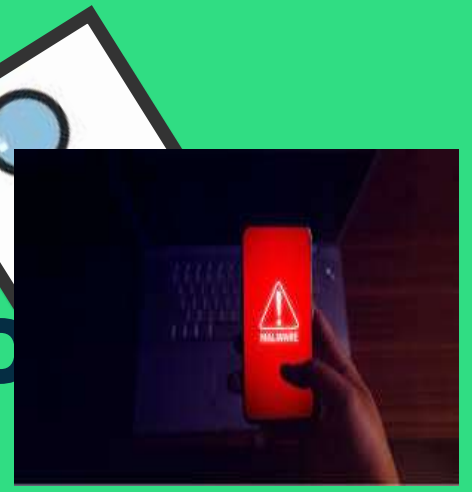
Analyse d’applicatio portefeuilles et trading



* Realise par achraf benchehla
*encadré par : MR.koulali Mohamed-amine

sécurité mobile

#-Plan de projet-#

- Introduction .
- Definitions des notions et outils de base
- Analyse statique
- Analyse dynamique
- Conclusion

Introduction

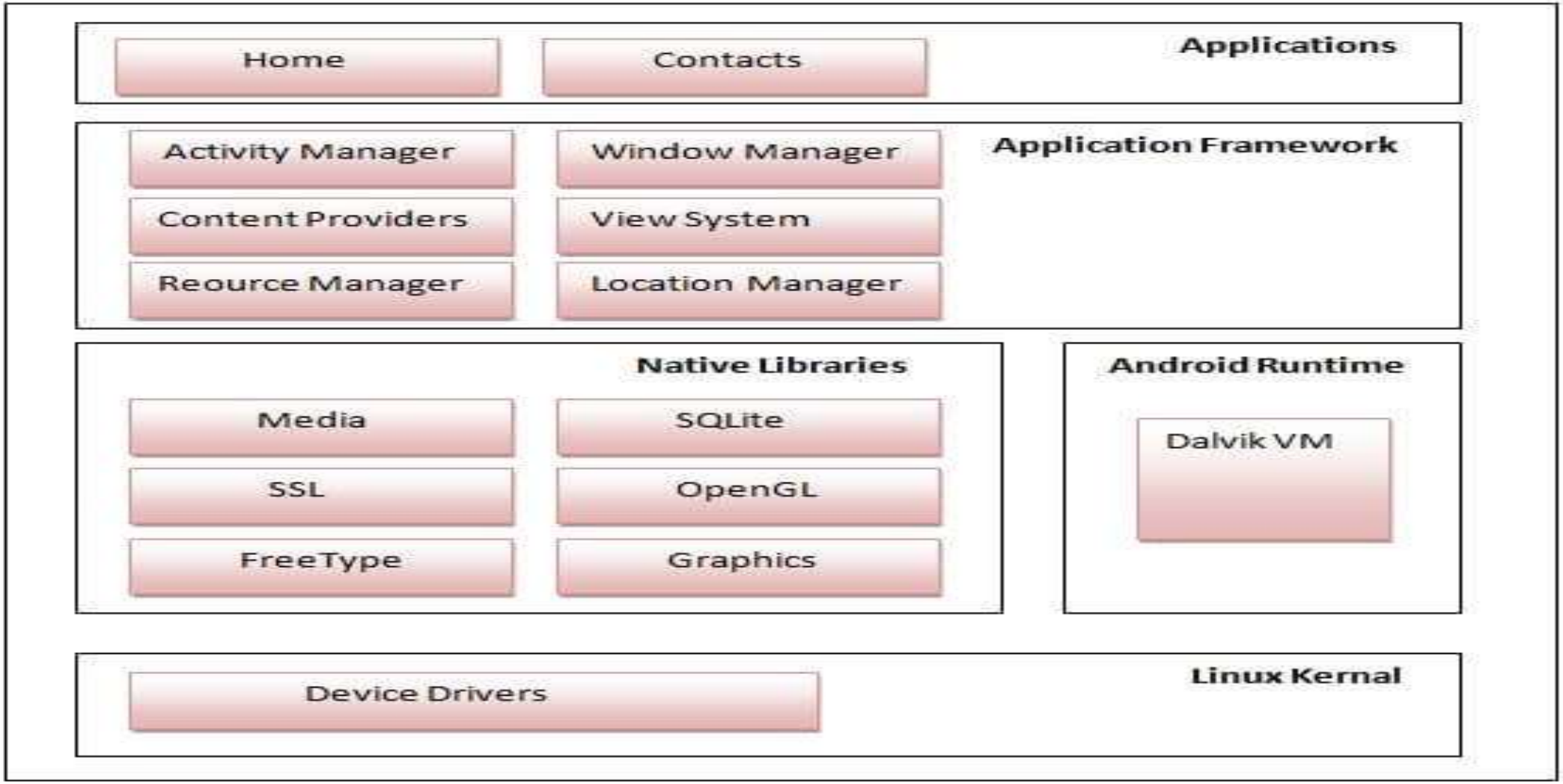
- Trading –
- Android
- App de trading -

android

C’est quoi un android ?

- Android est le système d'exploitation mobile crée par Google. Il équipe la majorité des téléphones portables du moment (smartphones). Son principal concurrent est Apple avec l'iPhone. Android est un système vous permettant de personnaliser votre téléphone, télécharger des applications (navigateur Internet, GPS, Facebook...). Android équipe également les tablettes tactiles.

android


Home
Contacts
Applications
Activity Manager
Window Manager
Application Framework
Content Providers
View System
Reource Manager
Location Manager
Native Libraries
Android Runtime
Media
SQLite
Dalvik VM
SSL
OpenGL
FreeType
Graphics
Linux Kernal
Device Drivers

android

Application de trading

- Une application de trading mobile est un logiciel spécialement conçu pour être utilisé sur un appareil mobile. Il peut s'agir d'un smartphone ou d'une tablette exécutant un système d'exploitation mobile Android ou iOS.

- L'aspect et la convivialité seront légèrement différents par rapport au logiciel que vous utiliseriez si vous aviez recours à une plateforme de trading en ligne via le navigateur de votre téléphone, ou un logiciel installé sur votre MAC ou PC

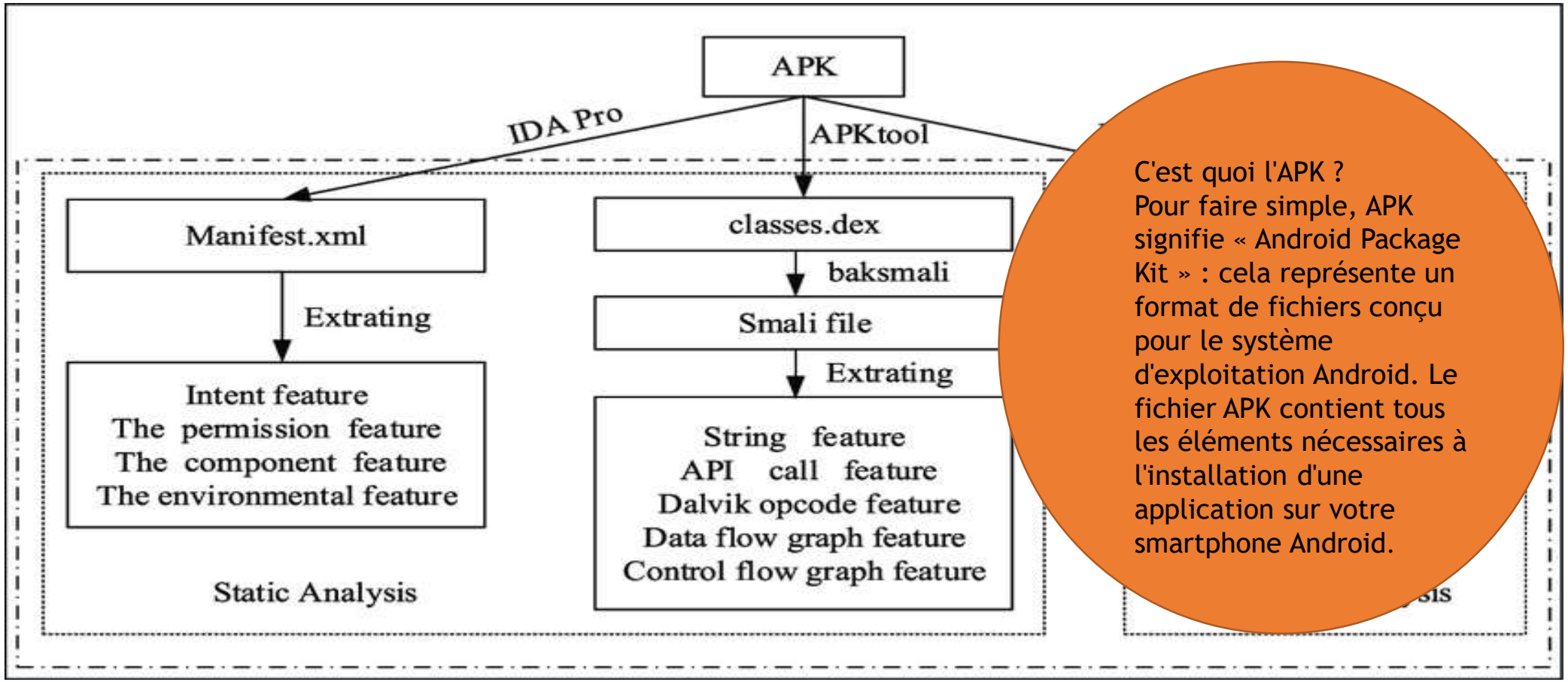
Le trading

- *Le trading d'actions consiste à acheter et à vendre fréquemment des actions dans le but de chronométrer le marché. L'objectif des négociants en bourse est de capitaliser sur les événements du marché à court terme pour vendre des actions à profit ou acheter des actions à un prix bas.*

Definitions des notions et outils de base

android

Analyse statique d'une application



C'est quoi l'APK ?
Pour faire simple, APK signifie « Android Package Kit » : cela représente un format de fichiers conçu pour le système d'exploitation Android. Le fichier APK contient tous les éléments nécessaires à l'installation d'une application sur votre smartphone Android.

android

L’analyse statique consiste à décompiler l’application afin d’en étudier le code. Cette méthode appelée reverse-engineering, a pour défaut que le temps passé à analyser le code peut être considéré comme du temps en moins pour tester la sécurité de l’application.

Normalement toutes les vulnérabilités du côté client peuvent être détectées sans avoir à lancer le code, mais dans la pratique, cela se révèle plus compliqué. L’objectif de l’analyse de code sera donc plutôt de détecter des problèmes de sécurité plus ou moins évidents et de se faire une idée sur la sécurité globale de l’application.

Jadx-gui ?

- *A quoi sert JADX ?*
- *JADX est utilisé pour convertir le code DEX/Smali en code source Java . Notez que le JADX GitHub mentionne "JDK 8 ou supérieur doit être installé" mais j'ai exécuté les deux commandes ci-dessus au cas où. JRE est l'environnement d'exécution Java, qui permet d'exécuter du code Jav*

AndroidManifest.xml

- Le fichier AndroidManifest.xml contient des informations sur votre package , y compris les composants de l'application tels que les activités, les services, les récepteurs de diffusion, les fournisseurs de contenu, etc.
- Il effectue également d'autres tâches :
- Il est responsable de protéger l'application pour accéder à toutes les parties protégées en fournissant les autorisations.
- Il déclare également l'API Android que l'application va utiliser.
- Il répertorie les classes d'instrumentation . Les classes d'instrumentation fournissent le profilage et d'autres informations. Ces informations sont supprimées juste avant la publication de l'application, etc.
- Il s'agit du fichier xml requis pour toutes les applications Android et situé dans le répertoire racine.

* Fichier Android _R.java_ *

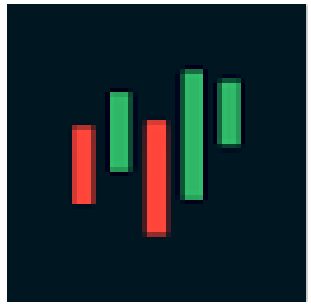
- *Android R.java est un fichier généré automatiquement par aapt (Android Asset Packaging Tool) qui contient les ID de ressource pour toutes les ressources du répertoire res/.*

- *Si vous créez un composant dans le fichier activity_main.xml, l'identifiant du composant correspondant est automatiquement créé dans ce fichier. Cet identifiant peut être utilisé dans le fichier source de l'activité pour effectuer n'importe quelle action sur le composant.*

Analyse statique des apps

android

Applications de trading & portefeuille

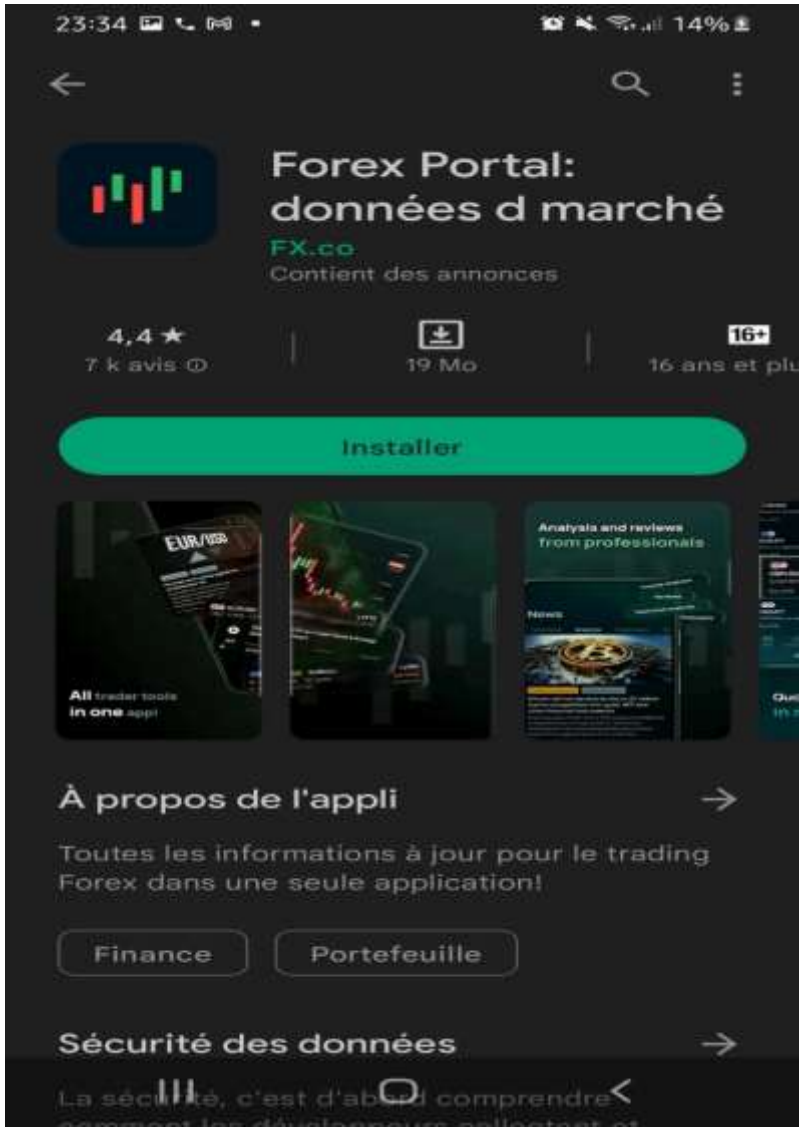


Forex portal

android

Forex portal : donnes de marche

SCAN ME



android

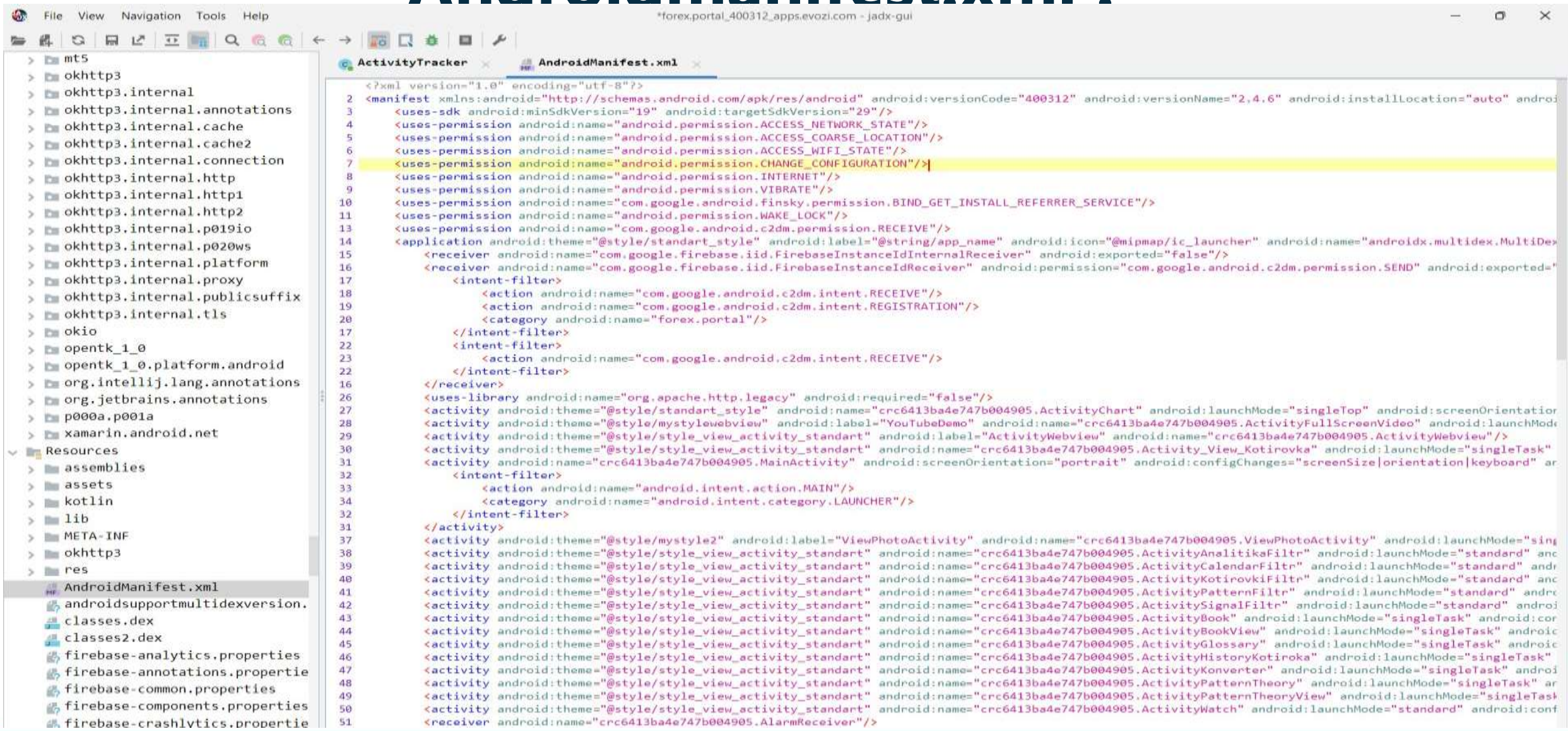
On ouvre apk avec jadx

- On cherche application sur google play store et ou obtient url de l'app puit on la trasnforme sous la forme .apk

- :

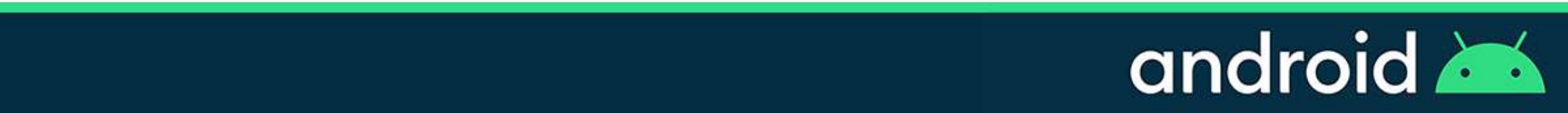
- on ouvre l' apk avec jadx :

Androidmanifest.xml :

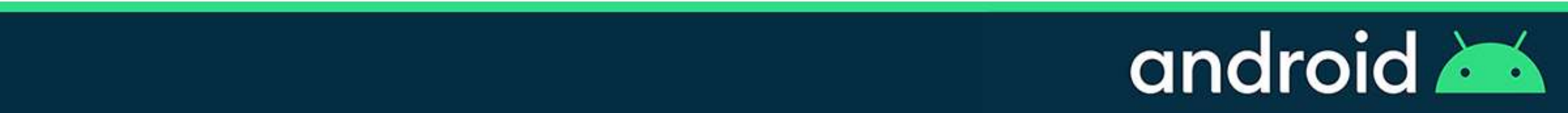


android

```
<activity android:name="crc6413ba4e747b004905.MainActivity" android:screenOrientation="portrait" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
<activity android:theme="@style/mystyle2" android:label="ViewPhotoActivity" android:name="crc6413ba4e747b004905.ViewPhotoActivity" android:launchMode="singleTask" android:screenOrientation="sensor" android:configChanges="keyboard|orientation|screenSize" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityAnalitikaFiltr" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityCalendarFiltr" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityKotirovkiFiltr" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityPatternFiltr" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivitySignalFiltr" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityBook" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityBookView" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityGlossary" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityHistoryKotiroka" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityKonverter" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityPatternTheory" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityPatternTheoryView" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityWatch" android:launchMode="standard" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<receiver android:name="crc6413ba4e747b004905.AlarmReceiver" />
<receiver android:name="crc6413ba4e747b004905.AlarmReciverUser" />
<service android:name="mt5.MyFirebaseListenerService">
    <intent-filter>
        <action android:name="com.google.firebase.MESSAGING_EVENT" />
    </intent-filter>
</service>
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityAddingAnalitika" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityNewsAdding" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivityStartSub" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc6413ba4e747b004905.ActivitySubscribingMain" android:launchMode="singleTask" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc648102bd9d67589d93.ActivitySettings" android:launchMode="standard" android:configChanges="keyboard|orientation|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc64e087220af55cc7fe.CurrentLessonActivity" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc64e087220af55cc7fe.LessonsActivity" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc64e087220af55cc7fe.LessonsThemsActivity" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<activity android:theme="@style/style_view_activity_standart" android:name="crc64e087220af55cc7fe.TestingActivity" android:launchMode="standard" android:configChanges="keyboard|screenSize" android:windowSoftInputMode="adjustPan" />
<service android:name="crc640f1fe57ce48cbf60.MetricaMonoRuntimeLoaderService" android:process=":Metrica" />
<provider android:name="mono.android.MultiDexLoader" android:exported="false" android:authorities="forex.portal.mono.android.MultiDexLoader.__mono_init__" android:initOrder="1999999999" />
<provider android:name="mono.MonoRuntimeProvider" android:exported="false" android:authorities="forex.portal.mono.MonoRuntimeProvider.__mono_init__" android:initOrder="1999999998" />
<provider android:name="mono.MonoRuntimeProvider_1" android:exported="false" android:process=":Metrica" android:authorities="forex.portal.mono.MonoRuntimeProvider_1.__mono_init__" android:initOrder="1999999997" />
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version" />
<provider android:name="com.google.firebase.provider.FirebaseInitProvider" android:exported="false" android:authorities="forex.portal.firebaseinitprovider" android:initOrder="100" android:directBootAware="true" />
<service android:name="com.google.firebase.components.ComponentDiscoveryService" android:exported="false" android:directBootAware="true">
    <meta-data android:name="com.google.firebase.components:com.google.firebase.dynamicloading.DynamicLoadingRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.installations.FirebaseInstallationsRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.analytics.connector.internal.AnalyticsConnectorRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.iid.Registrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.datatransport.TransportRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.messaging.FirebaseMessagingRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
```



```
        <meta-data android:name="com.google.firebase.components:com.google.firebase.analytics.connector.internal.AnalyticsConnectorRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
        <meta-data android:name="com.google.firebase.components:com.google.firebase.iid.Registrar" android:value="com.google.firebase.components.ComponentRegistrar" />
        <meta-data android:name="com.google.firebase.components:com.google.firebase.datatransport.TransportRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
        <meta-data android:name="com.google.firebase.components:com.google.firebase.messaging.FirebaseMessagingRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
        <meta-data android:name="com.google.firebase.components:com.google.firebase.crashlytics.CrashlyticsRegistrar" android:value="com.google.firebase.components.ComponentRegistrar" />
    </service>
    <receiver android:name="com.google.android.gms.measurement.AppMeasurementReceiver" android:enabled="true" android:exported="false" />
    <service android:name="com.google.android.gms.measurement.AppMeasurementService" android:enabled="true" android:exported="false" />
    <service android:name="com.google.android.gms.measurement.AppMeasurementJobService" android:permission="android.permission.BIND_JOB_SERVICE" android:enabled="true" android:exported="false" />
    <activity android:theme="@android:style/Theme.Translucent.NoTitleBar" android:name="com.google.android.gms.common.api.GoogleApiActivity" android:exported="false" />
    <service android:name="com.google.firebase.messaging.FirebaseMessagingService" android:exported="false" android:directBootAware="true">
        <intent-filter android:priority="-500">
            <action android:name="com.google.firebase.MESSAGING_EVENT" />
        </intent-filter>
    </service>
    <service android:name="com.google.android.datatransport.runtime.backends.TransportBackendDiscovery" android:exported="false">
        <meta-data android:name="backend:com.google.android.datatransport.cct.CctBackendFactory" android:value="cct" />
    </service>
    <service android:name="com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService" android:permission="android.permission.BIND_JOB_SERVICE" android:exported="false" />
    <receiver android:name="com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver" android:exported="false" />
    <service android:name="com.yandex.metrica.MetricaService" android:enabled="true" android:exported="true" android:process=":Metrica">
        <intent-filter>
            <category android:name="android.intent.category.DEFAULT" />
            <action android:name="com.yandex.metrica.IMetricaService" />
            <data android:scheme="metrica" />
        </intent-filter>
        <meta-data android:name="metrica:api:level" android:value="81" />
    </service>
    <service android:name="com.yandex.metrica.ConfigurationService" android:enabled="true" android:exported="false" android:process=":Metrica">
        <meta-data android:name="metrica:configuration:api:level" android:value="3" />
        <intent-filter>
            <action android:name="com.yandex.metrica.configuration.ACTION_INIT" />
        </intent-filter>
    </service>
    <service android:name="com.yandex.metrica.ConfigurationJobService" android:permission="android.permission.BIND_JOB_SERVICE" android:enabled="true" android:exported="false" android:process=":Metrica" />
    <receiver android:name="com.yandex.metrica.MetricaEventHandler" android:enabled="true" android:exported="true">
        <intent-filter>
            <action android:name="com.android.vending.INSTALL_REFERRER" />
        </intent-filter>
    </receiver>
  </application>
</manifest>
```



android.permission.ACCESS_COARSE_LOCATION

Accédez à des sources de localisation grossières, telles que la base de données du réseau mobile, pour déterminer un emplacement approximatif du téléphone, le cas échéant. Des applications malveillantes peuvent l'utiliser pour déterminer approximativement où vous vous trouvez.

android.permission.CHANGE_CONFIGURATION

Permet à une application de modifier la configuration actuelle, telle que les paramètres régionaux ou la taille de police globale.

android.permission.INTERNET

Permet à une application de créer des sockets réseau.

com.google.android.c2dm.permission.RECEIVe

Autorisation pour la messagerie cloud vers appareil.

android.permission.VIBRATE

Permet à l'application de contrôler le vibreur.

Apk signature :

android

App has a Network Security Configuration [android:networkSecurityConfig=@xml/net_security]

La fonctionnalité de configuration de la sécurité réseau permet aux applications de personnaliser leurs paramètres de sécurité réseau dans un fichier de configuration sûr et déclaratif sans modifier le code de l'application. Ces paramètres peuvent être configurés pour des domaines spécifiques et pour une application spécifique.

Icône de validation par la communauté

Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.
Permission: com.google.android.c2dm.permission.SEND [android:exported=true]

Un récepteur de diffusion se trouve être partagé avec d'autres applications sur l'appareil, le laissant ainsi accessible à toute autre application sur l'appareil. Il est protégé par une permission qui n'est pas définie dans l'application analysée. Par conséquent, le niveau de protection de l'autorisation doit être vérifié là où il est défini. S'il est défini sur normal ou dangereux, une application malveillante peut demander et obtenir l'autorisation et interagir avec le composant. S'il est défini sur signature, seules les applications signées avec le même certificat peuvent obtenir l'autorisation.

Cette application peut avoir des capacités de détection de racine.

```
@NonNull
public static com.yandex.metrica.b a(@NonNull Context context) {
    DisplayMetrics displayMetrics = context.getResources().getDisplayMetrics();
    Point b2 = b(context);
    int i = b2.x;
    int i2 = b2.y;
    float f = displayMetrics.density;
    float f2 = i;
    float f3 = i2;
    float min = Math.min(f2 / f, f3 / f);
    float f4 = f * 160.0f;
    float f5 = f2 / f4;
    float f6 = f3 / f4;
    double sqrt = Math.sqrt((f5 * f5) + (f6 * f6));
    if (a(context, sqrt)) {
        return com.yandex.metrica.b.TV;
    }
    if (sqrt >= 7.0d || min >= 600.0f) {
        return com.yandex.metrica.b.TABLET;
    }
    return com.yandex.metrica.b.PHONE;
}
```

L'application utilise un générateur de nombres aléatoires non sécurisé.

```java
package com.yandex.metrica.impl.ob;

import android.support.annotation.NonNull;
import java.util.Random;
/* loaded from: classes.dex */
public class tk {
    @NonNull

    /* renamed from: a  reason: collision with root package name */
    private final Random f682a;

    public tk() {
        this(new Random());
    }

    public tk(@NonNull Random random) {
        this.f682a = random;
    }

    public long a(long j, long j2) {
        if (j >= j2) {
            throw new IllegalArgumentException("min should be less than max");
        }
        long nextLong = this.f682a.nextLong();
        if (nextLong == Long.MIN_VALUE) {
            nextLong = 0;
        } else if (nextLong < 0) {
            nextLong = -nextLong;
        }
        return j + (nextLong % (j2 - j));
    }
}
```

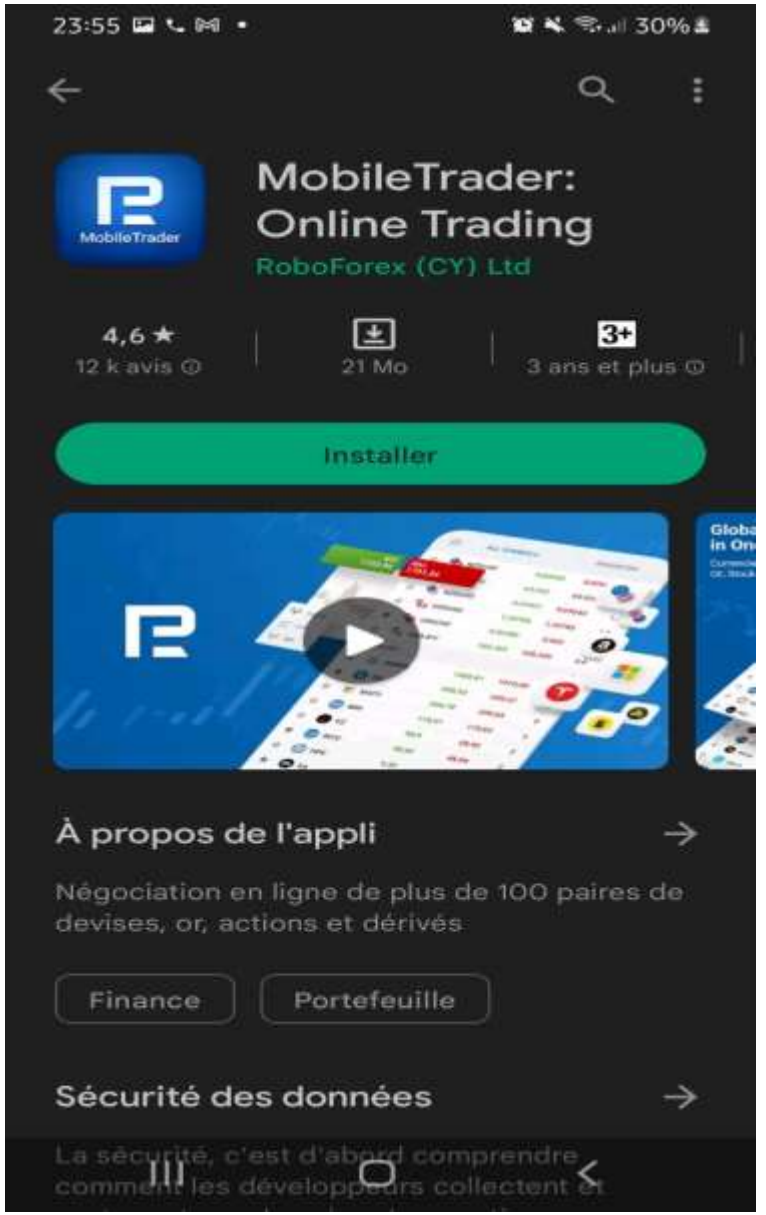
Cette application écoute les modifications du Presse-papiers. Certains logiciels malveillants écoutent également les modifications apportées au Presse-papiers.
Icône de validation par la communauté

```
import mono.android.IGCUserPeer;
import mono.android.Runtime;
import mono.android.TypeManager;
/* loaded from: classes2.dex */
public class ClipboardManager_OnPrimaryClipChangedListenerImplementor implements IGCUserPeer, ClipboardManager.OnPrimaryClipChangedListener {
    public static final String __md_methods = "n_onPrimaryClipChanged:()V:GetOnPrimaryClipChangedHandler:Android.Content.ClipboardManager/IOnPrimaryClipChangedListenerInvoker, Mono.Android, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null\n";
    private ArrayList refList;

    private native void n_onPrimaryClipChanged();

    static {
        Runtime.register("Android.Content.ClipboardManager+IOnPrimaryClipChangedListenerImplementor, Mono.Android", ClipboardManager_OnPrimaryClipChangedListenerImplementor.class, __md_methods);
    }

    public ClipboardManager_OnPrimaryClipChangedListenerImplementor() {
        if (ClipboardManager_OnPrimaryClipChangedListenerImplementor.class == ClipboardManager_OnPrimaryClipChangedListenerImplementor.class) {
            TypeManager.Activate("Android.Content.ClipboardManager+IOnPrimaryClipChangedListenerImplementor, Mono.Android", "", this, new Object[0]);
        }
    }

    @Override // android.content.ClipboardManager.OnPrimaryClipChangedListener
    public void onPrimaryClipChanged() {
        n_onPrimaryClipChanged();
    }

    @Override // mono.android.IGCUserPeer
    public void monodroidAddReference(Object obj) {
        if (this.refList == null) {
            this.refList = new ArrayList();
        }
        this.refList.add(obj);
    }

    @Override // mono.android.IGCUserPeer
    public void monodroidClearReferences() {
        ArrayList arrayList = this.refList;
        if (arrayList != null) {
            arrayList.clear();
        }
    }
}
```

android

Mobile trader: online trading

SCAN ME



android