androguard_demo

December 18, 2017

```
In [1]: from androguard.misc import *
        apk, dvm, vmx = AnalyzeAPK("3f33367040dc423ff97aab7196aa6748ff11cc45")
        apk.get_activities()

Out[1]: ['com.spynote.software.stubspynote.MainActivity',
         'com.spynote.software.stubspynote.screamon']

In [2]: apk.get_app_name()

Out[2]: u'wifi\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'

In [3]: apk.get_permissions()

Out[3]: ['android.permission.WRITE_SETTINGS',
         'android.permission.SYSTEM_ALERT_WINDOW',
         'android.permission.WRITE_EXTERNAL_STORAGE',
         'android.permission.SET_WALLPAPER',
         'android.permission.SET_WALLPAPER_HINTS',
         'android.permission.SEND_SMS',
         'android.permission.RECEIVE_BOOT_COMPLETED',
         'android.permission.KILL_BACKGROUND_PROCESSES',
         'android.permission.VIBRATE',
         'android.permission.CAMERA',
         'android.permission.GET_ACCOUNTS',
         'android.permission.WAKE_LOCK',
         'android.permission.ACCESS_NETWORK_STATE',
         'android.permission.WRITE_CONTACTS',
         'android.permission.READ_CONTACTS',
         'android.permission.WRITE_EXTERNAL_STORAGE',
         'android.permission.RECORD_AUDIO',
         'android.permission.READ_SMS',
         'android.permission.ACCESS_WIFI_STATE',
         'android.permission.CHANGE_WIFI_STATE',
         'android.permission.READ_CALL_LOG',
         'android.permission.INTERNET',
         'android.permission.READ_PHONE_STATE',
         'android.permission.CALL_PHONE',
         'android.permission.ACCESS_COARSE_LOCATION',
          'android.permission.ACCESS_FINE_LOCATION',
          'android.permission.RECEIVE_BOOT_COMPLETED']
```

```
In [4]: dvm.get_strings()[10:20]
```

```
Out[4]: [u'  #',
         u'  Canceling: ',
         u'  Created new loader ',
         u'  Current loader is running; attempting to cancel',
         u'  Current loader is stopped; replacing',
         u'  Destroying: ',
         u'  Enqueuing as new pending loader',
         u'  Filter did not match: ',
         u'  Filter matched!  match=0x',
         u"  Filter's target already added"]
```

```
In [5]: dvm.get_classes()[:10]
```

```
Out[5]: [<androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3050>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c30d0>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3110>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3150>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3190>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c31d0>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3210>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3250>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c3290>,
         <androguard.core.bytecodes.dvm.ClassDefItem at 0x7f8a807c32d0>]
```

```
In [6]: dvm.get_methods()[:10]
```

```
Out[6]: [<androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251dd0>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251e50>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251e90>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251ed0>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251f10>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251f90>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a251fd0>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a25b090>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a25b0d0>,
         <androguard.core.bytecodes.dvm.EncodedMethod at 0x7f8a7a25b150>]
```

```
In [7]: method = dvm.get_methods()[535]
        method.get_class_name()
```

```
Out[7]: u'Landroid/support/v4/app/ActivityCompat;'
```

```
In [8]: print(method.get_source())
```

```
    public android.net.Uri getReferrer(android.app.Activity p6)
    {
        int v1_0;
        if (android.os.Build$VERSION.SDK_INT < 22) {
            android.content.Intent v0 = p6.getIntent();
            v1_0 = ((android.net.Uri) v0.getParcelableExtra("android.intent.extra.REFERRER"));
            if (v1_0 == 0) {
                String v2 = v0.getStringExtra("android.intent.extra.REFERRER_NAME");
                if (v2 == null) {
                    v1_0 = 0;
                } else {
                    v1_0 = android.net.Uri.parse(v2);
                }
            }
        } else {
            v1_0 = android.support.v4.app.ActivityCompat22.getReferrer(p6);
        }
        return v1_0;
    }
```

```
In [9]: method.get_name()

Out[9]: u'getReferrer'

In [10]: from androguard.core.bytecode import PrettyShow
         method_analysis = vmx.get_method(method)
         method_analysis

Out[10]: <androguard.core.analysis.analysis.MethodAnalysis at 0x7f8a71f2fd50>

In [11]: PrettyShow(method_analysis, method_analysis.basic_blocks.get())

getReferrer-BB@0x0 :
        0  (00000000) sget                 v3, Landroid/os/Build$VERSION;->SDK_INT I
        1  (00000004) const/16             v4, 22
        2  (00000008) if-lt                v3, v4, 7 [ getReferrer-BB@0xc getReferrer-BB@0x16 ]

getReferrer-BB@0xc :
        3  (0000000c) invoke-static        v6, Landroid/support/v4/app/ActivityCompat22;->getRefe
        4  (00000012) move-result-object   v1 [ getReferrer-BB@0x14 ]

getReferrer-BB@0x14 :
        5  (00000014) return-object        v1

getReferrer-BB@0x16 :
        6  (00000016) invoke-virtual       v6, Landroid/app/Activity;->getIntent()Landroid/conten
        7  (0000001c) move-result-object  v0
        8  (0000001e) const-string        v3, u'android.intent.extra.REFERRER'
        9  (00000022) invoke-virtual      v0, v3, Landroid/content/Intent;->getParcelableExtra(L
        10 (00000028) move-result-object  v1
        11 (0000002a) check-cast          v1, Landroid/net/Uri;
        12 (0000002e) if-nez              v1, -13 [ getReferrer-BB@0x32 getReferrer-BB@0x14 ]

getReferrer-BB@0x32 :
        13 (00000032) const-string        v3, u'android.intent.extra.REFERRER_NAME'
        14 (00000036) invoke-virtual      v0, v3, Landroid/content/Intent;->getStringExtra(Ljava
        15 (0000003c) move-result-object  v2
        16 (0000003e) if-eqz              v2, 7 [ getReferrer-BB@0x42 getReferrer-BB@0x4c ]

getReferrer-BB@0x42 :
        17 (00000042) invoke-static       v2, Landroid/net/Uri;->parse(Ljava/lang/String;)Landro
        18 (00000048) move-result-object  v1
        19 (0000004a) goto                -27 [ getReferrer-BB@0x14 ]

getReferrer-BB@0x4c :
        20 (0000004c) const/4             v1, 0
        21 (0000004e) goto                -29 [ getReferrer-BB@0x14 ]
```