Predefined Dictionary for suspected Malicious Behaviour

We have formulated the predefined dictionary for suspected malicious behaviour in APK file including Manifest, and dex file. We have collected this information based on literature review and listed all those suspected properties with pixel value.

Suspected API Calls:

API Call	Value
Ljavax/sql/ConnectionEvent;-><init>	250
Ljava/nio/channels/WritableByteChannel;->close	240
Landroid/service/carrier/CarrierService;->stopSelf	230
Landroid/opengl/Matrix;->getClass	220
Landroid/view/ViewStructure;->setCheckable	210
Landroid/text/method/BaseKeyListener;->getInputType	200
Landroid/provider/MediaStore$Images$Media;->wait	190
Ljava/lang/Runtime;->exec	180
Ljava/lang/System;->loadLibrary	180
Landroid/widget/AdapterView;->refreshDrawableState	170
Landroid/widget/MultiAutoCompleteTextView;->saveHierarchyState	170
Ljava/io/BufferedOutputStream;-><init>	160
Ljava/io/FileOutputStream;-><init>	160

Landroid/app/PendingIntent;->send	150
Landroid/app/AlarmManager;->Set	150
Landroid/app/NativeActivity;->getVolumeControlStream	140
Landroid/app/AcitivityManager;->killBackgroudProcess	140
Landroid/content/pm/PacakageManager;->removePackageFromPrefe	130
Landroid/content/pm/PacakageManager;->getInastallerPackageName	130
Landroid/content/pm/PacakageManager;->getInstalledPackages	130
Landroid/content/pm/PacakageManager;->getInstalledApplications	130
Landroid/content/Intent;->startActivity	120
Landroid/content/Intent;->getAction	120
Landroid/content/Intent;->setDataAndType	120
Landroid/content/ContentResolver;->delete	115
Landroid/content/ContentResolver;->update	115
Landroid/content/ContentResolver;->insert	115
Landroid/content/Context;->getPackageManager	115
Landroid/content/BroadcastReceiver;->abortBroadcast	115
Landroid/database/sqlote/SQLiteDatabase;->execSQL	110

Landroid/media/MediaRecorder;->MediaRecorder	100
Ljava/net/HttpURLConnection;->connect	95
Ljava/net/URLConnection-;>connect	95
Lorg/apache/http/impl/client;->DefaultHttpClient	90
Ljavax/crypto/Cipher;->getInstance	85
Ljavax/crypto/Cipher;->Init	85
Ljavax/crypto/Cipher;->doFinal	85
Landroid/telephony/TelephonyManager;->getDataActivity	80
Landroid/telephony/TelephonyManager;->getCallState	80
Landroid/telephony/TelephonyManager;->getLine1Number	80
Landroid/telephony/TelephonyManager;->getCellLocation	80
Landroid/telephony/TelephonyManager;->getSubscriberId	80
Landroid/telephony/TelephonyManager;->getDeviceId	80
Landroid/telephony/TelephonyManager;->getNetworkType	80
Landroid/telephony/TelephonyManager;->getSimOperator	80
Landroid/telephony/TelephonyManager;->getSimSerialNumber	80
Landroid/telephony/TelephonyManager;->getSimState	80

Landroid/telephony/TelephonyManager;->getSubscriberId	80
Landroid/telephony/SmsManager;->sendTextMessage	75
Landroid/telephony/SmsManager;->sendMultipartTextMessage	75
Landroid/telephony/SmsManager;->sendDataMessage	75
Landroid/telephony/SmsMessage;->getServiceCenterAddress	75
Landroid/telephony/gsm/SmsManager;->sendMultipartTextMessage	70
Landroid/telephony/gsm/SmsManager;->sendDataMessage	70
Landroid/telephony/gsm/SmsManager;->sendTextMessage	70
Landroid/telephony/gsm/SmsManager;->getDisplayOriginatingAddress	70
Landroid/telephony/gsm/SmsManager;->getDisplayMessageBody	70
Landroid/telephony/PhoneStateListener;->onCallStateChanged	65
Ldalvik/system/DexClassLoader;->loadClass	60
Ldalvik/system/PathClassLoader;->loadClass	60
Landroid/net/wifi/WifiInfo;->getSupplicantState	50
Landroid/net/wifi/WifiManager;->getConnectionInfo	40
Landroid/ContentResolver;->query	30
Landroid/location/LocationManager;->getLastKnownLocation	20

Suspected Permissions:

Permissions	Value
CAMERA	250
RECORD_AUDIO	240
READ_CONTACTS	230
READ_CALL_LOG	220
CALL_PHONE	210
WRITE_CALL_LOG	200
CHANGE_WIFI_STATE	190
READ_CALENDAR	180
ACCESS_WIFI_STATE	170
GET_ACCOUNTS	160
WAKE_LOCK	150
GET_TASKS	130
'VIBRATE'	120
PROCESS_OUTGOING_CALLS	110
SYSTEM_ALERT_WINDOWS	100
WRITE_SETTING	90

WRITE_EXTERNAL_STORAGE	80
READ_EXTERNAL_STORAGE	70
WRITE_CALENDAR	60
ACCESS_NETWORK_STATE	50
READ_HISTORY_BOOKMARKS	40

Suspected Declared (but not used) Permissions:

Permissions	**Value**
CAMERA	250
RECORD_AUDIO	230
READ_CONTACTS	210
READ_CALL_LOG	200
CALL_PHONE	190
WRITE_CALL_LOG	180
CHANGE_WIFI_STATE	170
GET_ACCOUNTS	160
READ_CALENDAR	140

ACCESS_WIFI_STATE	130
ACCESS_COARSE_LOCATION	120
ACCESS_FINE_LOCATION	110
READ_PHONE_STATE	90
WRITE_EXTERNAL_STORAGE	80
READ_EXTERNAL_STORAGE	70
ACCESS_NETWORK_STATE	60
WRITE_CALENDAR	50
SEND_SMS	40
READ_SMS	30

Suspected Activities:

Activity	**Value**
ACCESS_COARSE_LOCATION	250
ACCESS_FINE_LOCATION	240
READ_SMS	230
SEND_SMS	220

READ_PHONE_STATE	210
READ_CONTACTS	200
READ_HISTORY_BOOKMARKS	190
MOUNT_UNMOUNT_FILESYSTEMS	180
RECEIVE_SMS	170

Suspected Services:

Service	**Value**
SEND_SMS	160
READ_SMS	150
ACCESS_COARSE_LOCATION	140
ACCESS_FINE_LOCATION	130
READ_PHONE_STATE	120

Suspected Broadcast Receivers:

Receiver	**Value**
SEND_SMS	110
READ_SMS	100

ACCESS_COARSE_LOCATION	90
ACCESS_FINE_LOCATION	80
READ_PHONE_STATE	70

Suspected Intents:

Intent	**Value**
BOOT_COMPLETED	60
SMS_RECEIVED	50
BATTERY_CHANGE_ACTION	40
MOUNT_UNMOUNT_FILESYSTEMS	30

References:

[1] Android Malware Detection Using Fine-Grained Features
[2] PERMISSION ANALYSIS FOR ANDROID MALWARE DETECTION
[3] Android Malware Detection based on Useful API Calls and Machine Learning
[4] Mining API Calls and Permissions for Android Malware Detection