**App Name :** NomadNote

**Package Name : "com.devstories.nomadnote\_android"**

**Version Code : 32**

**Version Name :** 1.0.0

**Compile SDK version : 28**

**Build version code : 32**

**Minimum SDK version : 17**

**Target SDK version : 26**

1. This application is being validated for **spyware PHA**
2. Let us understand the definition of spyware again

Spyware track the activities of user’s mobile phone and collects the data like contacts, sms, call logs, history, files, audio etc and send it to the third parties or hacker without user consent.

1. Permissions responsible for spyware :

* android.permission.READ\_CONTACTS
* android.permission.RECEIVE\_SMS
* android.permission.READ\_SMS
* android.permission.READ\_EXTERNAL\_STORAGE
* android.permission.READ\_CALL\_LOG
* android.permission.RECORD\_AUDIO
* android.permission.READ\_CALENDER
* android.permission.ACCESS\_COARSE\_LOCATION
* android.permission.ACCESS\_FINE\_LOCATION
* com.android.browser.permission.READ\_HISTORY\_BOOKMARKS

1. Lets start reversing it.
2. We will check the spyware related permission in this app.





Here we can see list of permission like RECEIVE\_SMS, READ\_SMS, READ\_EXTERNAL\_STORAGE which is suspicious.

We will start with RECEIVE\_SMS.

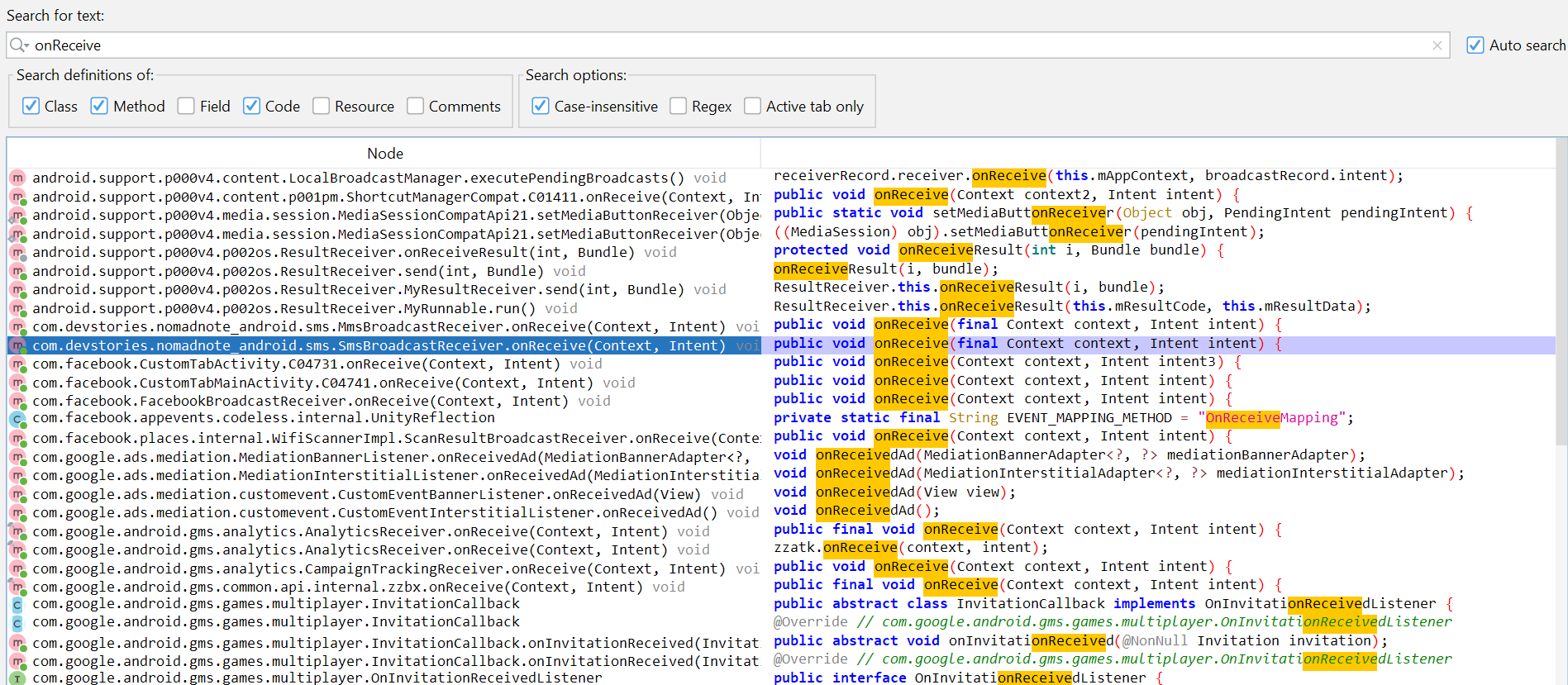
1. Before proceeding further , we will check whether this app is using any framework or not by using engineer danny framework as shown below.

A screenshot of a computer program

Description automatically generated

Here we can see that this app **is built using java/Kotlin.**

1. Now we will check search onReceive through lens icon as shown below



Here we will go with smsBroadCastReceiver package as highlighted above.

1. Now double click the searched result

A computer code with text

Description automatically generated with medium confidence



Here we can see that intent value is assigned to extras and extras is passed into **parseSMS**( ) method.

1. Now we will search **the declaration** of parseSMS( ) method to know where it is used further in code.

A computer code with text

Description automatically generated



Here we can see that str is passed into SmsRegisterOperation( ) constructor

1. Now we will check **declaration** of SmsRegisterOperation( )

A screenshot of a computer code

Description automatically generated



Here we can see that str is passed into contentsReference and contentsReference is passed into **registSms**( ) method of registerSms () method.

1. Now we will check **declaration** of registSms( ) method to know about this method.

A screenshot of a computer code

Description automatically generated



Here we can see that str is passed into requestParams and requestParams is passed to syncHttpClient.post( ) method and in this post method there is config.url

1. Now we will check config.url

A computer code with numbers and letters

Description automatically generated

Base url



Here we can see base url : "http://52.79.207.123"

Whole url is " <http://52.79.207.123/api/sms/regist_sms>" on which data is being sent.

1. Now we will check disclosure part with keyword like upload,sms,collect to check whether app is taking user consent or not.

On searching we are not getting any disclosure.

So from the above steps performed, we can conclude that app is sending data to an url without taking any user consent.

**So this app is spyware.**

**VERDICT - TTP**