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

**My BMW（ 5.5.0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 | My BMW |
| 版本 | 5.5.0 |
| 包名 | de.bmw.connected.mobile20.cn |
| 域名线索 | 130条 |
| URL线索 | 127条 |
| APP图标 |  |
| 分析日期 | 2025年6月18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 | 20250523110944874692789349.apk |
| 文件大小 | 443.07MB |
| MD5值 | 814309ff6a5a5bf25dea7ec1975197d5 |
| SHA1值 | 6baf869608d49d8c5fb8eafaedd30ee12fac0984 |
| SHA256值 | 3b27bc296b3fecbac24152a0b5d4fff01bed52a60238e26e97c0a4d2571cc15b |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | My BMW |
| 包名 | de.bmw.connected.mobile20.cn |
| 主活动Activity | com.mobileconnected.MainActivity |
| 安卓版本名称 | 5.5.0 |
| 安卓版本 | 43024 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ichannel.snssdk.com | IP: 111.202.5.195 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| logback.qos.ch | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息.  |
| sdk.faceid.qq.com | IP: 221.198.69.152 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.google.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.ximalaya.com | IP: 101.91.133.50 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| applog.snssdk.com | IP: 106.74.132.32 所属国家: China 地区: Shandong 城市: Jinan  |
| othstr.beacon.qq.com | IP: 140.206.162.29 所属国家: China 地区: Shanghai 城市: Shanghai  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| zxid-m.mobileservice.cn | IP: 101.69.207.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| gtc.getui.nethttps | 没有服务器地理信息.  |
| rttgpsreport.map.qq.com | IP: 60.28.215.71 所属国家: China 地区: Tianjin 城市: Tianjin  |
| journeyapps.com | IP: 18.65.168.85 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| image.cnamedomain.com | 没有服务器地理信息.  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| testlogin.kuwo.cn | IP: 111.206.98.20 所属国家: China 地区: Beijing 城市: Beijing  |
| kyccdn.tencentcloudapi.com | IP: 119.188.44.168 所属国家: China 地区: Shandong 城市: Jinan  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.countly-preprod.bmwusa.com | IP: 172.212.144.58 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| loggw-exsdk.alipay.com | IP: 110.76.6.82 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| corssdk.map.qq.com | IP: 116.130.220.64 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.android.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| realm.io | IP: 3.173.219.44 所属国家: United States of America 地区: Washington 城市: Seattle  |
| mclient.alipay.com | IP: 218.61.164.134 所属国家: China 地区: Liaoning 城市: Shenyang  |
| toblog-alink.ctobsnssdk.com | IP: 42.56.93.211 所属国家: China 地区: Liaoning 城市: Shenyang  |
| mt.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| b-gtc.getui.nethttps | 没有服务器地理信息.  |
| idasc-kyc-test.tencentcloudapi.com | IP: 123.207.114.133 所属国家: China 地区: Beijing 城市: Beijing  |
| 111.230.161.197 | IP: 111.230.161.197 所属国家: China 地区: Beijing 城市: Beijing  |
| www.opengis.net | IP: 217.154.231.107 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Brighton  |
| api.countly-preprod.bmwgroup.com | IP: 4.184.156.158 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| docs.mongodb.com | IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.example.com | IP: 92.122.244.33 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| ocr.tencentcloudapi.com | IP: 120.53.72.73 所属国家: China 地区: Beijing 城市: Beijing  |
| mp.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| cs.map.qq.com | IP: 125.36.181.143 所属国家: China 地区: Tianjin 城市: Tianjin  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| api.test.ximalaya.com | IP: 10.146.3.40 所属国家: - 地区: - 城市: -  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| sdk-open-phone.getui.com | IP: 124.160.155.42 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| zxid.mobileservice.cn | IP: 101.69.207.69 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.236 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pub.dev | IP: 34.36.0.14 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| databyterangers.com.cn | 没有服务器地理信息.  |
| miniprogram-kyc.tencentcloudapi.com | IP: 193.112.232.253 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| tdid.m.qq.com | IP: 60.29.240.40 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| int-b2vapi.bmwgroup.com | IP: 160.46.225.136 所属国家: Germany 地区: Bayern 城市: Munich  |
| open.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| testdatalbs.sparta.html5.qq.com | IP: 157.255.4.30 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| h5app.kuwo.cn | IP: 116.196.151.15 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| lstest.map.qq.com | IP: 220.194.120.95 所属国家: China 地区: Tianjin 城市: Tianjin  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| api.countly.bmw.com.cn | IP: 143.64.73.11 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| en.wikipedia.org | IP: 31.13.94.37 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| kycwa.tencentcloudapi.com | IP: 42.193.129.244 所属国家: China 地区: Beijing 城市: Beijing  |
| log.snssdk.com | IP: 42.56.93.209 所属国家: China 地区: Liaoning 城市: Shenyang  |
| c-gtc.getui.nethttps | 没有服务器地理信息.  |
| test-wbd.kuwo.cn | IP: 111.206.98.20 所属国家: China 地区: Beijing 城市: Beijing  |
| m.test.ximalaya.com | IP: 10.146.3.14 所属国家: - 地区: - 城市: -  |
| digitalkeypairing.org | IP: 34.210.173.62 所属国家: United States of America 地区: Oregon 城市: Portland  |
| music.163.com | IP: 220.197.30.65 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.tencentcloud.com | IP: 43.175.52.13 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| mobilegw.alipay.com | IP: 203.209.243.27 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| issuetracker.google.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| i.y.qq.com | IP: 140.206.162.227 所属国家: China 地区: Shanghai 城市: Shanghai  |
| rtapplog.snssdk.com | IP: 123.6.21.191 所属国家: China 地区: Henan 城市: Zhengzhou  |
| manual.sensorsdata.cn | IP: 61.182.131.226 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.118.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.ximalaya.com | IP: 101.91.133.109 所属国家: China 地区: Shanghai 城市: Shanghai  |
| h5app-test.kuwo.cn | IP: 119.188.149.190 所属国家: China 地区: Shandong 城市: Jinan  |
| rtlog.snssdk.com | IP: 106.74.132.32 所属国家: China 地区: Shandong 城市: Jinan  |
| www.hyphenation.org | IP: 46.4.94.215 所属国家: Germany 地区: Bayern 城市: Gunzenhausen  |
| analytics.map.qq.com | IP: 125.36.181.143 所属国家: China 地区: Tianjin 城市: Tianjin  |
| miniprogram-kyc-test.tencentcloudapi.com | IP: 123.207.114.133 所属国家: China 地区: Beijing 城市: Beijing  |
| eadrax-bmw-na-dly-65732.firebaseio.com55https | 没有服务器地理信息.  |
| b2vapi.bmwgroup.com | IP: 160.46.245.252 所属国家: Germany 地区: Bayern 城市: Munich  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| api.countly.bmwgroup.com | IP: 4.184.67.169 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| apmplus.volces.com | IP: 125.39.135.101 所属国家: China 地区: Tianjin 城市: Tianjin  |
| lbs-trpc.map.qq.com | IP: 116.130.224.82 所属国家: China 地区: Beijing 城市: Beijing  |
| confinfo.map.qq.com | IP: 116.130.223.83 所属国家: China 地区: Beijing 城市: Beijing  |
| h.trace.qq.com | IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi  |
| wbd.kuwo.cn | IP: 111.206.98.20 所属国家: China 地区: Beijing 城市: Beijing  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| mcgw.alipay.com | IP: 111.202.5.210 所属国家: China 地区: Beijing 城市: Beijing  |
| wappaygw.alipay.com | IP: 111.202.5.209 所属国家: China 地区: Beijing 城市: Beijing  |
| lbs6.map.qq.com | IP: 116.130.220.102 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| otheve.beacon.qq.com | IP: 113.56.189.125 所属国家: China 地区: Hubei 城市: Huangshi  |
| d-gt.getui.com | 没有服务器地理信息.  |
| oss.aliyuncs.com | IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| eadrax-bmw-na-dly-65732.firebaseio.com | IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| c-hzgt2.getui.com | IP: 124.160.155.59 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| api.countly.bmwusa.com | IP: 172.212.178.219 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| nisportal.10010.com | IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing  |
| api.countly-preprod.bmw.com.cn | IP: 143.64.49.130 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| idasc-kyc.tencentcloudapi.com | IP: 193.112.232.253 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| apm.volccdn.com | IP: 123.6.149.140 所属国家: China 地区: Henan 城市: Zhengzhou  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| attest.approoval.com | IP: 34.49.166.75 所属国家: United States of America 地区: California 城市: Mountain View  |
| h5.m.taobao.com | IP: 60.9.1.94 所属国家: China 地区: Hebei 城市: Hengshui  |
| nlp.map.qq.com | IP: 116.130.220.102 所属国家: China 地区: Beijing 城市: Beijing  |
| im-int-api.lingyue-digital.com | IP: 59.110.247.198 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| mon.snssdk.com | IP: 111.161.204.190 所属国家: China 地区: Tianjin 城市: Tianjin  |
| i.kuwo.cn | IP: 111.206.98.20 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.countly.bmwusa.com  | ab/b.java  |
| https://api.countly-preprod.bmwusa.com  | ab/b.java  |
| https://api.countly.bmwgroup.com  | ab/b.java  |
| https://api.countly-preprod.bmwgroup.com  | ab/b.java  |
| https://api.countly.bmw.com.cn  | ab/b.java  |
| https://api.countly-preprod.bmw.com.cn  | ab/b.java  |
| https://tdid.m.qq.com?mc=2  | bv/c1.java  |
| https://rttgpsreport.map.qq.com/report  | c/t/m/g/f3.java  |
| https://cs.map.qq.com/key  | c/t/m/g/f3.java  |
| https://analytics.map.qq.com/  | c/t/m/g/f3.java  |
| https://analytics.map.qq.com/tr  | c/t/m/g/f3.java  |
| https://nlp.map.qq.com/  | c/t/m/g/f3.java  |
| https://lbs6.map.qq.com/k  | c/t/m/g/f3.java  |
| https://lbs6.map.qq.com/loc  | c/t/m/g/f3.java  |
| https://lbs-trpc.map.qq.com/k  | c/t/m/g/f3.java  |
| https://mt.map.qq.com/key  | c/t/m/g/f3.java  |
| https://corssdk.map.qq.com/key  | c/t/m/g/f3.java  |
| https://lstest.map.qq.com/nlpdr?sf  | c/t/m/g/l.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?sf  | c/t/m/g/l.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?wf4  | c/t/m/g/j.java  |
| https://testdatalbs.sparta.html5.qq.com/tr?utr  | c/t/m/g/i.java  |
| https://apis.map.qq.com/ws/geocoder/v1/?location=  | c/t/m/g/g5.java  |
| https://testlogin.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://i.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://test-wbd.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://wbd.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://h5app-test.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://h5app.kuwo.cn  | cn/kuwo/auth/kwauthsdk/utils/e.java  |
| https://ip.  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://image.cnamedomain.com'!  | com/alibaba/sdk/android/oss/OSSImpl.java  |
| http://oss-cn-hangzhou.aliyuncs.com  | com/alibaba/sdk/android/oss/common/OSSConstants.java  |
| http://oss.aliyuncs.com  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| http://127.0.0.1  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| http://image.cnamedomain.com'!  | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.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://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://apmplus.volces.com/monitor/collect/c/cloudcontrol/file  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/native\_bin\_crash  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/settings/get  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/core\_dump\_collect  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/crash\_portrait  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/exception  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/logcollect  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/crash  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/exception/dump\_collection  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com/monitor/collect/c/rapheal\_file\_collect  | com/apm/insight/runtime/ConfigManager.java  |
| https://apmplus.volces.com  | com/apm/applog/UriConfig.java  |
| https://int-b2vapi.bmwgroup.com  | com/bmwgroup/connected/util/token/TokenConstants.java  |
| https://b2vapi.bmwgroup.com  | com/bmwgroup/connected/util/token/TokenConstants.java  |
| http://www.google.com/kml/ext/2.2  | com/bmwgroup/connected/util/kmz/KmzHelper.java  |
| http://www.opengis.net/kml/2.2  | com/bmwgroup/connected/util/kmz/KmzHelper.java  |
| http://xmlpull.org/v1/doc/features.html  | com/bmwgroup/connected/util/kmz/KmzHelper.java  |
| https://attest.approoval.com/token  | com/criticalblue/approovsdk/h.java  |
| https://miniprogram-kyc.tencentcloudapi.com/api/server/getAdvFaceId?orderNo=  | com/example/face\_live/FaceLivePlugin.java  |
| https://miniprogram-kyc.tencentcloudapi.com/api/oauth2/api\_ticket?app\_id=  | com/example/face\_live/FaceLivePlugin.java  |
| https://miniprogram-kyc.tencentcloudapi.com/api/oauth2/access\_token?app\_id=TIDA7OKt&secret=&grant\_type=client\_credential&version=1.0.0  | com/example/face\_live/SignUseCase.java  |
| https://miniprogram-kyc.tencentcloudapi.com  | com/example/face\_live/SignUseCase.java  |
| https://miniprogram-kyc.tencentcloudapi.com/api/oauth2/api\_ticket?app\_id=TIDA7OKt&access\_token=  | com/example/face\_live/SignUseCase.java  |
| https://c-gtc.getui.net,https://c-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://gtc.getui.net,https://gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://b-gtc.getui.net,https://b-gtc.gepush.com  | com/getui/gtc/c/b.java  |
| https://sdk-open-phone.getui.com/api.php  | com/igexin/push/a.java  |
| https://c-hzgt2.getui.com/api.php  | com/igexin/push/a.java  |
| https://d-gt.getui.com/api.htm  | com/igexin/push/a.java  |
| https://bi.  | com/igexin/push/config/b.java  |
| https://config.  | com/igexin/push/config/b.java  |
| https://bi.  | com/igexin/push/config/h.java  |
| https://config.  | com/igexin/push/config/h.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://en.wikipedia.org/wiki/Hostname  | com/sensorsdata/analytics/android/sdk/SensorsDataAPI.java  |
| https://manual.sensorsdata.cn/sa/latest/flutter-22257963.html\  | com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java  |
| https://manual.sensorsdata.cn/sa/latest/tech\_sdk\_client\_web\_use-7545346.html\  | com/sensorsdata/analytics/android/sdk/visual/utils/AlertMessageUtils.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/idasc/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/idasc/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/idasc/proguard/ac.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/idasc/crashreport/common/strategy/StrategyBean.java  |
| https://apis.map.qq.com/ws/  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/distance/v1/matrix  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/district/v1/getchildren  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/district/v1/list  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/district/v1/search  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/place/v1/explore  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/customapi/mobike/geocoder  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/geocoder/v1  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/streetview/v1/getpano  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/direction/v1/bicycling  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/direction/v1/driving  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/direction/v1/transit  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/direction/v1/trucking  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/direction/v1/walking  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/place/v1/detail  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/place/v1/search  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/place/v1/suggestion  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://apis.map.qq.com/ws/coord/v1/translate  | com/tencent/lbssearch/httpresponse/UrlConstant.java  |
| https://confinfo.map.qq.com/confinfo?  | com/tencent/mapsdk/internal/qz.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/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://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| https://ocr.tencentcloudapi.com  | com/tencent/ocr/sdk/entity/OcrSetting.java  |
| https://sdk.faceid.qq.com/api/v1/data/device-info  | com/tencent/ocr/sdk/common/g.java  |
| https://sdk.faceid.qq.com/api/common/error-report  | com/tencent/ocr/sdk/common/g.java  |
| https://111.230.161.197  | com/tencent/ocr/sdk/net/c.java  |
| https://www.tencentcloud.com/zh/document/product/1005/50444?!editLang=en  | com/tencent/ocr/sdk/component/d.java  |
| https://otheve.beacon.qq.com/analytics/v2\_upload  | com/tencent/tmsbeacon/base/net/b/b.java  |
| https://othstr.beacon.qq.com/analytics/v2\_upload  | com/tencent/tmsbeacon/base/net/b/b.java  |
| https://h.trace.qq.com/kv  | com/tencent/tmsbeacon/a/b/d.java  |
| https://im-int-api.lingyue-digital.com/api/tcbusApi/api/sdk/v1  | com/tinet/timclientlib/common/constans/TUrlConstants.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fh.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fw.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/ch.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fx.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ex.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/q.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/q.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/ax.java  |
| https://nisportal.10010.com:9001  | com/zx/a/I8b7/h1.java  |
| https://zxid-m.mobileservice.cn/sdk/config/v2/init  | com/zx/a/I8b7/p.java  |
| https://zxid-m.mobileservice.cn/sdk/config/init  | com/zx/a/I8b7/m.java  |
| https://zxid-m.mobileservice.cn/sdk/app/depAnalysis  | com/zx/a/I8b7/f1.java  |
| https://zxid-m.mobileservice.cn/sdk/module/getCoreModule  | com/zx/a/I8b7/h0.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken  | com/zx/a/I8b7/x1.java  |
| https://zxid.mobileservice.cn/privacy  | com/zx/a/I8b7/n3.java  |
| https://zxid-m.mobileservice.cn/sdk/config/token  | com/zx/a/I8b7/n.java  |
| https://zxid-m.mobileservice.cn/sdk/uaid/get  | com/zx/a/I8b7/y1.java  |
| https://zxid-m.mobileservice.cn/sdk/extend/tag  | com/zx/a/I8b7/e2.java  |
| https://zxid-m.mobileservice.cn/sdk/ext/pconfig  | com/zx/a/I8b7/g.java  |
| https://zxid-m.mobileservice.cn/sdk/channel/report  | com/zx/a/I8b7/r1.java  |
| https://api.ximalaya.com/oauth2/v2/authorize?  | com/ximalaya/ting/android/opensdk/auth/component/XmlyBrowserComponent.java  |
| https://api.test.ximalaya.com/oauth2/v2/authorize?  | com/ximalaya/ting/android/opensdk/auth/component/XmlyBrowserComponent.java  |
| http://www.slf4j.org/codes.html  | ca0/d.java  |
| http://www.slf4j.org/codes.html  | ca0/c.java  |
| http://logback.qos.ch/codes.html  | f6/g.java  |
| https://mobilegw.alipay.com/mgw.htm  | f8/a.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | h9/o.java  |
| https://docs.flutter.dev/deployment/android  | io/flutter/embedding/engine/loader/FlutterLoader.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://realm.io/docs/java/latest/  | io/realm/r0.java  |
| https://docs.mongodb.com/realm/sdk/android/install/  | io/realm/k0.java  |
| https://github.com/realm/realm-java/tree/master/examples/rxJavaExample  | io/realm/k0.java  |
| https://issuetracker.google.com/issues/36918154  | io/realm/d0.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/j.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/w.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/b.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/n.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/b.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/h.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/z.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/q.java  |
| https://developer.android.com/reference/com/google/android/play/core/review/model/ReviewErrorCode.html  | km/a.java  |
| https://invalidURLmyBMW  | jb/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | lz/d.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | lz/f.java  |
| http://xml.org/sax/features/validation  | o6/e.java  |
| http://xml.org/sax/features/namespaces  | o6/e.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | oy/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | oy/d.java  |
| https://invalidURLmyBMW  | pb/b.java  |
| http://logback.qos.ch/codes.html  | t6/f.java  |
| https://kyccdn.tencentcloudapi.com  | us/c.java  |
| https://log.snssdk.com/apm/device\_register  | v/s.java  |
| https://ichannel.snssdk.com/service/2/app\_alert\_check/  | v/s.java  |
| https://log.snssdk.com/monitor/collect/c/session  | v/s.java  |
| https://applog.snssdk.com/monitor/collect/c/session  | v/s.java  |
| https://rtlog.snssdk.com/monitor/collect/c/session  | v/s.java  |
| https://rtapplog.snssdk.com/monitor/collect/c/session  | v/s.java  |
| https://log.snssdk.com/service/2/log\_settings/  | v/s.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/attribution\_data  | v/s.java  |
| https://toblog-alink.ctobsnssdk.com/service/2/alink\_data  | v/s.java  |
| https://apmplus.volces.com/apm/device\_register  | v/s.java  |
| https://apmplus.volces.com/monitor/collect/c/session  | v/s.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | u8/l.java  |
| https://mobilegw.dl.alipaydev.com/mgw.htm  | u8/l.java  |
| https://digitalkeypairing.org/v1/%s?friendlyName=%s&technology=%s&graphics=%s&fromWallet=%s  | wq/e.java  |
| https://kycwa.tencentcloudapi.com/rcrm-codcs/mob-data-collect  | vt/b.java  |
| http://logback.qos.ch/codes.html  | x6/t.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | za0/m.java  |
| https://github.com/grpc/grpc-java/issues/11492  | ze/j.java  |
| https://kycwa.tencentcloudapi.com/rcrm-codcs/mob-data-collect  | ys/e.java  |
| https://idasc-kyc.tencentcloudapi.com  | ys/c.java  |
| https://idasc-kyc-test.tencentcloudapi.com  | ys/c.java  |
| https://miniprogram-kyc.tencentcloudapi.com  | ys/c.java  |
| https://miniprogram-kyc-test.tencentcloudapi.com  | ys/c.java  |
| http://logback.qos.ch/codes.html  | w6/h.java  |
| http://logback.qos.ch/codes.html  | w6/b.java  |
| http://logback.qos.ch/codes.html  | w6/g.java  |
| http://logback.qos.ch/codes.html  | fa0/a.java  |
| https://i.y.qq.com/n2/m/  | ja/l.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | ab0/n.java  |
| https://invalidURLmyBMW  | sc/a.java  |
| http://logback.qos.ch/codes.html  | n6/e.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | h8/a.java  |
| https://m.ximalaya.com/login?  | xw/c.java  |
| http://m.test.ximalaya.com/login?  | xw/c.java  |
| https://m.ximalaya.com/xiaoya/login?  | xw/c.java  |
| http://m.test.ximalaya.com/xiaoya/login?  | xw/c.java  |
| https://api.ximalaya.com/oauth2/v2/authorize?  | xw/c.java  |
| http://api.test.ximalaya.com/oauth2/v2/authorize?  | xw/c.java  |
| https://mon.snssdk.com/monitor/collect/c/cloudcontrol/file  | k5/a.java  |
| https://mcgw.alipay.com/sdklog.do  | o8/c.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | o8/d.java  |
| https://databyterangers.com.cn  | n/a.java  |
| https://invalidURLmyBMW  | kb/b.java  |
| https://music.163.com/st/platform/oauth/authorize?clientId=  | ia/b.java  |
| https://pub.dev/packages/in\_app\_review  | cx/d.java  |
| https://play.google.com/store/apps/details?id=  | cx/d.java  |
| https://eadrax-bmw-na-dly-65732.firebaseio.com  | 摸瓜V1引擎  |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://apm.volccdn.com/mars-web/apmplus/web/browser.cn.js?aid=0&globalName=  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://eadrax-bmw-na-dly-65732.firebaseio.com  | 摸瓜V3引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V3引擎  |
| http://www.hyphenation.org/tex  | 摸瓜V3引擎  |
| https://eadrax-bmw-na-dly-65732.firebaseio.com55https://github.com/journeyapps/zxing-android-embedde  | 摸瓜V3引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V3引擎  |
| https://journeyapps.com/  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V3引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| poi\_icon@2x.png poi\_icon\_indoor\_ex@2x.png icon\_indoor\_ex\_night@2x.png  | com/tencent/mapsdk/internal/em.java  |
| try\_loyalty\_purchase@3x.webp phone-rsu-darkmode@3x.webp phone-rsu-lightmode@3x.webp ent-modal-banner-bmw@3x.webp nt-modal-banner-mini@3x.webp interiorid7@2x.webp interiorid8c@2x.webp map\_icon\_driver@2x.png caextendedwarranty@2x.webp cawarranty@2x.webp  | 摸瓜V2引擎  |
| 18@2x.webp 1@2x.webp 2@2x.webp 3@2x.webp 4@2x.webp 5@2x.webp 6@2x.webp 7@2x.webp 8@2x.webp 9@2x.webp 10@2x.webp 11@2x.webp 12@2x.webp 13@2x.webp 14@2x.webp 15@2x.webp 16@2x.webp 17@2x.webp 19@2x.webp 20@2x.webp 21@2x.webp 22@2x.webp 23@2x.webp 24@2x.webp 25@2x.webp 26@2x.webp 27@2x.webp 28@2x.webp  | 摸瓜V2引擎  |
| cheng.cui@partner.bmw siman.chuan@partner.bmw  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13222222222  | bv/p2.java  |
| 14222222222  | bv/p2.java  |
| 17146314752  | j70/j.java  |
| 17512775099  | pm/a.java  |
| 13129340006  | v70/g.java  |
| 15311520693  | lib/arm64-v8a/libYTImageRefinerPub.so  |
| 15713703727  | lib/arm64-v8a/libYTImageRefinerPub.so  |
| 13755503429  | lib/arm64-v8a/libYTImageRefinerPub.so  |
| 18988633568  | lib/arm64-v8a/libYTImageRefinerPub.so  |
| 15735274653  | lib/arm64-v8a/libapp.so  |
| 14736395667  | lib/arm64-v8a/libapp.so  |
| 14603134346  | lib/arm64-v8a/libapp.so  |
| 17461238838  | lib/arm64-v8a/libapp.so  |
| 14083424482  | lib/arm64-v8a/libapp.so  |
| 14054271516  | lib/arm64-v8a/libapp.so  |
| 16360377347  | lib/arm64-v8a/libapp.so  |
| 15866282137  | lib/arm64-v8a/libapp.so  |
| 13272299608  | lib/arm64-v8a/libapp.so  |
| 14521158961  | lib/arm64-v8a/libapp.so  |
| 15220060793  | lib/arm64-v8a/libapp.so  |
| 16634220692  | lib/arm64-v8a/libapp.so  |
| 18303205052  | lib/arm64-v8a/libapp.so  |
| 18219420711  | lib/arm64-v8a/libapp.so  |
| 13866236427  | lib/arm64-v8a/libapp.so  |
| 14463071505  | lib/arm64-v8a/libapp.so  |
| 17050179402  | lib/arm64-v8a/libapp.so  |
| 17842439106  | lib/arm64-v8a/libapp.so  |
| 13526311248  | lib/arm64-v8a/libapp.so  |
| 13928158214  | lib/arm64-v8a/libapp.so  |
| 16773195083  | lib/arm64-v8a/libapp.so  |
| 17307014824  | lib/arm64-v8a/libapp.so  |
| 18291378369  | lib/arm64-v8a/libapp.so  |
| 15612168314  | lib/arm64-v8a/libapp.so  |
| 15402316060  | lib/arm64-v8a/libapp.so  |
| 14948291004  | lib/arm64-v8a/libapp.so  |
| 18038034181  | lib/arm64-v8a/libapp.so  |
| 17940498824  | lib/arm64-v8a/libapp.so  |
| 16541071428  | lib/arm64-v8a/libapp.so  |
| 13616389093  | lib/arm64-v8a/libapp.so  |
| 13581355212  | lib/arm64-v8a/libapp.so  |
| 15607138198  | lib/arm64-v8a/libapp.so  |

## **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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2020-07-02 10:04:52+00:00 有效期至: 2047-11-18 10:04:52+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0x4a8d0ac3 哈希算法: sha256 md5值: 7b2de4f9952910daa92313fbe89f03f2 sha1值: 767d9ed693b4ce11cd5c399b2da395c1a95044ef sha256值: 2416a50735c83d18dd7589ac76b2521b3cf88286a15afecd998dd8dbc4f9893c sha512值: 09ea13e52992c0346e2524a12173b3e219f6ca3f459a35b8996c0072cf5950fd11562d09eafff40141e4f838cd30ebef63199459ace70983a59eaaf8bc693f12 公钥算法: rsa 密钥长度: 2048 指纹: 408d7cef296779e6c3208f3a42630cd49bf8136a7c4b49dc15f566dde96ca17b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "auth\_failure\_token\_failuer" : "The network is unstable, please retry."  |
| "firebase\_database\_url" : "https://eadrax-bmw-na-dly-65732.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyAlCUWiGaWXA2eWeTJlHrgiqClJco9T\_2c"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAlCUWiGaWXA2eWeTJlHrgiqClJco9T\_2c"  |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |
| "auth\_failure\_token\_failuer" : "网络异常，请重试。"  |

## **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 |
| --- | --- | --- | --- |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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\_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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| 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。  |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.dck.permission.DIGITAL\_KEY\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.dck.permission.DIGITAL\_KEY\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| org.carconnectivity.android.digitalkey.permission.DIGITAL\_KEY\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| org.carconnectivity.android.digitalkey.permission.DIGITAL\_KEY\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| ANDROID.PERMISSION.CAMERA | 未知 | Unknown permission | Unknown permission from android reference |
| 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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_CONNECTED\_DEVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| de.bmw.connected.mobile20.cn.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| getui.permission.GetuiService.de.bmw.connected.mobile20.cn | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| de.bmw.connected.mobile20.cn.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| de.bmw.connected.mobile20.cn.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| de.bmw.connected.mobile20.cn.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| org.carconnectivity.android.digitalkey.permission.DIGITAL\_KEY\_PRIVILEGED | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.mobileconnected.MainActivity | **Schemes**: https://, de.bmw.connected.mobile20.cn://, com.bmw.connected://, wechatextmsg://, de.bmw.connected.mobile20.cn.bmw.qqmusic://, gtpushscheme://, mybmwmobile://, **Hosts:** mobile20-express.bmw.com.cn, @string/lwa\_host, @string/incarlogin\_host, @string/customer\_host, registerComplete, @string/deeplink\_host, @string/digital\_key\_first\_host, esim, route, de.bmw.connected.mobile20.cn, com.mobile.connected, **Mime Types:** text/\*, **Paths:** /, /main, **Path Patterns:** @string/lwa\_pathPattern, @string/incarlogin\_pathPattern, @string/customer\_pathPattern, @string/deeplink\_pathPattern, @string/digital\_key\_first\_short\_pathPattern, @string/digital\_key\_first\_pathPattern,  |

**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。**