ANALYSIS-1

Monday, October 21, 2019 12:00 PM

Dogwar is a game . And thr apk name is dog war-beta:

LETS DECOMPILE THE CODE AND SEE WHY IT IS MALWARE AND WHAT ACTION PERFORMED BY THIS APPPLICATION.

I AM CHECKING THIS APPLICATION IN ANDROID 5.1 (LOLIPOP). YOU KNOW THAT IN ANDROID VERSION 5 OR BELOW THIS. THE PERMISSION I S AUTOMATICALLY SET AT RUN TIME. THERE IS NO ANY PROMPT TO AN USER TO GIVE PERMISSION. IT IS A FLAW IN ANDROID VERSION 5 OR BELOW: SO ANDROID UPGRADED THE VERSION . AND ABOVE THIS LIKE IN AND ROID MARSHMALLOW , OREO, PIE, YOU HAVE TO GIVE PERMISSION MANUALLY OR
OR GIVE PERMISSION ON RUN OF APPLICATION. IN ABOVE 5 VERSION THE PERMISSION IS NOT AUTOMATICALLY SET BY THE DEVICE.

.

1. **Lets decompile the apk , and read mainfest.xml file FIRST SEE AT PERMISSION :**

```
<supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true" android:smallScreens="false"/>
  <uses-permission android:name="android.permission.VIBRATE"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
  <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
  <uses-permission android:name="android.permission.SEND_SMS"/>
  <uses-permission android:name="android.permission.WRITE_SMS"/>
  <uses-permission android:name="android.permission.READ_CONTACTS"/>
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

This application can access sms , send sms, and also read all contacts.

```
<receiver android:name=".PuppyLoveWidgetProvider">
      <intent-filter>
        <action android:name="android.appwidget.action.APPWIDGET_UPDATE"/>
      </intent-filter>
```

There is broadcast receiver that receive on action android.appwidget.action.APPWIDGET_UPDATE.

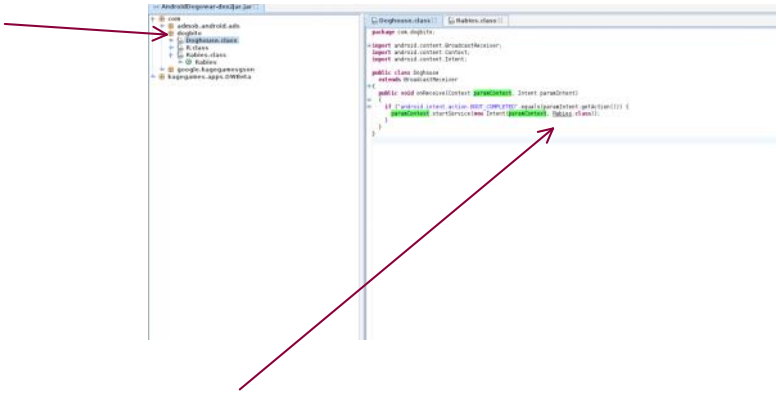
```
</activity>
    <service android:name="com.dogbite.Rabies">
      <intent-filter>
        <action android:name=".Rabies"/>
      </intent-filter>
---
```

There is a service name RABIES:

```
<receiver android:name="com.dogbite.Doghouse">
      <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
      </intent-filter>
    </receiver>
```

THERE IS A BROADCAT RECEIVER THAT RECEIVE THE BROADCAST ON MOBILE DEVICE BOOT

3. **NOW CONVERT DEX FILE INTO HUMAN READABLE FORMAT : BY DEX2JAR- AND OPEN WITH JD-GUI :**



on receive broadcast service rabies is started , lets see the Rabies.class and their functionality:

send text message to all contacts in the list

On start it reads all the contact no in device:

This malware not work in oreo/pie devices because in these devices . Developer have to register the broadcast receiver in java file not in manifest file.

https://medium.com/@iiro.krankka/its-time-to-kiss-goodbye-to-your-implicit-broadcastreceivers-eefafd9f4f8a