Evaluation Warning: The document was created with Spire.Doc for Python.

**铁塔换电（ 4.3.11版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 铁塔换电 |
| 版本 | 4.3.11 |
| 包名 | com.chinatower.tthd |
| 域名线索 | 125条 |
| URL线索 | 107条 |
| APP图标 |  |
| 分析日期 | 2025年9月23日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | \_V-40311\_C-4.3.11\_2021-11-11 10：14\_.apk |
| 文件大小 | 55.16MB |
| MD5值 | 99b22f234e0c4a2533346cfefa1e541a |
| SHA1值 | 011c47f49013ed5851888016ca29a71dcb39b887 |
| SHA256值 | 001c37cc75ed6433fe4f4767472e70d6a0bbcf2918a449e1d38619a60d60b8cf |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 铁塔换电 |
| 包名 | com.chinatower.tthd |
| 主活动Activity | com.chinatower.fghd.customer.MainActivity |
| 安卓版本名称 | 4.3.11 |
| 安卓版本 | 40311 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| dldir1.qq.com | IP: 61.49.23.135  所属国家: China  地区: Beijing  城市: Beijing |
| open.weixin.qq.com | IP: 109.244.144.48  所属国家: China  地区: Beijing  城市: Beijing |
| im5.7x24cc.com | IP: 123.57.186.112  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wappaygw.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| wapmap.baidu.com | IP: 111.206.209.212  所属国家: China  地区: Beijing  城市: Beijing |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.smpte-ra.org | IP: 52.20.185.129  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| daohang.map.baidu.com | IP: 111.206.209.190  所属国家: China  地区: Beijing  城市: Beijing |
| long.open.weixin.qq.com | IP: 109.244.217.35  所属国家: China  地区: Beijing  城市: Beijing |
| debugx5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| log.tbs.qq.com | IP: 109.244.244.32  所属国家: China  地区: Beijing  城市: Beijing |
| vectormap0.bdimg.com | IP: 39.91.128.35  所属国家: China  地区: Shandong  城市: Jinan |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| appcashier.test.95516.com | IP: 42.81.147.159  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.map.baidu.com | IP: 111.206.209.166  所属国家: China  地区: Beijing  城市: Beijing |
| itsdata.map.baidu.com | IP: 111.206.209.180  所属国家: China  地区: Beijing  城市: Beijing |
| test.opensso.tencent-cloud.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| metrics1.data.hicloud.com | IP: 114.115.188.66  所属国家: China  地区: Beijing  城市: Beijing |
| metrics2.data.hicloud.com | IP: 80.158.2.190  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| resolver.msg.xiaomi.net | IP: 120.92.96.13  所属国家: China  地区: Beijing  城市: Beijing |
| resolver.msg.global.xiaomi.net | IP: 8.219.211.108  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 117.78.10.90 | IP: 117.78.10.90  所属国家: China  地区: Guangdong  城市: Guangzhou |
| cloud.tim.qq.com | IP: 120.53.77.94  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| mapoffdownload.bdstatic.com | IP: 218.68.136.36  所属国家: China  地区: Tianjin  城市: Tianjin |
| newvector.map.baidu.com | IP: 111.206.209.171  所属国家: China  地区: Beijing  城市: Beijing |
| test.tim.qq.com | IP: 106.55.123.101  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| mobile.unionpay.com | 没有服务器地理信息. |
| idmb.register.xmpush.global.xiaomi.com | IP: 52.66.182.128  所属国家: India  地区: Maharashtra  城市: Mumbai |
| bbs.lbsyun.baidu.com | 没有服务器地理信息. |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| offmap2.baidu.com | IP: 101.72.203.35  所属国家: China  地区: Hebei  城市: Tangshan |
| h5.m.taobao.com | IP: 111.225.210.166  所属国家: China  地区: Hebei  城市: Langfang |
| restapi.amap.com | IP: 203.119.175.194  所属国家: China  地区: Beijing  城市: Beijing |
| configapi-api.glqa.jpushoa.com | IP: 172.17.5.42  所属国家: -  地区: -  城市: - |
| play.google.com | IP: 59.24.3.174  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| app.navi.baidu.com | IP: 111.206.209.213  所属国家: China  地区: Beijing  城市: Beijing |
| tcdns.myqcloud.com | IP: 119.45.78.99  所属国家: China  地区: Beijing  城市: Beijing |
| docs.jpush.io | 没有服务器地理信息. |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pms.mb.qq.com | IP: 175.27.12.246  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.asia | 没有服务器地理信息. |
| ce3e75d5.jpush.cn | IP: 183.232.58.252  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mlvbdc.live.qcloud.com | IP: 183.47.103.246  所属国家: China  地区: Guangdong  城市: Huizhou |
| a1.7x24cc.com | IP: 39.106.255.228  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| v.map.baidu.com | IP: 111.206.209.185  所属国家: China  地区: Beijing  城市: Beijing |
| itsmap3.baidu.com | IP: 153.37.235.49  所属国家: China  地区: Jiangsu  城市: Suzhou |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.135.32  所属国家: United States of America  地区: California  城市: San Francisco |
| 49.4.79.188 | IP: 49.4.79.188  所属国家: China  地区: Beijing  城市: Beijing |
| a5.7x24cc.com | IP: 39.105.60.156  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| reactjs.org | IP: 76.76.21.21  所属国家: United States of America  地区: California  城市: Walnut |
| appgallery.cloud.huawei.com | IP: 121.36.118.136  所属国家: China  地区: Guangdong  城市: Guangzhou |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5  所属国家: Singapore  地区: Singapore  城市: Singapore |
| issues.apache.org | IP: 168.119.33.54  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| 180.153.49.103 | IP: 180.153.49.103  所属国家: China  地区: Shanghai  城市: Shanghai |
| loc.map.baidu.com | IP: 111.206.209.175  所属国家: China  地区: Beijing  城市: Beijing |
| yun.tim.qq.com | IP: 109.244.172.104  所属国家: China  地区: Beijing  城市: Beijing |
| cn.register.xmpush.xiaomi.com | IP: 220.181.106.176  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.com | IP: 49.4.41.160  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| fr.register.xmpush.global.xiaomi.com | IP: 52.58.96.106  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| fx-beta.chinatowercom.cn | 没有服务器地理信息. |
| cloud-test.tim.qq.com | IP: 175.27.38.77  所属国家: China  地区: Beijing  城市: Beijing |
| map.baidu.com | IP: 111.206.208.32  所属国家: China  地区: Beijing  城市: Beijing |
| www.openssl.org | IP: 104.71.138.221  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.jivesoftware.com | IP: 141.193.213.10  所属国家: United States of America  地区: Texas  城市: Austin |
| ceshi02.7x24cc.com | IP: 101.201.239.37  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| android.bugly.qq.com | IP: 109.244.244.35  所属国家: China  地区: Beijing  城市: Beijing |
| ns.adobe.com | 没有服务器地理信息. |
| tcdnsipv6.myqcloud.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| d.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| newclient.map.baidu.com | IP: 111.206.209.170  所属国家: China  地区: Beijing  城市: Beijing |
| 120.52.40.38 | IP: 120.52.40.38  所属国家: China  地区: Hebei  城市: Langfang |
| official.opensso.tencent-cloud.com | IP: 118.126.71.18  所属国家: China  地区: Beijing  城市: Beijing |
| client.map.baidu.com | IP: 111.206.209.120  所属国家: China  地区: Beijing  城市: Beijing |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| jsperf.com | IP: 104.16.184.24  所属国家: United States of America  地区: California  城市: San Francisco |
| store.hispace.hicloud.com | IP: 121.36.119.209  所属国家: China  地区: Guangdong  城市: Guangzhou |
| im.7x24cc.com | IP: 123.56.86.104  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| debugtbs.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| indoorsearch.map.baidu.com | IP: 111.206.209.201  所属国家: China  地区: Beijing  城市: Beijing |
| redux.js.org | IP: 18.139.194.139  所属国家: Singapore  地区: Singapore  城市: Singapore |
| brain.baidu.com | IP: 110.242.69.34  所属国家: China  地区: Hebei  城市: Baoding |
| obs-test1-zs.obs.cn-north-4.myhuaweicloud.com | IP: 49.4.112.90  所属国家: China  地区: Beijing  城市: Beijing |
| ceshi01.7x24cc.com | IP: 123.56.20.159  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobilegw.alipay.com | IP: 203.209.245.77  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 10.138.32.176 | IP: 10.138.32.176  所属国家: -  地区: -  城市: - |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| face.baidu.com | IP: 112.34.111.253  所属国家: China  地区: Beijing  城市: Beijing |
| speedtest.trtc.tencent-cloud.com | IP: 162.14.6.106  所属国家: China  地区: Beijing  城市: Beijing |
| avc.qcloud.com | IP: 157.148.32.34  所属国家: China  地区: Guangdong  城市: Guangzhou |
| mclient.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| cfg.imtt.qq.com | IP: 175.27.12.246  所属国家: China  地区: Beijing  城市: Beijing |
| mcgw.alipay.com | IP: 124.239.239.237  所属国家: China  地区: Hebei  城市: Langfang |
| fb.me | IP: 31.13.77.35  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| livepullipv6.myqcloud.com | IP: 119.147.190.45  所属国家: China  地区: Guangdong  城市: Guangzhou |
| applet-hd.chinatowercom.cn | IP: 123.60.14.81  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| render.alipay.com | IP: 36.102.211.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| loggw-exsdk.alipay.com | IP: 110.76.6.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| metrics-dra.dt.hicloud.com | IP: 94.74.84.62  所属国家: Singapore  地区: Singapore  城市: Singapore |
| android.googlesource.com | IP: 74.125.23.82  所属国家: United States of America  地区: California  城市: Mountain View |
| mdc.html5.qq.com | IP: 175.27.9.46  所属国家: China  地区: Beijing  城市: Beijing |
| a6.7x24cc.com | IP: 39.106.255.228  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| informal.opensso.tencent-cloud.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| grs.dbankcloud.cn | IP: 49.4.41.160  所属国家: China  地区: Beijing  城市: Beijing |
| livepull.myqcloud.com | IP: 183.47.114.223  所属国家: China  地区: Guangdong  城市: Huizhou |
| sv.map.baidu.com | IP: 111.206.209.186  所属国家: China  地区: Beijing  城市: Beijing |
| s.file.myqcloud.com | IP: 150.138.42.166  所属国家: China  地区: Shandong  城市: Jinan |
| ai.baidu.com | IP: 110.242.69.34  所属国家: China  地区: Hebei  城市: Baoding |
| ofloc.map.baidu.com | IP: 110.242.70.118  所属国家: China  地区: Hebei  城市: Baoding |
| momentjs.com | IP: 104.17.93.38  所属国家: United States of America  地区: California  城市: San Francisco |
| ant.design | IP: 104.21.81.48  所属国家: United States of America  地区: California  城市: San Francisco |
| daup.map.baidu.com | IP: 110.242.69.98  所属国家: China  地区: Hebei  城市: Baoding |
| fx.chinatowercom.cn | IP: 124.70.64.141  所属国家: China  地区: Guangdong  城市: Guangzhou |
| appcashier256.95516.com | IP: 222.79.76.149  所属国家: China  地区: Fujian  城市: Xiamen |
| j.map.baidu.com | IP: 111.206.209.187  所属国家: China  地区: Beijing  城市: Beijing |
| astat.bugly.qcloud.com | IP: 150.109.27.253  所属国家: Singapore  地区: Singapore  城市: Singapore |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Observable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Maybe.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Flowable.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| http://configapi-api.glqa.jpushoa.com/v1/status | cn/jiguang/bc/f.java |
| https://ce3e75d5.jpush.cn/wi/op8jdu | cn/jiguang/s/c.java |
| https://ce3e75d5.jpush.cn | cn/jiguang/b/b.java |
| https://ce3e75d5.jpush.cn/wi/cjc4sa | cn/jiguang/ay/c.java |
| https://ce3e75d5.jpush.cn/wi/d8n3hj | cn/jiguang/ay/c.java |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n | com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java |
| https://api.map.baidu.com/lbs\_sdkcc/report | com/baidu/mapsdkplatform/comapi/b/a/c.java |
| https://ai.baidu.com/activation/key/activate | com/baidu/vis/unified/license/BDLicenseActivator.java |
| https://ai.baidu.com/activation/key/activate | com/baidu/idl/main/facesdk/FaceAuth.java |
| http://brain.baidu.com/record/api | com/baidu/idl/main/facesdk/statistic/PostDeviceInfo.java |
| https://brain.baidu.com/record/api | com/baidu/idl/face/platform/stat/Ast.java |
| http://10.138.32.176:8518/api/v3/person/verify\_sec?appid=7758258 | com/baidu/idl/face/platform/ui/utils/SecRequest.java |
| http://face.baidu.com/openapi/v2/stat/sdkdata | com/baidu/idl/face/platform/network/LogRequest.java |
| http://face.baidu.com/gate/api/userverifydemo | com/baidu/idl/face/platform/network/NoMotionRequest.java |
| http://map.baidu.com/zt/client/index/?fr=sdk\_[ | com/baidu/mapapi/utils/OpenClientUtil.java |
| http://api.map.baidu.com/direction? | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java |
| http://api.map.baidu.com/place/detail? | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java |
| http://api.map.baidu.com/place/search? | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java |
| http://app.navi.baidu.com/mobile/ | com/baidu/mapapi/navi/BaiduMapNavigation.java |
| http://daohang.map.baidu.com/mobile/ | com/baidu/mapapi/navi/BaiduMapNavigation.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1 | com/baidu/mapapi/cloud/CloudRgcInfo.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1 | com/baidu/mapapi/cloud/CloudRgcInfo.java |
| https://api.map.baidu.com/geosearch/v2/bound | com/baidu/mapapi/cloud/BoundSearchInfo.java |
| http://api.map.baidu.com/geosearch/v2/bound | com/baidu/mapapi/cloud/BoundSearchInfo.java |
| https://api.map.baidu.com/geosearch/v2/local | com/baidu/mapapi/cloud/LocalSearchInfo.java |
| http://api.map.baidu.com/geosearch/v2/local | com/baidu/mapapi/cloud/LocalSearchInfo.java |
| https://api.map.baidu.com/geosearch/v2/detail/ | com/baidu/mapapi/cloud/DetailSearchInfo.java |
| http://api.map.baidu.com/geosearch/v2/detail/ | com/baidu/mapapi/cloud/DetailSearchInfo.java |
| https://api.map.baidu.com/geosearch/v2/nearby | com/baidu/mapapi/cloud/NearbySearchInfo.java |
| http://api.map.baidu.com/geosearch/v2/nearby | com/baidu/mapapi/cloud/NearbySearchInfo.java |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/ | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2 | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/ | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/ | com/baidu/platform/domain/a.java |
| http://j.map.baidu.com/ | com/baidu/platform/domain/a.java |
| http://client.map.baidu.com/imap/share/ps | com/baidu/platform/domain/a.java |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s | com/baidu/platform/domain/a.java |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/ | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2 | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/ | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/ | com/baidu/platform/domain/b.java |
| https://j.map.baidu.com/ | com/baidu/platform/domain/b.java |
| https://client.map.baidu.com/imap/share/ps | com/baidu/platform/domain/b.java |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s | com/baidu/platform/domain/b.java |
| http://map.baidu.com/?newmap=1&s= | com/baidu/platform/core/e/e.java |
| http://wapmap.baidu.com/s?tn=Detail&pid= | com/baidu/platform/core/e/c.java |
| http://loc.map.baidu.com/sdk.php | com/baidu/location/h/l.java |
| http://loc.map.baidu.com/user\_err.php | com/baidu/location/h/l.java |
| http://loc.map.baidu.com/oqur.php | com/baidu/location/h/l.java |
| https://loc.map.baidu.com/tcu.php | com/baidu/location/h/l.java |
| http://loc.map.baidu.com/rtbu.php | com/baidu/location/h/l.java |
| http://loc.map.baidu.com/iofd.php | com/baidu/location/h/l.java |
| http://loc.map.baidu.com/wloc | com/baidu/location/h/l.java |
| https://loc.map.baidu.com/sdk\_ep.php | com/baidu/location/h/l.java |
| https://loc.map.baidu.com/sdk.php | com/baidu/location/h/l.java |
| https://daup.map.baidu.com/cltr/rcvr | com/baidu/location/h/l.java |
| https://loc.map.baidu.com/cfgs/loc/commcfgs | com/baidu/location/c/e.java |
| https://loc.map.baidu.com/gpsz | com/baidu/location/c/a.java |
| http://ofloc.map.baidu.com/offline\_loc | com/baidu/location/e/h.java |
| https://ofloc.map.baidu.com/offline\_loc | com/baidu/location/e/g.java |
| https://ofloc.map.baidu.com/offline\_loc | com/baidu/location/e/k.java |
| http://%s/%s | com/baidu/location/e/c.java |
| https://ofloc.map.baidu.com/offline\_loc | com/baidu/location/e/c.java |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php | com/baidu/location/b/i.java |
| https://loc.map.baidu.com/cc.php | com/baidu/location/b/g.java |
| https://loc.map.baidu.com/cfgs/loc/commcfgs | com/baidu/location/b/a.java |
| https://ofloc.map.baidu.com/locnu | com/baidu/location/b/aa.java |
| https://api.map.baidu.com/sdkcs/verify | com/baidu/lbsapi/auth/LBSAuthManager.java |
| http://schemas.android.com/apk/res/android | com/baidu/liantian/g/d.java |
| http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt | com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java |
| http://www.w3.org/ns/ttml | com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java |
| http://www.w3.org/1999/XSL/Transform\ | com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java |
| http://xml.apache.org/xslt | com/googlecode/mp4parser/authoring/tracks/ttml/TtmlHelpers.java |
| https://github.com/Polidea/RxAndroidBle/tree/master/mockrxandroidble' | com/polidea/rxandroidble2/RxBleClientImpl.java |
| https://android.googlesource.com/platform/external/bluetooth/bluedroid/+/android-5.1.0\_r1/stack/include/gatt\_api.h | com/polidea/rxandroidble2/exceptions/BleGattException.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/gj.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties\ | com/xiaomi/push/gc.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/ff.java |
| https://%1$s/gslb/?ver=4.0 | com/xiaomi/push/cs.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/gk.java |
| http://xmlpull.org/v1/doc/features.html | com/xiaomi/push/fr.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/m.java |
| https://register.xmpush.global.xiaomi.com | com/xiaomi/push/service/m.java |
| https://fr.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/m.java |
| https://ru.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/m.java |
| https://idmb.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/m.java |
| https://resolver.msg.global.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bj.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bj.java |
| https://a6.7x24cc.com/commonInte | com/hollycrm/trtcsdk/net/HttpUtils.java |
| http://a5.7x24cc.com/commonInte | com/hollycrm/hollycrmsdk/utils/CommonUtils.java |
| https://ceshi02.7x24cc.com/clientPhone?account= | com/hollycrm/hollycrmsdk/utils/CommonUtils.java |
| https://a6.7x24cc.com/clientPhone?account= | com/hollycrm/hollycrmsdk/utils/CommonUtils.java |
| http://a5.7x24cc.com/commonInte | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| http://a1.7x24cc.com/commonInte | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| http://ceshi01.7x24cc.com/open\_platform/uploadVoiceFile | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| http://im.7x24cc.com/open\_platform/uploadVoiceFile | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| https://a1.7x24cc.com | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| https://a6.7x24cc.com | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| https://ceshi02.7x24cc.com | com/hollycrm/hollycrmsdk/net/HollyUrl.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/cons/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/data/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://restapi.amap.com | com/chinatower/fghd/customer/location/NaviPopWindow.java |
| https://d.alipay.com | com/chinatower/fghd/customer/web/WebViewActivity.java |
| https://applet-hd.chinatowercom.cn/applet-exc/assist/queryEmergencyStatus | com/chinatower/fghd/customer/Constant/Constant.java |
| http://180.153.49.103:28080/onese/ | com/chinatower/fghd/customer/Constant/Constant.java |
| http://im5.7x24cc.com/phone\_webChat.html?accountId=N000000022137&chatId=c7961533-d60f-422e-a550-71d4e216e3e6&phone= | com/chinatower/fghd/customer/Constant/Constant.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/a.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/m.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/m.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/m.java |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/d.java |
| http://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/j.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| http://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047 | com/tencent/smtt/sdk/ui/dialog/d.java |
| http://%s/timeshift/%s/%s/timeshift.m3u8?delay=%d | com/tencent/liteav/j.java |
| http://%s/%s/%s/timeshift.m3u8?starttime=%s&appid=%s&txKbps=0 | com/tencent/liteav/j.java |
| http://%s/timeshift/%s/%s/timeshift.m3u8?delay=0 | com/tencent/liteav/j.java |
| http://%s/%s/%s/timeshift.m3u8?delay=0&appid=%s&txKbps=0 | com/tencent/liteav/j.java |
| http://dldir1.qq.com/hudongzhibo/liteavsvrcfg/serverconfig\_en.zip | com/tencent/liteav/basic/d/c.java |
| https://livepull.myqcloud.com/getpulladdr | com/tencent/liteav/network/g.java |
| https://livepullipv6.myqcloud.com/getpulladdr | com/tencent/liteav/network/g.java |
| https://tcdns.myqcloud.com/queryip | com/tencent/liteav/network/c.java |
| https://tcdnsipv6.myqcloud.com/queryip | com/tencent/liteav/network/c.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/b.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\ | com/unionpay/UPPayAssistEx.java |
| https://play.google.com/store | Mogua Engine V1 |
| https://appgallery.cloud.huawei.com/app/ | Mogua Engine V1 |
| https://play.google.com/store/apps/details?id= | Mogua Engine V1 |
| https://appgallery.cloud.huawei.com | Mogua Engine V1 |
| https://store.hispace.hicloud.com/hwmarket/api/ | Mogua Engine V1 |
| https://grs.dbankcloud.com | Mogua Engine V2 |
| https://grs.dbankcloud.cn | Mogua Engine V2 |
| https://grs.dbankcloud.eu | Mogua Engine V2 |
| https://grs.dbankcloud.asia | Mogua Engine V2 |
| https://metrics1.data.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics-dra.dt.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics2.data.hicloud.com:6447 | Mogua Engine V2 |
| https://metrics5.data.hicloud.com:6447 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.w3.org/html/wg/drafts/html/master/browsers.html | Mogua Engine V2 |
| http://jsperf.com/b64tests | Mogua Engine V2 |
| http://server/myapp/index.html | Mogua Engine V2 |
| https://issues.apache.org/jira/browse/CB-11522 | Mogua Engine V2 |
| http://117.78.10.90:8091'; | Mogua Engine V2 |
| http://fx.chinatowercom.cn:8091'; | Mogua Engine V2 |
| http://fx-beta.chinatowercom.cn:8091'; | Mogua Engine V2 |
| http://49.4.79.188:18091'; | Mogua Engine V2 |
| https://fb.me/react-polyfills | Mogua Engine V2 |
| http://fb.me/use-check-prop-types | Mogua Engine V2 |
| http://www.w3.org/2000/svg | Mogua Engine V2 |
| http://www.w3.org/1999/xlink | Mogua Engine V2 |
| https://redux.js.org/api-reference/store | Mogua Engine V2 |
| http://a | Mogua Engine V2 |
| http://a/c%20d?a=1&c=3 | Mogua Engine V2 |
| https://a@b | Mogua Engine V2 |
| http://\u0442\u0435\u0441\u0442 | Mogua Engine V2 |
| http://x | Mogua Engine V2 |
| http://api.map.baidu.com/geoconv/v1/?coords= | Mogua Engine V2 |
| http://im5.7x24cc.com/phone\_webChat.html?accountId=N000000022137&chatId=8bd6ba4a-1b03-4813-bae4-e269b7192c57&phone= | Mogua Engine V2 |
| https://github.com/crypto-browserify/crypto-browserify | Mogua Engine V2 |
| https://github.com/indutny/elliptic/issues | Mogua Engine V2 |
| https://github.com/indutny/elliptic | Mogua Engine V2 |
| http://api.map.baidu.com/geoconv/v1/?from=1&to=5&ak=C88UR4sSYNZD2IBbrchiVlnu1nxEXA5e | Mogua Engine V2 |
| https://ant.design/components/form/ | Mogua Engine V2 |
| https://ant.design/components/input/ | Mogua Engine V2 |
| https://ant.design/components/icon | Mogua Engine V2 |
| http://120.52.40.38:1032/file/video/f1f09ffc6efd4f10acb88dba58fd3fae.mp4 | Mogua Engine V2 |
| https://reactjs.org/docs/error-decoder.html?invariant= | Mogua Engine V2 |
| http://momentjs.com/guides/ | Mogua Engine V2 |
| https://obs-test1-zs.obs.cn-north-4.myhuaweicloud.com/haha/00/CigBz17GOtCAMniKAAA5Pejp\_0k057.jpg | Mogua Engine V2 |
| http://www.w3.org/XML/1998/namespace | Mogua Engine V2 |
| http://www.w3.org/1999/xhtml | Mogua Engine V2 |
| http://www.w3.org/1998/Math/MathML | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://server/myapp/index.html | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://docs.jpush.io/client/android\_api/ | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://www.apache.org/licenses/LICENSE-2.0 | Mogua Engine V2 |
| http://client.map.baidu.com/imap/sdk/tj?qt=vmap | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/statistics/v1/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newclient.map.baidu.com/client/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://client.map.baidu.com/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://v.map.baidu.com/low/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://v.map.baidu.com/indoorinside/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://v.map.baidu.com/high/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newclient.map.baidu.com/pic/newvector/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newvector.map.baidu.com/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://vectormap0.bdimg.com/vecdata/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newclient.map.baidu.com/its/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://itsmap3.baidu.com/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newclient.map.baidu.com/pic/starpic/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| http://api.map.baidu.com/sdkws/heatmap? | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://sv.map.baidu.com | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://sv.map.baidu.com/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://client.map.baidu.com/offline-search/? | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://offmap2.baidu.com/offline-search/? | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://mapoffdownload.bdstatic.com/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newvector.map.baidu.com/grid\_vc/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newvector.map.baidu.com/travel\_vc/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://newvector.map.baidu.com/inst\_grid/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| https://indoorsearch.map.baidu.com/is/ | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url= | lib/armeabi/libBaiduMapSDK\_map\_v6\_4\_0.so |
| http://www.openssl.org/support/faq.html | lib/armeabi/libuptsmaddonmi.so |
| http://ns.adobe.com/xap/1.0/ | lib/armeabi/libimagepipeline.so |
| http://www.openssl.org/support/faq.html | lib/armeabi/libtxffmpeg.so |
| https://appcashier.test.95516.com/gateway/mobile/json | lib/armeabi/libentryexpro.so |
| https://appcashier256.95516.com/gateway/mobile/json | lib/armeabi/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/json | lib/armeabi/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/json | lib/armeabi/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/hft | lib/armeabi/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/hft | lib/armeabi/libentryexpro.so |
| https://appcashier.test.95516.com/app/mobile/conf | lib/armeabi/libentryexpro.so |
| https://appcashier256.95516.com/app/mobile/conf | lib/armeabi/libentryexpro.so |
| http://mlvbdc.live.qcloud.com/ | lib/armeabi/libliteavsdk.so |
| https://test.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo?sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json | lib/armeabi/libliteavsdk.so |
| https://informal.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo?sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json | lib/armeabi/libliteavsdk.so |
| https://official.opensso.tencent-cloud.com/v4/openim/jsonvideoinfo?sdkappid=%d&identifier=%s&usersig=%s&random=99999999&contenttype=json | lib/armeabi/libliteavsdk.so |
| http://obfjaaaafhiehjjf/ohae.oiaa | lib/armeabi/libliteavsdk.so |
| https://avc.qcloud.com/log/appsign.php | lib/armeabi/libliteavsdk.so |
| https://avc.qcloud.com/log/report.php | lib/armeabi/libliteavsdk.so |
| https://yun.tim.qq.com | lib/armeabi/libliteavsdk.so |
| https://test.tim.qq.com | lib/armeabi/libliteavsdk.so |
| https://cloud.tim.qq.com/v3/liveinterface/ | lib/armeabi/libliteavsdk.so |
| https://cloud-test.tim.qq.com/v3/liveinterface/ | lib/armeabi/libliteavsdk.so |
| https://speedtest.trtc.tencent-cloud.com | lib/armeabi/libliteavsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| mywallet-gray@3x.a4e7871b  mywallet-orange@3x.11b4781c  git@github.com  fedor@indutny.com  mywallet-red@3x.4f7e7ed6 | Mogua Engine V2 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118 | com/baidu/mapsdkplatform/comapi/util/b.java |
| 13000000000 | com/baidu/idl/face/platform/ui/utils/SecRequest.java |
| 15060355040 | com/unionpay/UPPayAssistEx.java |
| 14782472537 | Mogua Engine V1 |
| 19919152923 | Mogua Engine V2 |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CHN, ST=北京, L=北京, O=铁塔能源有限公司, OU=铁塔能源有限公司, CN=张环宇 签名算法: rsassa\_pkcs1v15 有效期自: 2020-05-25 10:05:01+00:00 有效期至: 2045-05-19 10:05:01+00:00 发行人: C=CHN, ST=北京, L=北京, O=铁塔能源有限公司, OU=铁塔能源有限公司, CN=张环宇 序列号: 0xd0dcf86 哈希算法: sha256 md5值: 8fb360938e59f36ca5da2d2f78ea0f29 sha1值: ab86ae5b1b466c41da2528d8f27b18a96bac0ca1 sha256值: 477e5319b5e3a3b9924bec016d4d6b9f4468c823b28bfcc220b24c72283ed8c8 sha512值: 9c91ff891bcbccaae270a8776010d03af0b77c43a4d7143918aceaf2792372fbf1bd5a7c7d190b0b0c32dcd609aa0b406ac04394ecac6414e72574dce67a90bd 公钥算法: rsa 密钥长度: 2048 指纹: 5bd463d7ea89f655b9d702bb91e7c4a4c19e74c0830477b87bbe655100e6d302**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "alart\_un\_auth" : "您尚未实名认证,是否实名认证?" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.chinatower.tthd.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| org.simalliance.openmobileapi.SMARTCARD | 未知 | Unknown permission | Unknown permission from android reference |
| com.chinatower.tthd.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| com.chinatower.tthd.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.chinatower.tthd.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**