loaded APK file ...
>>> a
<androguard.core.bytecodes.apk.APK object at 0x7eff59e30a60>
>>> d
[<androguard.core.bytecodes.dvm.DalvikVMFormat object at 0x7eff597c3970>, <androguard.core.bytecodes.dvm.DalvikVMFormat object at 0x7eff571ca
bf0>, <androguard.core.bytecodes.dvm.DalvikVMFormat object at 0x7eff337e2e90>]
>>> dx
<analysis.Analysis VMS: 3, Classes: 25412, Strings: 30243>

Androguard version 3.3.5 started
1
```

By using androguard we find the android version ,android resources ,android applications icon ,android applications name and which are the permissions for android applications.

```
root@kali: /home/manisha/Downloads

File Actions Edit View Help

In [4]: a.get_androidversion_code()
Out[4]: '5100200'

In [5]: a.get_android_resources()
Out[5]: <androguard.core.bytecodes.xml.ARSCParser at 0x7efef7490f40>

In [6]: a.get_app_icon()
Out[6]: 'res/mipmap-anydpi-v26/logo.xml'

In [7]: a.get_app_name()
Out[7]: 'Daily Horoscope'

In [8]:
```

```
root@kali: /home/manisha/Downloads

File Actions Edit View Help

In [10]: a.get_details_permissions()
Out[10]:
{'android.permission.SCHEDULE_EXACT_ALARM': ['normal',
'Unknown permission from android reference'],
'android.permission.INTERNET': ['normal|instant',
'have full network access',
'Allows the app to create\n        network sockets and use custom network protocols. The browser and other\n        applications provide means to
send data to the internet, so this\n        permission is not required to send data to the internet.'],
'com.google.android.gms.permission.AD_ID': ['normal',
'Unknown permission from android reference'],
'com.android.vending.BILLING': ['normal',
'Unknown permission from android reference'],
'android.permission.POST_NOTIFICATIONS': ['normal',
'Unknown permission from android reference'],
'android.permission.ACCESS_NETWORK_STATE': ['normal|instant',
'view network connections',
'Allows the app to view\n        information about network connections such as which networks exist and are\n        connected.'],
'com.google.android.c2dm.permission.RECEIVE': ['normal',
'Unknown permission from android reference'],
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE': ['normal',
'Unknown permission from android reference'],
'info.android.horoscope.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION': ['normal',
'Unknown permission from android reference'],
'android.permission.WAKE_LOCK': ['normal|instant',
'prevent phone from sleeping',
'Allows the app to prevent the phone from going to sleep.'],
'android.permission.RECEIVE_BOOT_COMPLETED': ['normal',
'run at startup',
'Allows the app to\n        have itself started as soon as the system has finished booting.\n        This can make it take longer to start
the phone and allow the\n        app to slow down the overall phone by always running.'],
'android.permission.FOREGROUND_SERVICE': ['normal|instant',
'run foreground service',
'Allows the app to make use of foreground services.']}

In [11]:
```

We downloaded given apk in santoku and created new directory

```
santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 32856
drwxrwxr-x 3 santoku santoku 4096 nov 15 12:01 -f
-rw-r--r-- 1 santoku santoku 17476151 nov 3 22:35 Horoscope.apk
drwxrwxr-x 10 santoku santoku 4096 nov 15 12:03 Horoscope.apk_FILES
-rwxrwx--- 1 santoku santoku 16155164 nov 15 11:34 Horoscope.zip
santoku@santoku-VirtualBox:~/Downloads$ mkdie newvirus_unzipped
No command 'mkdie' found, did you mean:
  Command 'mkdic' from package 'canna-utils' (universe)
  Command 'mkdir' from package 'coreutils' (main)
mkdie: command not found
santoku@santoku-VirtualBox:~/Downloads$ mkdir newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads$ ls -l
total 32860
drwxrwxr-x 3 santoku santoku 4096 nov 15 12:01 -f
-rw-r--r-- 1 santoku santoku 17476151 nov 3 22:35 Horoscope.apk
drwxrwxr-x 10 santoku santoku 4096 nov 15 12:03 Horoscope.apk_FILES
-rwxrwx--- 1 santoku santoku 16155164 nov 15 11:34 Horoscope.zip
drwxrwxr-x 2 santoku santoku 4096 nov 15 17:15 newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads$
```

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File Edit Tabs Help
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Palau
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Pitcairn
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Pohnpei
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Port Moresby
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Rarotonga
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Saipan
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tahiti
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tarawa
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Tongatapu
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Wake
inflating: newVirus_unzipped/org/joda/time/tz/data/Pacific/Wallis
santoku@santoku-VirtualBox:~/Downloads$ cd newVirus_unzipped
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls -l
total 18356
-rw-rw-r-- 1 santoku santoku 41940 nov 3 23:35 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku 53 nov 3 23:35 androidsupportmultidexversion.txt
drwxrwxr-x 8 santoku santoku 4096 nov 15 17:24 assets
-rw-rw-r-- 1 santoku santoku 58 nov 3 23:35 billing-ktx.properties
-rw-rw-r-- 1 santoku santoku 50 nov 3 23:35 billing.properties
-rw-rw-r-- 1 santoku santoku 8343804 nov 3 23:35 classes2.dex
-rw-rw-r-- 1 santoku santoku 492784 nov 3 23:35 classes3.dex
-rw-rw-r-- 1 santoku santoku 8635060 nov 3 23:35 classes.dex
drwxrwxr-x 4 santoku santoku 4096 nov 15 17:24 com
-rw-rw-r-- 1 santoku santoku 1738 nov 3 23:35 DebugProbesKt.bin
-rw-rw-r-- 1 santoku santoku 62 nov 3 23:35 firebase-ads.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-analytics-ktx.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 firebase-analytics.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-annotations.properties
-rw-rw-r-- 1 santoku santoku 88 nov 3 23:35 firebase-appcheck-interop.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-appindexing.properties
-rw-rw-r-- 1 santoku santoku 80 nov 3 23:35 firebase-auth-interop.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-auth-ktx.properties
-rw-rw-r-- 1 santoku santoku 64 nov 3 23:35 firebase-auth.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 firebase-common-ktx.properties
-rw-rw-r-- 1 santoku santoku 68 nov 3 23:35 firebase-common.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 firebase-components.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-crashlytics.properties
-rw-rw-r-- 1 santoku santoku 94 nov 3 23:35 firebase-database-collection.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-database.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-datatransport.properties
-rw-rw-r-- 1 santoku santoku 90 nov 3 23:35 firebase-dynamic-links-ktx.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-dynamic-links.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-encoders-json.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-encoders.properties
-rw-rw-r-- 1 santoku santoku 84 nov 3 23:35 firebase-encoders-proto.properties
```

We unzip the apk file and copy that unzipped file to new directory we created

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File Edit Tabs Help
-rw-rw-r-- 1 santoku santoku 90 nov 3 23:35 firebase-dynamic-links-ktx.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-dynamic-links.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-encoders-json.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-encoders.properties
-rw-rw-r-- 1 santoku santoku 84 nov 3 23:35 firebase-encoders-proto.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-iid-interop.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 firebase-installations-interop.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-installations.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 firebase-measurement-connector.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 firebase-messaging.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-storage-ktx.properties
-rw-rw-r-- 1 santoku santoku 70 nov 3 23:35 firebase-storage.properties
drwxrwxr-x 3 santoku santoku 4096 nov 15 17:24 javax
drwxrwxr-x 8 santoku santoku 4096 nov 15 17:24 kotlin
-rw-rw-r-- 1 santoku santoku 628 nov 3 23:35 kotlin-tooling-metadata.json
drwxrwxr-x 3 santoku santoku 4096 nov 15 17:24 META-INF
drwxrwxr-x 3 santoku santoku 4096 nov 15 17:24 okhttp3
drwxrwxr-x 3 santoku santoku 4096 nov 15 17:24 org
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 play-services-ads-base.properties
-rw-rw-r-- 1 santoku santoku 94 nov 3 23:35 play-services-ads-identifier.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 play-services-ads-lite.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 play-services-ads.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 play-services-appset.properties
-rw-rw-r-- 1 santoku santoku 94 nov 3 23:35 play-services-auth-api-phone.properties
-rw-rw-r-- 1 santoku santoku 84 nov 3 23:35 play-services-auth-base.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 play-services-auth.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 play-services-basement.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 play-services-base.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-cloud-messaging.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-measurement-api.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 play-services-measurement-base.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 play-services-measurement-impl.properties
-rw-rw-r-- 1 santoku santoku 88 nov 3 23:35 play-services-measurement.properties
-rw-rw-r-- 1 santoku santoku 104 nov 3 23:35 play-services-measurement-sdk-api.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-measurement-sdk.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 play-services-stats.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 play-services-tasks.properties
drwxrwxr-x 37 santoku santoku 4096 nov 15 17:24 res
-rw-rw-r-- 1 santoku santoku 1094464 nov 3 23:35 resources.arsc
-rw-rw-r-- 1 santoku santoku 32 nov 3 23:35 stamp-cert-sha256
-rw-rw-r-- 1 santoku santoku 62 nov 3 23:35 transport-api.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 transport-backend-cct.properties
-rw-rw-r-- 1 santoku santoku 70 nov 3 23:35 transport-runtime.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 user-messaging-platform.properties
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
```

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ll
total 18364
drwxrwxr-x 10 santoku santoku 4096 nov 15 17:24 ./
drwxr-xr-x 5 santoku santoku 4096 nov 15 17:15 ../
-rw-rw-r-- 1 santoku santoku 41940 nov 3 23:35 AndroidManifest.xml
-rw-rw-r-- 1 santoku santoku 53 nov 3 23:35 androidsupportmultidexversion.txt
drwxrwxr-x 8 santoku santoku 4096 nov 15 17:24 assets/
-rw-rw-r-- 1 santoku santoku 58 nov 3 23:35 billing-ktx.properties
-rw-rw-r-- 1 santoku santoku 50 nov 3 23:35 billing.properties
-rw-rw-r-- 1 santoku santoku 8343004 nov 3 23:35 classes2.dex
-rw-rw-r-- 1 santoku santoku 492784 nov 3 23:35 classes3.dex
-rw-rw-r-- 1 santoku santoku 8635060 nov 3 23:35 classes.dex
drwxrwxr-x 4 santoku santoku 4096 nov 15 17:24 com/
-rw-rw-r-- 1 santoku santoku 1738 nov 3 23:35 DebugProbesKt.bin
-rw-rw-r-- 1 santoku santoku 62 nov 3 23:35 firebase-ads.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-analytics-ktx.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 firebase-analytics.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-annotations.properties
-rw-rw-r-- 1 santoku santoku 88 nov 3 23:35 firebase-appcheck-interop.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-appindexing.properties
-rw-rw-r-- 1 santoku santoku 80 nov 3 23:35 firebase-auth-interop.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-auth-ktx.properties
-rw-rw-r-- 1 santoku santoku 64 nov 3 23:35 firebase-auth.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 firebase-common-ktx.properties
-rw-rw-r-- 1 santoku santoku 68 nov 3 23:35 firebase-common.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 firebase-components.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-crashlytics.properties
-rw-rw-r-- 1 santoku santoku 94 nov 3 23:35 firebase-database-collection.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-database.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-datatransport.properties
-rw-rw-r-- 1 santoku santoku 90 nov 3 23:35 firebase-dynamic-links-ktx.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-dynamic-links.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-encoders-json.properties
-rw-rw-r-- 1 santoku santoku 72 nov 3 23:35 firebase-encoders.properties
-rw-rw-r-- 1 santoku santoku 84 nov 3 23:35 firebase-encoders-proto.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-iid-interop.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 firebase-installations-interop.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 firebase-installations.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 firebase-measurement-connector.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 firebase-messaging.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 firebase-storage-ktx.properties
-rw-rw-r-- 1 santoku santoku 70 nov 3 23:35 firebase-storage.properties
drwxrwxr-x 3 santoku santoku 4096 nov 15 17:24 javax/
drwxrwxr-x 8 santoku santoku 4096 nov 15 17:24 kotlin/
-rw-rw-r-- 1 santoku santoku 628 nov 3 23:35 kotlin-tooling-metadata.json
```

```
santoku@santoku-VirtualBox: ~/Downloads/newVirus_unzipped
File Edit Tabs Help
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 play-services-auth.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 play-services-basement.properties
-rw-rw-r-- 1 santoku santoku 74 nov 3 23:35 play-services-base.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-cloud-messaging.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-measurement-api.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 play-services-measurement-base.properties
-rw-rw-r-- 1 santoku santoku 98 nov 3 23:35 play-services-measurement-impl.properties
-rw-rw-r-- 1 santoku santoku 88 nov 3 23:35 play-services-measurement.properties
-rw-rw-r-- 1 santoku santoku 104 nov 3 23:35 play-services-measurement-sdk-api.properties
-rw-rw-r-- 1 santoku santoku 96 nov 3 23:35 play-services-measurement-sdk.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 play-services-stats.properties
-rw-rw-r-- 1 santoku santoku 76 nov 3 23:35 play-services-tasks.properties
drwxrwxr-x 37 santoku santoku 4096 nov 15 17:24 res/
-rw-rw-r-- 1 santoku santoku 1004464 nov 3 23:35 resources.arsc
-rw-rw-r-- 1 santoku santoku 32 nov 3 23:35 stamp-cert-sha256
-rw-rw-r-- 1 santoku santoku 62 nov 3 23:35 transport-api.properties
-rw-rw-r-- 1 santoku santoku 78 nov 3 23:35 transport-backend-cct.properties
-rw-rw-r-- 1 santoku santoku 70 nov 3 23:35 transport-runtime.properties
-rw-rw-r-- 1 santoku santoku 82 nov 3 23:35 user-messaging-platform.properties
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$ ls
AndroidManifest.xml          firebase-database.properties      play-services-appset.properties
androidsupportmultidexversion.txt  firebase-datatransport.properties  play-services-auth-api-phone.properties
assets                       firebase-dynamic-links-ktx.properties  play-services-auth-base.properties
billing-ktx.properties        firebase-dynamic-links.properties    play-services-auth.properties
billing.properties           firebase-encoders-json.properties    play-services-basement.properties
classes2.dex                 firebase-encoders.properties        play-services-base.properties
classes3.dex                 firebase-encoders-proto.properties  play-services-cloud-messaging.properties
classes.dex                  firebase-iid-interop.properties     play-services-measurement-api.properties
com                          firebase-installations-interop.properties  play-services-measurement-base.properties
DebugProbesKt.bin           firebase-installations.properties    play-services-measurement-impl.properties
firebase-ads.properties     firebase-measurement-connector.properties  play-services-measurement.properties
firebase-analytics-ktx.properties  firebase-messaging.properties      play-services-measurement-sdk-api.properties
firebase-analytics.properties  firebase-storage-ktx.properties    play-services-measurement-sdk.properties
firebase-annotations.properties  firebase-storage.properties       play-services-stats.properties
firebase-appcheck-interop.properties  javax                             play-services-tasks.properties
firebase-appindexing.properties  kotlin                            res
firebase-auth-interop.properties  kotlin-tooling-metadata.json      resources.arsc
firebase-auth-ktx.properties    META-INF                          stamp-cert-sha256
firebase-auth.properties       okhttp3                            transport-api.properties
firebase-common-ktx.properties  org                               transport-backend-cct.properties
firebase-common.properties     play-services-ads-base.properties  transport-runtime.properties
firebase-components.properties  play-services-ads-identifier.properties  user-messaging-platform.properties
firebase-crashlytics.properties  play-services-ads-lite.properties
firebase-database-collection.properties  play-services-ads.properties
santoku@santoku-VirtualBox:~/Downloads/newVirus_unzipped$
```

We try to decompile the file using apk tool

```
santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads$ apktool d Horoscope.apk -f
I: Baksmaling...
I: Loading resource table...
Exception in thread "main" brut.androlib.AndrolibException: Could not decode arsc file
    at brut.androlib.res.decoder.ARSCDecoder.decode(ARSCDecoder.java:56)
    at brut.androlib.res.AndrolibResources.getResPackagesFromApk(AndrolibResources.java:491)
    at brut.androlib.res.AndrolibResources.loadMainPkg(AndrolibResources.java:74)
    at brut.androlib.res.AndrolibResources.getResTable(AndrolibResources.java:66)
    at brut.androlib.Androlib.getResTable(Androlib.java:50)
    at brut.androlib.ApkDecoder.getResTable(ApkDecoder.java:189)
    at brut.androlib.ApkDecoder.decode(ApkDecoder.java:114)
    at brut.apktool.Main.cmdDecode(Main.java:146)
    at brut.apktool.Main.main(Main.java:77)
Caused by: java.io.IOException: Expected: 0x001c0001, got: 0x00000000
    at brut.util.ExtDataInput.skipCheckInt(ExtDataInput.java:48)
    at brut.androlib.res.decoder.StringBlock.read(StringBlock.java:44)
    at brut.androlib.res.decoder.ARSCDecoder.readPackage(ARSCDecoder.java:102)
    at brut.androlib.res.decoder.ARSCDecoder.readTable(ARSCDecoder.java:83)
    at brut.androlib.res.decoder.ARSCDecoder.decode(ARSCDecoder.java:49)
    ... 8 more
santoku@santoku-VirtualBox:~/Downloads$
```


Using ls command, we try to find all files containing in the Horoscope.apk

```
santoku@santoku-VirtualBox: ~/Downloads/Horoscope.apk_FILES/small
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ ls
AndroidManifest.xml      firebase-database.properties      play-services-appset.properties
androidsupportmultidexversion.txt  firebase-datatransport.properties  play-services-auth-api-phone.properties
assets                   firebase-dynamic-links.properties  play-services-auth-base.properties
billing-ktx.properties    firebase-dynamic-links.properties  play-services-auth.properties
classes2.dex             firebase-encoders.json.properties  play-services-basement.properties
classes3.dex             firebase-encoders.properties       play-services-base.properties
classes.dex              firebase-encoders-proto.properties  play-services-cloud-messaging.properties
com                      firebase-iid-interop.properties     play-services-measurement-api.properties
DebugProbesKt.bin        firebase-installations-interop.properties  play-services-measurement-base.properties
firebase-ads.properties  firebase-installations.properties    play-services-measurement-impl.properties
firebase-analytics-ktx.properties  firebase-measurement-connector.properties  play-services-measurement.properties
firebase-analytics.properties    firebase-messaging.properties          play-services-measurement-sdk-api.properties
firebase-annotations.properties  firebase-storage-ktx.properties         play-services-measurement-sdk.properties
firebase-appcheck-interop.properties  firebase-storage.properties           play-services-stats.properties
firebase-appindexing.properties      java                                  play-services-tasks.properties
firebase-auth-interop.properties      kotlin                               resources.arsc
firebase-auth-ktx.properties          kotlin-tooling-metadata.json          smali
firebase-auth.properties             META-INF                             stamp-cert-sha256
firebase-common.properties           okhttp3                              transport-api.properties
firebase-common-ktx.properties       org                                  transport-backend-ctt.properties
firebase-components.properties      play-services-ads-base.properties     transport-runtime.properties
firebase-crashlytics.properties     play-services-ads-identifier.properties  user-messaging-platform.properties
firebase-database-collection.properties  play-services-ads-lite.properties
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ cd smali
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/smali$ ls
a  a3  b  b3  c2  d  d3  e0  f  f3  g2  h0  i  i3  j  k  k2  l  m  n2  p  q2  r2  s2  t2  u2  w  x1  y1  z1
a0 android b0 c c3 d0 de e2 f0 g g3 h2 i0 info j2 k2 l m2 o p2 r s t u v w1 x2 y2 z2
a2 androidx b2 c0 com d2 e e3 f2 g0 h h3 i2 io java k kotlin l2 n o2 q r1 s1 t1 u1 v1 x y z
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/smali$
```

Now We can check the resource folder under the decompiled apk file which may tell what the application is intended to do

```
santoku@santoku-VirtualBox: ~/Downloads/Horoscope.apk_FILES
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com/fasterxml/jackson/core/json$ cd
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com$ cd D
Desktop/ Documents/ Downloads/
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com/Downloads$ cd Horoscope.apk_FILES
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com/Downloads/Horoscope.apk_FILES$ cd res
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/com/Downloads/Horoscope.apk_FILES/res$ ls
anim          drawable-hdpi      drawable-ldrtl-mdpi  drawable-nodpi      interpolator      layout-watch      mipmap-xhdpi
animator      drawable-land       drawable-ldrtl-xhdpi  drawable-watch      layout           menu              mipmap-xxhdpi
color         drawable-land-nodpi  drawable-ldrtl-xxhdpi  drawable-xhdpi      layout-land       mipmap-anydpi-v26  mipmap-xxxhdpi
drawable      drawable-ldpi        drawable-ldrtl-xxxhdpi  drawable-xxxhdpi    layout-sw600dp    mipmap-hdpi        raw
drawable-anydpi  drawable-ldrtl-hdpi  drawable-mdpi         drawable-xxxhdpi    layout-v26        mipmap-mdpi        xml
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/res$ cd
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/res$ cd D
Desktop/ Documents/ Downloads/
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/res$ cd Horoscope.apk_FILES
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES/res/Horoscope.apk_FILES$ dex2jar classes.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar classes.dex -> classes dex2jar.jar
com.googlecode.dex2jar.DexException: while accept method:[Landroidx/activity/result/ActivityResultRegistry;.c(ILjava/lang/Object;)[Z]
    at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:694)
    at com.googlecode.dex2jar.reader.DexFileReader.acceptClass(DexFileReader.java:441)
    at com.googlecode.dex2jar.reader.DexFileReader.accept(DexFileReader.java:323)
    at com.googlecode.dex2jar.v3.Dex2jar.doTranslate(Dex2jar.java:85)
    at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:261)
    at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:252)
    at com.googlecode.dex2jar.v3.Main.doData(Main.java:43)
    at com.googlecode.dex2jar.v3.Main.doData(Main.java:35)
    at com.googlecode.dex2jar.v3.Main.doFile(Main.java:63)
    at com.googlecode.dex2jar.v3.Main.main(Main.java:86)
Caused by: com.googlecode.dex2jar.DexException: while accept parameter annotation in method:[Landroidx/activity/result/ActivityResultRegistry;.c(ILjava/lang/Object;)[Z], parameter:[0]
    at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:663)
    ... 9 more
Caused by: java.lang.IllegalArgumentException: Id out of bound
    at com.googlecode.dex2jar.reader.DexFileReader.getType(DexFileReader.java:556)
    at com.googlecode.dex2jar.reader.DexAnnotationReader.accept(DexAnnotationReader.java:51)
    at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:660)
    ... 9 more
Done.
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ ls
```

```
santoku@santoku-VirtualBox: ~/Downloads/Horoscope.apk_FILES
File Edit Tabs Help

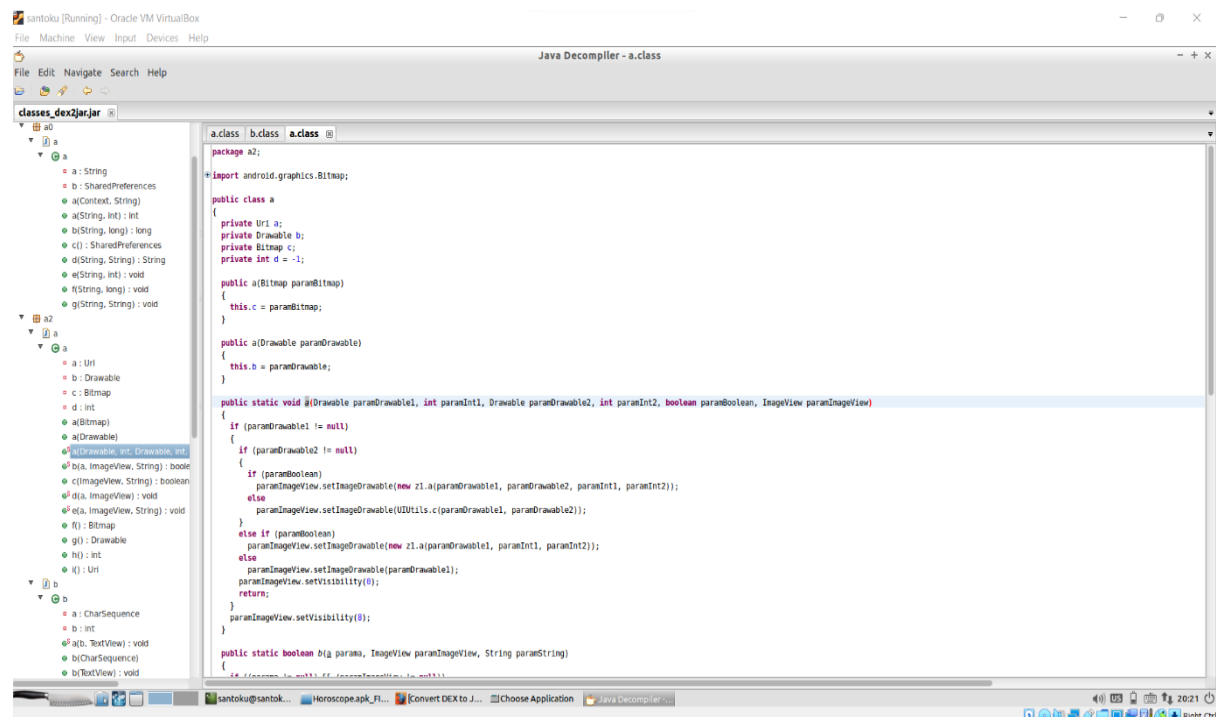
at com.googlecode.dex2jar.v3.Dex2jar.doTranslate(Dex2jar.java:85)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:261)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:252)
at com.googlecode.dex2jar.v3.Main.doData(Main.java:43)
at com.googlecode.dex2jar.v3.Main.doData(Main.java:35)
at com.googlecode.dex2jar.v3.Main.doFile(Main.java:63)
at com.googlecode.dex2jar.v3.Main.main(Main.java:86)
Caused by: com.googlecode.dex2jar.DexException: while accept parameter annotation in method:[Landroidx/activity/result/ActivityResultRegistry;.(Ljava/lang/Object;)Z], parameter:[0]
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:663)
... 9 more
Caused by: java.lang.IllegalArgumentException: Id out of bound
at com.googlecode.dex2jar.reader.DexFileReader.getType(DexFileReader.java:556)
at com.googlecode.dex2jar.reader.DexAnnotationReader.accept(DexAnnotationReader.java:51)
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:660)
... 9 more
Done.
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ ls
AndroidManifest.xml      firebase-database-collection.properties  play-services-ads.properties
androidsupportmultidexversion.txt  firebase-database.properties            play-services-appset.properties
assets                   firebase-datatransport.properties        play-services-auth-api-phone.properties
billing-ktx.properties    firebase-dynamic-links-ktx.properties    play-services-auth-base.properties
billing.properties        firebase-dynamic-links.properties        play-services-auth.properties
classes2.dex              firebase-encoders-json.properties         play-services-basement.properties
classes3.dex              firebase-encoders-proto.properties        play-services-base.properties
classes.dex               firebase-iid-interop.properties           play-services-cloud-messaging.properties
classes_dex2jar.jar       firebase-installations-interop.properties play-services-measurement-api.properties
com                       firebase-installations.properties         play-services-measurement-base.properties
DebugProbesKt.bin         firebase-measurement-connector.properties play-services-measurement-impl.properties
firebase-ads.properties    firebase-messaging.properties            play-services-measurement.properties
firebase-analytics-ktx.properties  firebase-messaging.properties            play-services-measurement-sdk-api.properties
firebase-analytics.properties  firebase-storage-ktx.properties          play-services-measurement-sdk.properties
firebase-annotations.properties  firebase-storage.properties              play-services-stats.properties
firebase-appcheck-interop.properties  javax                                    play-services-tasks.properties
firebase-appindexing.properties  kotlin                                   res
firebase-auth-interop.properties  kotlin-tooling-metadata.json             resources.arsc
firebase-auth-ktx.properties      META-INF                                 smali
firebase-auth.properties          okhttp3                                   stamp-cert-sha256
firebase-common-ktx.properties    org                                       transport-api.properties
firebase-common.properties        play-services-ads-base.properties         transport-backend-cct.properties
firebase-components.properties    play-services-ads-identifier.properties   transport-runtime.properties
firebase-crashlytics.properties   play-services-ads-lite.properties         user-messaging-platform.properties
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$
```

This application contains three classes.dex files. Now we can convert the classes.dex file to jar in the original unzipped file in the malware, which allow us to access the source file. (using JD-GUI inside Santoku

```
santoku@santoku-VirtualBox: ~/Downloads/Horoscope.apk_FILES
File Edit Tabs Help

firebase-appindexing.properties  kotlin      res
firebase-auth-interop.properties kotlin-tooling-metadata.json  resources.arsc
firebase-auth-ktx.properties    META-INF    smali
firebase-auth.properties        okhttp3     stamp-cert-sha256
firebase-common-ktx.properties  org         transport-api.properties
firebase-common.properties      play-services-ads-base.properties  transport-backend-cct.properties
firebase-components.properties  play-services-ads-identifier.properties  transport-runtime.properties
firebase-crashlytics.properties play-services-ads-lite.properties    user-messaging-platform.properties
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ dex2jar classes(2).dex
bash: syntax error near unexpected token '('
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ dex2jar classes2.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar classes2.dex -> classes2_dex2jar.jar
com.googlecode.dex2jar.DexException: while accept method:[Lcom/google/android/gms/internal/ads/zzbdr;.<init>()Landroid/content/Context;Ljava/lang/String;Lcom/google/android/gms/ads/internal/client/zzdr;ILcom/google/android/gms/ads/appopen/AppOpenAd$AppOpenAdLoadCallback;JV]
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:694)
at com.googlecode.dex2jar.reader.DexFileReader.acceptClass(DexFileReader.java:436)
at com.googlecode.dex2jar.reader.DexFileReader.accept(DexFileReader.java:323)
at com.googlecode.dex2jar.v3.Dex2jar.doTranslate(Dex2jar.java:85)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:261)
at com.googlecode.dex2jar.v3.Dex2jar.to(Dex2jar.java:252)
at com.googlecode.dex2jar.v3.Main.doData(Main.java:43)
at com.googlecode.dex2jar.v3.Main.doData(Main.java:35)
at com.googlecode.dex2jar.v3.Main.doFile(Main.java:63)
at com.googlecode.dex2jar.v3.Main.main(Main.java:86)
Caused by: com.googlecode.dex2jar.DexException: while accept parameter annotation in method:[Lcom/google/android/gms/internal/ads/zzbdr;.<init>()Landroid/content/Context;Ljava/lang/String;Lcom/google/android/gms/ads/internal/client/zzdr;ILcom/google/android/gms/ads/appopen/AppOpenAd$AppOpenAdLoadCallback;JV], parameter:[0]
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:663)
... 9 more
Caused by: java.lang.RuntimeException: EOF
at com.googlecode.dex2jar.reader.io.ArrayDataIn.readUByte(ArrayDataIn.java:131)
at com.googlecode.dex2jar.reader.DexAnnotationReader.accept(DexAnnotationReader.java:49)
at com.googlecode.dex2jar.reader.DexFileReader.acceptMethod(DexFileReader.java:660)
... 9 more
Done.
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$ dex2jar classes3.dex
this cmd is deprecated, use the d2j-dex2jar if possible
dex2jar version: translator-0.0.9.15
dex2jar classes3.dex -> classes3_dex2jar.jar
Done.
santoku@santoku-VirtualBox:~/Downloads/Horoscope.apk_FILES$
```

The jar file we created contains lots of random classes and sub classes. d we can see that it has a bunch of obfuscated and disassembled classes from the “jar” file.



Also we analyzed application by following way:

15

/ 66

15 security vendors and no sandboxes flagged this file as malicious

06d9b96f7aaa5ba97f4d4518b27d9c71d9de68fa3fb28ef7ab8ce651715c15

Horoscope.apk

android apk

16.67 MB

Size

2022-11-16 00:04:41 UTC

a moment ago

APK

DETECTION

DETAILS

RELATIONS

COMMUNITY

Security Vendors' Analysis

Avast	Android.Metasploit-G [PUP]	Avast-Mobile	Android.Metasploit-G [PUP]
AVG	Android.Metasploit-G [PUP]	Avira (no cloud)	ANDROID/Dldr.Agent.PAE.Gen
BitDefenderFalx	Android.Riskware.Metasploit.U	Cynet	Malicious (score: 99)
DrWeb	Android.RemoteCode.6833	ESET-NOD32	A Variant Of Android/TrojanDownloader...
Fortinet	Android/Agent.JNltr	Google	Detected
Ikarus	Trojan-Downloader.AndroidOS.Agent	Kaspersky	HEUR:Trojan-Downloader.AndroidOS.M...
QuickHeal	Android.Metasploit.B (PUP)	Sophos	Andr/Bckdr-RXM
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.AndroidOS.M...	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected

ClamAV	✔ Undetected	CMC	✔ Undetected
Comodo	✔ Undetected	Cyren	✔ Undetected
Emsisoft	✔ Undetected	eScan	✔ Undetected
F-Secure	✔ Undetected	GData	✔ Undetected
Gridinsoft (no cloud)	✔ Undetected	Jiangmin	✔ Undetected
K7AntiVirus	✔ Undetected	K7GW	✔ Undetected
Kingsoft	✔ Undetected	Lionic	✔ Undetected
Malwarebytes	✔ Undetected	MAX	✔ Undetected
MaxSecure	✔ Undetected	McAfee	✔ Undetected
McAfee-GW-Edition	✔ Undetected	Microsoft	✔ Undetected
NANO-Antivirus	✔ Undetected	Panda	✔ Undetected
Rising	✔ Undetected	Sangfor Engine Zero	✔ Undetected
SUPERAntiSpyware	✔ Undetected	Symantec	✔ Undetected
Symantec Mobile Insight	✔ Undetected	TACHYON	✔ Undetected
Tencent	✔ Undetected	Trellix (FireEye)	✔ Undetected
TrendMicro	✔ Undetected	TrendMicro-HouseCall	✔ Undetected
Trustlook	✔ Undetected	VBA32	✔ Undetected
VIPRE	✔ Undetected	VirIT	✔ Undetected
ViRobot	✔ Undetected	Yandex	✔ Undetected
Zillya	✔ Undetected	Zoner	✔ Undetected
CrowdStrike Falcon	🚫 Unable to process file type	Cybereason	🚫 Unable to process file type
Cylance	🚫 Unable to process file type	Elastic	🚫 Unable to process file type
Palo Alto Networks	🚫 Unable to process file type	SecureAge	🚫 Unable to process file type
SentinelOne (Static ML)	🚫 Unable to process file type	TEHTRIS	🚫 Unable to process file type
Trapmine	🚫 Unable to process file type	Webroot	🚫 Unable to process file type

Conclusion

This Application looks suspicious. most of the code was obfuscated.