Twitter Thread by Elliot Alderson



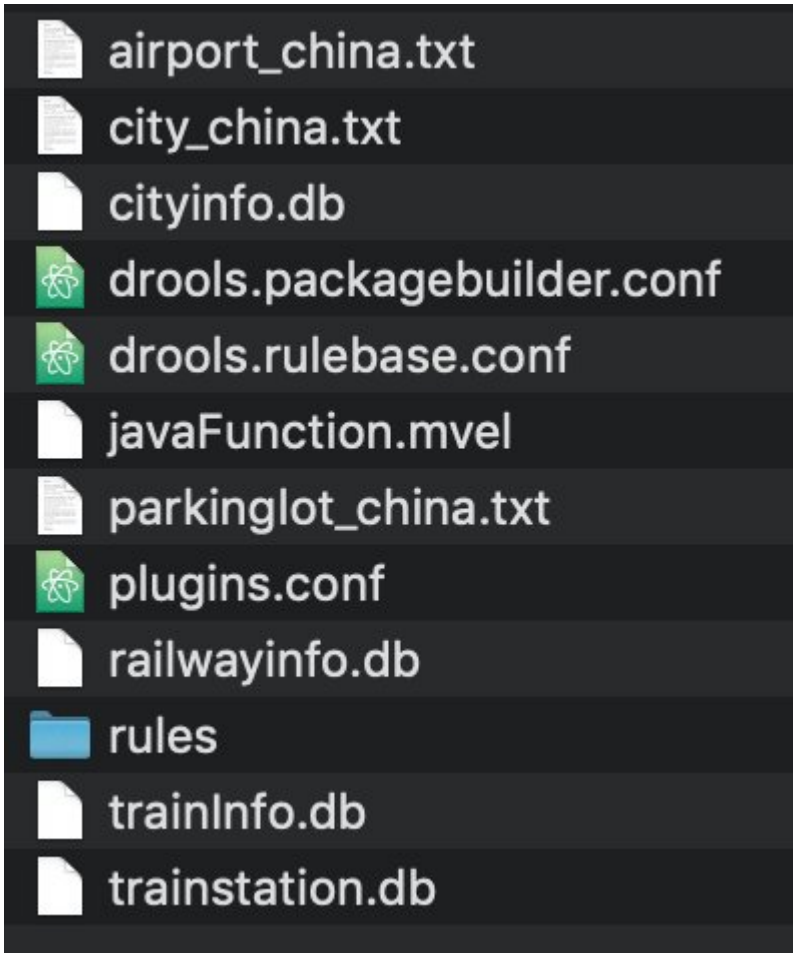
Elliot Alderson
@fs0c131y

THREAD: I'm looking at a Huawei P20 from China, let see what can I found

The 1st app I reversed is an app called Decision

Look at the name of the files contains in the assets folder:
- airport_china.txt
- city_china.txt
- cityinfo.db
- parkinglot_china.txt
- railwayinfo.db
- trainInfo.db
- trainstation.db

Interesting, no?



For example, the trainstation database contains:

- address
- name
- latitude
- longitude
- city

stationId	address	name	latitude	longitude	city	
1	黑龙江省哈尔滨市阿城区会宁路61号	阿城站	45.550814	126.996564	哈尔滨市	{"address":"黑龙江省哈尔滨市阿城区会宁路6
2	内蒙古自治区呼伦贝尔盟鄂伦春自治旗阿里河镇	阿里河站	50.580182	123.730512		{"address":"内蒙古自治区呼伦贝尔盟鄂伦春自
3	内蒙古自治区呼伦贝尔根河市阿龙山镇	阿龙山站	51.688821	121.879528	根河市	{"address":"内蒙古自治区呼伦贝尔根河市阿龙
4	黑龙江省大兴安岭地区漠河县劲涛镇	阿木尔站	52.86145	123.162635		{"address":"黑龙江省大兴安岭地区漠河县劲涛
5	黑龙江省安达市铁路街	安达站	46.402478	125.32266	安达市	{"address":"黑龙江省安达市铁路街","longitud
6	黑龙江省五常市安家镇	安家站	45.0524	127.067871	五常市	{"address":"黑龙江省五常市安家镇","longitud
7	黑龙江省齐齐哈尔市昂昂溪区陵园路23号	昂昂溪站	47.162148	123.814617	齐齐哈尔市	{"address":"黑龙江省齐齐哈尔市昂昂溪区陵园
8	黑龙江省穆棱市八面通镇	八面通站	44.92653	130.541867	穆棱市	{"address":"黑龙江省穆棱市八面通镇","longit
9	内蒙古自治区牙克石市巴林镇巴林车站	巴林站	48.315174	122.333892	牙克石市	{"address":"内蒙古自治区牙克石市巴林镇巴林
10	黑龙江省哈尔滨市呼兰区白奎镇	白奎堡站	46.371251	127.003721	哈尔滨市	{"address":"黑龙江省哈尔滨市呼兰区白奎镇",
11	黑龙江省林口县龙爪乡宝林村	宝林站	45.027713	129.979522		{"address":"黑龙江省林口县龙爪乡宝林村","l
12	黑龙江省鹤岗市萝北县宝泉岭镇哈萝公路西侧	宝泉岭站	47.430318	130.522742	鹤岗市	{"address":"黑龙江省鹤岗市萝北县宝泉岭镇哈
13	黑龙江省北安市	北安站	48.235688	126.512368	北安市	{"address":"黑龙江省北安市","longitude":126
14	黑龙江省五常市背荫河镇	背荫河站	45.171142	126.998595	五常市	{"address":"黑龙江省五常市背荫河镇","longit
15	黑龙江省双鸭山市集贤兴安乡	笔架山站	46.787457	131.003417	双鸭山市	{"address":"黑龙江省双鸭山市集贤兴安乡","l
16	黑龙江省哈尔滨市道外区滨江街28号	滨江站	45.775869	126.655948	哈尔滨市	{"address":"黑龙江省哈尔滨市道外区滨江街2
17	黑龙江省勃利县城西街站前路84号	勃利站	45.755934	130.559839		{"address":"黑龙江省勃利县城西街站前路84
18	内蒙古自治区牙克石市博克图镇大直街博克图站	博克图站	48.754412	121.918525	牙克石市	{"address":"内蒙古自治区牙克石市博克图镇大
19	黑龙江省海林市柴河镇	柴河站	44.767355	129.686489	海林市	{"address":"黑龙江省海林市柴河镇","longitud
20	黑龙江省海林市	长汀镇站	44.467028	128.934858	海林市	{"address":"黑龙江省海林市","longitude":128
21	黑龙江省黑河市孙吴县辰清镇	辰清站	49.141681	127.238722	黑河市	{"address":"黑龙江省黑河市孙吴县辰清镇","l
22	黑龙江省伊春市南岔区晨明镇	晨明站	46.97526	129.489985	伊春市	{"address":"黑龙江省伊春市南岔区晨明镇","l

In the manifest of this application, there is a GeoReceiver

```
<receiver android:name="com.huawei.ca.geofence.GeoReceiver" android:permission="huawei.permission.CASERVICE">
    <intent-filter>
        <action android:name="com.huawei.decision.action.GEO_ALARM_TRIGGERED"/>
    </intent-filter>
</receiver>
```

This receiver is receiving an UUID and will lookup an known fence id

```
public class GeoReceiver extends BroadcastReceiver {

    public void onReceive(Context context, Intent intent) {
        if (intent != null && "com.huawei.decision.action.GEO_ALARM_TRIGGERED".equals(intent.getAction())) {
            String stringExtra = intent.getStringExtra("alarmid");
            f.a("GeoReceiver", "receive uuid = " + stringExtra);
            if (!TextUtils.isEmpty(stringExtra)) {
                Object fenceIdByUUID = GeoFence.getFenceIdByUUID(stringExtra);
                if (TextUtils.isEmpty(fenceIdByUUID)) {
                    f.a("GeoReceiver", "match no fence id.");
                    a.a(stringExtra);
                    return;
                }

                d.a(new EnterGeoFenceEvent(fenceIdByUUID));
            }
        }
    }
}
```

I'm a stupid security researcher. For the moment, the keywords are: train, airport, city, geo fence... Do you see where we are going?

In the data folder, there is a file called CalcMain. Here some of the methods of this class:
- callGetBusTime
- callGetTaxiTime
- isTrafficBusy
- callGetHomeCity
- callHasHotelTicket
- callGetAirportMultiPoi
- callHasGroupBuyingTicket
- ...

```
callIsServiceTimeConflict(): boolean
callIsServiceTimeConflict(Object...): Object
callIsPoiAtHome(): boolean
callIsPoiAtHomeAtGeoPoint(GeoPoint): boolean
callIsPoiAtCompanyAtGeoPoint(GeoPoint): boolean
callIsPoiAtWorkPlace(): boolean
callIsPoiAtFamiliarPlace(): double
callIsPoiAtFamiliarPlace(Object...): Object
callIsWalkingMode(Object...): Object
callIsStillMode(Object...): Object
callInTime(double, double): boolean
callInTime(Date, double, double): boolean
callInTime(Calendar, double, double): boolean
callGetBusTime(Object...): double
callGetBusTime(GeoPoint, GeoPoint): double
callGetTaxiTime(GeoPoint, GeoPoint): double
callGetTaxiTime(Object...): Object
isTrafficBusy(): boolean
```

Nice data types haha

```java
public final class DataTypes {
    public static final String TYPE_ACTION = "Action";
    public static final String TYPE_CALENDAR = "Calendar";
    public static final String TYPE_CONCERNED_PLANE = "ConcernedPlane";
    public static final String TYPE_CONCERNED_TRAIN = "ConcernedTrain";
    public static final String TYPE_DAILY_SCHEDULE = "DailySchedule";
    public static final String TYPE_EXPRESS_CABINET = "ExpressCabinet";
    public static final String TYPE_EXPRESS_TICKET = "Express";
    public static final String TYPE_FLIGHT_TICKET = "PlaneTicket";
    public static final String TYPE_GROUP_BUYING_SUGGESTION = "GroupBuying";
    public static final String TYPE_GROUP_BUYING_TICKET = "GroupBuyingTicket";
    public static final String TYPE_HOTEL_TICKET = "Hotel";
    public static final String TYPE_MOVIE_TICKET = "Movie";
    public static final String TYPE_MY_DEVICES = "MyDevices";
    public static final String TYPE_PUBLIC = "Public";
    public static final String TYPE_THIRD_CALL_TAXI = "ThirdCallTaxi";
    public static final String TYPE_TRAIN_TICKET = "Train";
}
```

To be clear, this app is composed of 3 background services and 2 services. There is NO UI in this app.

Please be nice "DO NOT KILL ME >_<"

```java
public void onDestroy() {
    if (com.huawei.decision.c.a) {
        f.a( str: "RuleExecutorService",  str2: "onDestroy()");
    }
    a = null;
    super.onDestroy();
    if (!this.e) {
        f.c( str: "RuleExecutorService",  str2: "DO NOT KILL ME >_<");
        Intent intent = new Intent();
        intent.setClass( packageContext: this, RuleExecutorService.class);
        startService(intent);
    }
}
```

This is the kind of function that I love to find

```
public static boolean a() {
    String a = a( str: "persist.sys.huawei.debug.on",  str2: "0");
    Log.i( tag: "SystemPropertiesUtil",  msg: "debugOnFlag is:" + a);
    if ("1".equals(a)) {
        return true;
    }
    return false;
}
```

This app doesn't seems to send the data BUT they communicate with another service called HiActionService which is coming from an Huawei app called HiAction

```
public static void a(Context context) {
    if (context == null || b != null) {
        f.b(a,  str2: "service already binded");
        return;
    }
    f.b(a,  str2: "start bind service.");
    Intent intent = new Intent( action: "com.huawei.hiaction.inner");
    intent.setPackage("com.huawei.hiaction");
    try {
        f.a(a,  str2: "bind service ret : " + context.bindService(intent, c,  flags: 1));
    } catch (Throwable e) {
        f.b(a, e.getMessage(), e);
    }
}
```

The previous screenshot is from the class called ActionCommonUtil. We can easily that Decision is sending all his events to this service through the methods in this class.

*say