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

**PG电游城（ 110.0.1.8\_g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 | PG电游城 |
| 版本 | 110.0.1.8\_g |
| 包名 | com.tydssdhali513kaiyuangf.www |
| 域名线索 | 99条 |
| URL线索 | 88条 |
| APP图标 |  |
| 分析日期 | 2024年11月1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 | ujyjyhqy.apk |
| 文件大小 | 47.18MB |
| MD5值 | d97b52b233776a1753950493aa35cbc9 |
| SHA1值 | 6da6227dff3b93ec3ea6ade605fe791cea88afae |
| SHA256值 | 2d6fb6b2d03e1a45be17c100da5179413d2f29935f63ebd6de0abd9525f779c0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | PG电游城 |
| 包名 | com.tydssdhali513kaiyuangf.www |
| 主活动Activity | demo.sample.txcode.addfile.ui.acitivity.StartUpActivity |
| 安卓版本名称 | 110.0.1.8\_g |
| 安卓版本 | 110 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tun-cos-1258344701.file.myqcloud.com | IP: 123.6.25.199 所属国家: China 地区: Henan 城市: Zhengzhou  |
| livepullipv6.tlivesource.com | IP: 163.177.30.38 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| webrd0d.is.autonavi.com | 没有服务器地理信息.  |
| epalbigty513laosi.xn--ojqs38cba559m.cn | IP: 207.46.141.190 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| apiinit.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| issuetracker.google.com | IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| cloud.tim.qq.com | IP: 111.206.149.220 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  |
| intl.cloud.tencent.com | IP: 61.49.23.183 所属国家: China 地区: Beijing 城市: Beijing  |
| liteav.sdk.qcloud.com | IP: 42.236.89.7 所属国家: China 地区: Henan 城市: Zhengzhou  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| web.sdk.qcloud.com | IP: 123.6.37.172 所属国家: China 地区: Henan 城市: Zhengzhou  |
| lbs.amap.com | IP: 59.82.60.60 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mqqeve.beacon.qq.com | IP: 182.50.13.56 所属国家: China 地区: Beijing 城市: Beijing  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| apilocatesrc.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| otheve.beacon.qq.com | IP: 113.56.189.242 所属国家: China 地区: Hubei 城市: Huangshi  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| snowflake.qq.com | IP: 116.130.220.107 所属国家: China 地区: Beijing 城市: Beijing  |
| sdkconfig.tlivesource.com | IP: 140.207.121.106 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grid.amap.com | IP: 59.82.31.137 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 162.14.19.114 | IP: 162.14.19.114 所属国家: China 地区: Beijing 城市: Beijing  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| trtc-sdk-config-xjp-1258344699.cos.ap-singapore.intltencentcos.com | IP: 119.28.121.12 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mst0d.is.autonavi.com | 没有服务器地理信息.  |
| cgicol.amap.com | IP: 123.125.216.211 所属国家: China 地区: Beijing 城市: Beijing  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tcdns.tlivesource.com | IP: 109.244.168.185 所属国家: China 地区: Beijing 城市: Beijing  |
| zzh3.sin55ck8.xyz | IP: 20.24.194.210 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cos-android-sdk-doc-1253960454.cos.ap-shanghai.myqcloud.com | IP: 112.86.231.46 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| 119.29.29.98 | IP: 119.29.29.98 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dashif.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 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  |
| 1.12.12.12 | IP: 1.12.12.12 所属国家: China 地区: Beijing 城市: Beijing  |
| rtnkbigty513erfb.xn--mjrs9ykk0bopd.cn | IP: 123.126.74.190 所属国家: China 地区: Beijing 城市: Beijing  |
| common-proxy-test.rtc.tencent.com | IP: 175.27.204.228 所属国家: China 地区: Beijing 城市: Beijing  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 223.6.6.6 | IP: 223.6.6.6 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tm.amap.com | IP: 59.82.31.99 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| speedtestint.trtc.tencent-cloud.com | IP: 43.156.86.158 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| test.snowflake.qq.com | IP: 221.198.69.15 所属国家: China 地区: Tianjin 城市: Tianjin  |
| schemas.android.com | 没有服务器地理信息.  |
| logs.amap.com | IP: 123.125.216.212 所属国家: China 地区: Beijing 城市: Beijing  |
| 162.14.3.250 | IP: 162.14.3.250 所属国家: China 地区: Beijing 城市: Beijing  |
| maps.google.cn | IP: 114.250.69.34 所属国家: China 地区: Beijing 城市: Beijing  |
| buy.cloud.tencent.com | IP: 123.125.244.107 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.android.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| ns.adobe.com | 没有服务器地理信息.  |
| sdkdc.live.tlivesource.com | IP: 43.130.137.111 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| mdc.html5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| trtc-sdk-log-1258344699.cos.ap-guangzhou.tencentcos.cn | IP: 36.248.13.178 所属国家: China 地区: Fujian 城市: Fuzhou  |
| inland-sdklog.trtc.tencent-cloud.com | IP: 120.53.64.22 所属国家: China 地区: Beijing 城市: Beijing  |
| qaty366webapi.ebgb0c05.xyz | IP: 43.249.29.19 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| flvmock.tencent.com | 没有服务器地理信息.  |
| livepull.tlivesource.com | IP: 116.130.223.85 所属国家: China 地区: Beijing 城市: Beijing  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| speedtest.trtc.tencent-cloud.com | IP: 162.14.20.26 所属国家: China 地区: Beijing 城市: Beijing  |
| m5.amap.com | IP: 106.11.35.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 106.55.123.30 | IP: 106.55.123.30 所属国家: China 地区: Beijing 城市: Beijing  |
| restapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tbs.imtt.qq.com | IP: 124.95.177.244 所属国家: China 地区: Liaoning 城市: Shenyang  |
| wb.amap.com | IP: 59.82.31.104 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 1.0.0.1 | IP: 1.0.0.1 所属国家: United States of America 地区: California 城市: San Jose  |
| intl-sdklog.trtc.tencent-cloud.com | IP: 43.156.222.59 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dartbug.com | IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| common-proxy.rtc.tencent.com | IP: 106.53.137.225 所属国家: China 地区: Beijing 城市: Beijing  |
| othstr.beacon.qq.com | IP: 140.206.162.29 所属国家: China 地区: Shanghai 城市: Shanghai  |
| common-proxyintl.rtc.tencent.com | IP: 43.156.223.209 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| ipof.in | IP: 104.21.15.155 所属国家: United States of America 地区: California 城市: San Francisco  |
| mlvbdc.live.tlivesource.com | IP: 116.147.17.62 所属国家: China 地区: Beijing 城市: Beijing  |
| privacy.qq.com | IP: 123.6.33.209 所属国家: China 地区: Henan 城市: Zhengzhou  |
| www.ibm.com | IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| wap.amap.com | IP: 125.39.43.232 所属国家: China 地区: Tianjin 城市: Tianjin  |
| sdk-liteav-1252463788.cos.ap-hongkong.tencentcos.cn | IP: 43.128.240.61 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| trtc-client-log-overseas-1258344699.cos.ap-singapore.intltencentcos.com | IP: 150.109.0.195 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| apisgp.my-imcloud.com | IP: 123.123.191.101 所属国家: China 地区: Beijing 城市: Beijing  |
| www.tencentcloud.com | IP: 43.152.65.114 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| demos.trtc.tencent-cloud.com | IP: 123.125.244.54 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| events.my-imcloud.com | IP: 111.206.147.103 所属国家: China 地区: Beijing 城市: Beijing  |
| avmonitortest.trtc.tencent-cloud.com | IP: 106.53.137.253 所属国家: China 地区: Beijing 城市: Beijing  |
| tcdnsipv6.tlivesource.com | 没有服务器地理信息.  |
| cloud.tencent.com | IP: 61.49.23.183 所属国家: China 地区: Beijing 城市: Beijing  |
| htrace.wetvinfo.com | IP: 60.28.215.54 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 8.8.4.4 | IP: 8.8.4.4 所属国家: United States of America 地区: California 城市: Mountain View  |
| console.cloud.tencent.com | IP: 123.125.244.107 所属国家: China 地区: Beijing 城市: Beijing  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| im.sdk.qcloud.com | IP: 123.6.37.221 所属国家: China 地区: Henan 城市: Zhengzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://dashif.org/guidelines/last-segment-number  | a7/d.java  |
| http://dashif.org/guidelines/trickmode  | a7/d.java  |
| http://dashif.org/thumbnail\_tile  | a7/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | a7/d.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://wap.amap.com/  | com/amap/api/maps2d/AMapUtils.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://h.trace.qq.com/kv  | com/tencent/beacon/a/b/g.java  |
| https://htrace.wetvinfo.com/kv  | com/tencent/beacon/a/b/d.java  |
| https://h.trace.qq.com/kv  | com/tencent/beacon/a/b/d.java  |
| https://otheve.beacon.qq.com/analytics/v2\_upload  | com/tencent/beacon/base/net/b/b.java  |
| https://othstr.beacon.qq.com/analytics/v2\_upload  | com/tencent/beacon/base/net/b/b.java  |
| https://mqqeve.beacon.qq.com/analytics/v2\_upload  | com/tencent/beacon/base/net/b/b.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://h.trace.qq.com/kv  | com/tencent/bugly/proguard/ad.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/proguard/ac.java  |
| https://web.sdk.qcloud.com/component/tuiroom/index.html  | com/tencent/cloud/tuikit/roomkit/viewmodel/RoomInfoViewModel.java  |
| https://cos-android-sdk-doc-1253960454.cos.ap-shanghai.myqcloud.com/beacon\_cc/android/  | com/tencent/cos/xml/CloudControl.java  |
| http://xmlpull.org/v1/doc/features.html  | com/tencent/cos/xml/transfer/XmlSlimBuilder.java  |
| http://xmlpull.org/v1/doc/features.html  | com/tencent/cos/xml/transfer/XmlBuilder.java  |
| http://www.w3.org/2001/XMLSchema-instance  | com/tencent/cos/xml/transfer/XmlBuilder.java  |
| http://xmlpull.org/v1/doc/features.html  | com/tencent/qcloud/qcloudxml/core/QCloudXml.java  |
| http://second  | com/tencent/qcloud/tim/demo/DemoApplication.java  |
| http://debugtbs.qq.com  | com/tencent/qcloud/tim/demo/main/MainNormalActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tim/demo/profile/AboutIMActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tim/demo/profile/AboutIMMinamalistActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/avatar/avatar\_%s.png  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://privacy.qq.com/document/preview/c63a48325d0e4a35b93f675205a65a77  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://privacy.qq.com/document/preview/1cfe904fb7004b8ab1193a55857f7272  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://privacy.qq.com/document/preview/45ba982a1ce6493597a00f8c86b52a1e  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://privacy.qq.com/document/preview/dea84ac4bb88454794928b77126e9246  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://web.sdk.qcloud.com/document/Tencent-IM-User-Agreement.html  | com/tencent/qcloud/tim/demo/utils/Constants.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://cloud.tencent.com/document/product/269/11673?from=17219  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://www.tencentcloud.com/document/product/1047/34349  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/conversation-backgroundImage/backgroundImage\_%s\_full.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuicore/TUIConstants.java  |
| https://demos.trtc.tencent-cloud.com/prod/base/v1/events/stat  | com/tencent/qcloud/tuicore/TUIConfig.java  |
| https://buy.cloud.tencent.com/avc  | com/tencent/qcloud/tuikit/tuicallengine/a.java  |
| https://console.cloud.tencent.com/im/detail  | com/tencent/qcloud/tuikit/tuicallengine/a.java  |
| https://cloud.tencent.com/document/product/269/32458  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://intl.cloud.tencent.com/document/product/1047/36021?lang=en&pg=  | com/tencent/qcloud/tuikit/tuichat/TUIChatConstants.java  |
| https://cloud.tencent.com/document/product/269/3794  | com/tencent/qcloud/tuikit/tuichat/bean/CustomHelloMessage.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CreateCommunityActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/ui/page/CommunitySettingsActivity.java  |
| https://cloud.tencent.com/document/product/269/75979  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/community-cover/community\_cover\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_default.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/document/product/269/36852  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/act/pro/imnew?from=17971  | com/tencent/qcloud/tuikit/tuicommunity/utils/CommunityConstants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://www.tencentcloud.com/products/im?lang=en&pg=  | com/tencent/qcloud/tuikit/tuicontact/TUIContactConstants.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/GroupTypeSelectActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/classicui/pages/CreateGroupActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/GroupTypeSelectMinimalistActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://cloud.tencent.com/product/im  | com/tencent/qcloud/tuikit/tuicontact/minimalistui/pages/CreateGroupMinimalistActivity.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/TUIGroupConstants.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/classicui/page/GroupInfoFragment.java  |
| https://im.sdk.qcloud.com/download/tuikit-resource/group-avatar/group\_avatar\_%s.png  | com/tencent/qcloud/tuikit/tuigroup/minimalistui/page/GroupInfoMinimalistFragment.java  |
| https://tun-cos-1258344701.file.myqcloud.com/fp.js  | com/tencent/qimei/ae/a.java  |
| https://tun-cos-1258344701.file.myqcloud.com/fp.js  | com/tencent/qimei/ae/c.java  |
| https://tun-cos-1258344701.file.myqcloud.com/my.html  | com/tencent/qimei/ae/c.java  |
| https://snowflake.qq.com/ola  | com/tencent/qimei/h/b.java  |
| https://test.snowflake.qq.com/ola  | com/tencent/qimei/h/b.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/j.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  |
| 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://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | com/tencent/smtt/utils/d.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/o.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/o.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/o.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | d2/a.java  |
| https://ipof.in/txt  | dd/q.java  |
| http://zzh3.sin55ck8.xyz/api/v1/alert  | dd/q.java  |
| http://second  | dd/e.java  |
| http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red  | demo/sample/txcode/addfile/ui/acitivity/LocationAmapActivity.java  |
| http://schemas.android.com/apk/res/android  | e1/j.java  |
| http://ns.adobe.com/xap/1.0/  | g6/a.java  |
| https://8.8.4.4/resolve  | gc/a.java  |
| https://1.0.0.1/dns-query  | gc/a.java  |
| https://1.12.12.12/dns-query  | gc/a.java  |
| https://223.6.6.6/resolve  | gc/a.java  |
| http://restapi.amap.com/v3/place/around?  | i3/a.java  |
| http://restapi.amap.com/v3/place/text?  | i3/a.java  |
| http://restapi.amap.com/v3/config/district?  | i3/a.java  |
| http://restapi.amap.com  | i3/d4.java  |
| http://apilocate.amap.com/mobile/binary  | i3/f4.java  |
| http://apilocatesrc.amap.com/mobile/binary  | i3/f4.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | i3/f4.java  |
| http://restapi.amap.com/v3  | i3/g2.java  |
| https://restapi.amap.com/v3  | i3/g2.java  |
| http://yuntuapi.amap.com  | i3/g2.java  |
| https://yuntuapi.amap.com  | i3/g2.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | i3/g2.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | i3/g2.java  |
| http://tm.amap.com  | i3/i0.java  |
| http://wprd0%d.is.autonavi.com  | i3/i0.java  |
| http://webrd0%d.is.autonavi.com  | i3/i0.java  |
| http://grid.amap.com/grid/%d/%d/%d?ds=  | i3/i0.java  |
| http://mst0%d.is.autonavi.com  | i3/i0.java  |
| http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s  | i3/j4.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | i3/j7.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | i3/t3.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | i3/t3.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | i3/t3.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | i3/t3.java  |
| https://restapi.amap.com/v3/iasdkauth  | i3/x3.java  |
| http://apiinit.amap.com/v3/log/init  | i3/y3.java  |
| http://cgicol.amap.com/collection/writedata?ver=v1.0\_ali&  | i3/q6.java  |
| http://restapi.amap.com/v3/geocode/regeo  | i3/q6.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | ie/h.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | ie/c.java  |
| http://www.slf4j.org/codes.html  | ig/c.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | ke/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | ke/d.java  |
| http://www.w3.org/ns/ttml  | m7/c.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | o3/p.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/f.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextureView.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | q7/x.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | t1/m.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | w5/b1.java  |
| https://epalbigty513laosi.xn--ojqs38cba559m.cn/tynibigty513asd/pashroot  | Mogua Engine V1  |
| https://rtnkbigty513erfb.xn--mjrs9ykk0bopd.cn/tynibigty513asd/pashroot  | Mogua Engine V1  |
| https://cloud.tencent.com/document/product/269/37059  | Mogua Engine V1  |
| https://qaty366webapi.ebgb0c05.xyz  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | lib/armeabi-v7a/libflutter.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libflutter.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://sdkdc.live.tlivesource.com/liteav  | lib/armeabi-v7a/libliteavsdk.so  |
| https://mlvbdc.live.tlivesource.com/liteav  | lib/armeabi-v7a/libliteavsdk.so  |
| https://intl-sdklog.trtc.tencent-cloud.com/log/report  | lib/armeabi-v7a/libliteavsdk.so  |
| https://inland-sdklog.trtc.tencent-cloud.com/log/report  | lib/armeabi-v7a/libliteavsdk.so  |
| https://106.55.123.30/rainbowapi.configs/getdatas  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-sdk-config-xjp-1258344699.cos.ap-singapore.intltencentcos.com/liteavsvrcfg/v3/serverconfig\_enc.zip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://sdk-liteav-1252463788.cos.ap-hongkong.tencentcos.cn/sdkres/config/v2/serverconfig\_enc.zip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://intl-sdklog.trtc.tencent-cloud.com/log/appsign  | lib/armeabi-v7a/libliteavsdk.so  |
| https://inland-sdklog.trtc.tencent-cloud.com/log/appsign  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-sdk-log-1258344699.cos.ap-guangzhou.tencentcos.cn  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxy.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxy-test.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxyintl.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-client-log-overseas-1258344699.cos.ap-singapore.intltencentcos.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://test.tim.qq.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://events.my-imcloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://apisgp.my-imcloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://speedtest.trtc.tencent-cloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://speedtestint.trtc.tencent-cloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://avmonitortest.trtc.tencent-cloud.com:8000  | lib/armeabi-v7a/libliteavsdk.so  |
| http://flvmock.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://cloud.tencent.com/act/event/License  | lib/armeabi-v7a/libliteavsdk.so  |
| https://liteav.sdk.qcloud.com/sdkres/trtc/AiVoiceEnhancement  | lib/armeabi-v7a/libliteavsdk.so  |
| https://liteav.sdk.qcloud.com/sdkres/trtc/AiVoiceEnhancement/TNNE\_HOWLING\_SUPPRESSION\_1.37\_11.0.zip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://sdkconfig.tlivesource.com/rainbowapi.configs/getdatas  | lib/armeabi-v7a/libliteavsdk.so  |
| https://tcdns.tlivesource.com/queryip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://tcdnsipv6.tlivesource.com/queryip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://livepull.tlivesource.com/getpulladdr  | lib/armeabi-v7a/libliteavsdk.so  |
| https://livepullipv6.tlivesource.com/getpulladdr  | lib/armeabi-v7a/libliteavsdk.so  |
| https://cloud.tim.qq.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/1998/Math/MathML  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/svg  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList  | lib/armeabi-v7a/libImSDK.so  |
| http://119.29.29.98/d?id=39662  | lib/armeabi-v7a/libImSDK.so  |
| http://162.14.19.114/  | lib/armeabi-v7a/libImSDK.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided  | com/tencent/liteav/base/PiiElider.java  |
| x5tbs@tencent.com  | com/tencent/smtt/sdk/X5Downloader.java  |
| checked2@2x.png  | Mogua Engine V2  |
| \_nativesocket@14069316.listen \_httpparser@13463476.responsepa checked2@2x.png \_internetaddress@14069316.fixed \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_routedata@1070504625.ofroute \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_imagefilter@15065589.composed \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_invocationmirror@0150898.\_withtype androidstorage@27339836.implementa channelcontroller@29156646.implementa \_colorfilter@15065589.lineartosr \_growablelist@0150898.\_literal1 \_uri@0150898.file \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of authenticationscheme@13463476.fromstring \_pointerpanzoomdata@605213599.fromupdate \_list@0150898.of \_compressednode@107137193.single \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_future@4048458.value \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_assetmanifestbin@45287047.fromstanda \_list@0150898.\_ofother \_bytebuffer@7027147.\_new ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_hashcollisionnode@107137193.fromcollis \_imagefilter@15065589.fromcolorf \_colorfilter@15065589.srgbtoline \_uri@0150898.directory \_httpparser@13463476.requestpar \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_future@4048458.zonevalue \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/tencent/qcloud/tuikit/tuigroupnoteplugin/f/f.java  |
| 17179869184  | com/tencent/qcloud/tuikit/tuigroupnoteplugin/f/c.java  |
| 18222222222  | h6/e.java  |
| 19222222222  | h6/e.java  |
| 17512775099  | q8/a.java  |

## **5. 签名证书**

**无法读取代码签名证书.**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Proxy\_Authorization" : "6dDUxMw==c"  |
| "SecretKey" : ""  |
| "appzhifumima" : "APP支付密码："  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "haimeiyoushezhizhifumima\_qingxianshezhizhifumima" : "还没有设置支付密码，请先设置支付密码"  |
| "haimeiyoushezhizhifumima\_shifoushezhi" : "还没有设置支付密码，是否设置？"  |
| "input\_password" : "请输入密码"  |
| "jizhumima" : "记住密码"  |
| "liangcimimabuyizhi\_qingjiancha" : "两次密码不一致，请检查"  |
| "liangcimimarushubuyizhi" : "两次密码输入不一致"  |
| "meizuPushAppKey" : "xxxxxx"  |
| "mimabunengweikong" : "密码不能为空"  |
| "mimaxiugaichenggong" : "密码修改成功"  |
| "oppoPushAppKey" : "xxxxxx"  |
| "oppoPushAppSecret" : "xxxxxx"  |
| "password" : "密码"  |
| "please\_zhifumima" : "请输入支付密码"  |
| "private\_group" : "讨论组"  |
| "qingjietubaocunnindezhanghaohemima" : "请截图保存您的账号和密码： 账号：%s 密码：%s"  |
| "qingquerenxinmima" : "请确认新密码"  |
| "qingshezhizhifumima" : "设置支付密码"  |
| "qingshurujiumima" : "请输入旧密码"  |
| "qingshuruxinmima" : "请输入新密码"  |
| "qingshuruyuanmima" : "请输入原密码"  |
| "qingshuruzhifumima" : "请输入支付密码"  |
| "qingzaicishurumima" : "请再次输入密码"  |
| "qingzaicishuruquerenmima" : "请再次输入确认密码"  |
| "querenmima" : "确认密码"  |
| "tuiroomkit\_mute\_user" : "禁言"  |
| "tuiroomkit\_un\_mute\_user" : "取消禁言"  |
| "wangjimima" : "忘记密码"  |
| "xiaomiPushAppKey" : "xxxxxx"  |
| "xinmima" : "新密码"  |
| "xinmimabuyizhi" : "新密码不一致"  |
| "xinmimaqueren" : "新密码确认"  |
| "xiugaimima" : "修改密码"  |
| "xiugaizhifumima" : "修改支付密码"  |
| "yuanmima" : "原密码"  |
| "zhifumima" : "支付密码"  |
| "zhifumimashezhichenggong" : "支付密码设置成功"  |
| "zhifumimaxiugaichenggong" : "支付密码修改成功"  |
| "appzhifumima" : "APP 支払いパスワード:"  |
| "contact\_no\_such\_user" : "ユーザーは存在しません"  |
| "haimeiyoushezhizhifumima\_qingxianshezhizhifumima" : "支払いパスワードがまだ設定されていません。最初に支払いパスワードを設定してください。"  |
| "haimeiyoushezhizhifumima\_shifoushezhi" : "支払いパスワードがまだ設定されていませんが、設定されていますか?"  |
| "input\_password" : "パスワードを 6 ～ 20 文字の文字または数字で入力してください"  |
| "jizhumima" : "パスワードを覚えておいてください"  |
| "liangcimimabuyizhi\_qingjiancha" : "2 つのパスワードが一致しません。確認してください。"  |
| "liangcimimarushubuyizhi" : "入力された 2 つのパスワードは矛盾しています"  |
| "mimabunengweikong" : "パスワードを空にすることはできません"  |
| "mimaxiugaichenggong" : "パスワードが正常に変更されました"  |
| "password" : "パスワード"  |
| "please\_zhifumima" : "支払いパスワードを入力してください"  |
| "private\_group" : "ディスカッション グループ"  |
| "qingjietubaocunnindezhanghaohemima" : "スクリーンショットを撮ってアカウントとパスワードを保存してください: アカウント: %s パスワード: %s"  |
| "qingquerenxinmima" : "新しいパスワードを確認してください"  |
| "qingshezhizhifumima" : "支払いパスワードを設定する"  |
| "qingshuruxinmima" : "新しいパスワードを入力してください"  |
| "qingshuruyuanmima" : "元のパスワードを入力してください"  |
| "qingshuruzhifumima" : "支払いパスワードを入力してください"  |
| "qingzaicishurumima" : "パスワードをもう一度入力してください"  |
| "qingzaicishuruquerenmima" : "確認パスワードをもう一度入力してください"  |
| "querenmima" : "パスワードの確認"  |
| "tuiroomkit\_mute\_user" : "ミュート"  |
| "tuiroomkit\_un\_mute\_user" : "禁止解除"  |
| "wangjimima" : "パスワードを忘れた"  |
| "xinmima" : "新しいパスワード"  |
| "xinmimabuyizhi" : "新しいパスワードは一貫性がありません"  |
| "xinmimaqueren" : "新しいパスワードの確認"  |
| "xiugaimima" : "パスワードを変更"  |
| "xiugaizhifumima" : "支払いパスワードを変更する"  |
| "yuanmima" : "のパスワード"  |
| "zhifumimashezhichenggong" : "支払いパスワードが正常に設定されました"  |
| "zhifumimaxiugaichenggong" : "支払いパスワードが正常に変更されました"  |
| "appzhifumima" : "Mật khẩu thanh toán APP:"  |
| "contact\_no\_such\_user" : "Người dùng không tồn tại"  |
| "haimeiyoushezhizhifumima\_qingxianshezhizhifumima" : "Mật khẩu thanh toán chưa được đặt, vui lòng đặt mật khẩu thanh toán trước"  |
| "haimeiyoushezhizhifumima\_shifoushezhi" : "Mật khẩu thanh toán chưa được đặt, đã đặt chưa?"  |
| "input\_password" : "Vui lòng nhập mật khẩu, 6~20 chữ cái hoặc số"  |
| "jizhumima" : "Nhớ mật khẩu"  |
| "liangcimimabuyizhi\_qingjiancha" : "Hai mật khẩu không nhất quán, vui lòng kiểm tra"  |
| "liangcimimarushubuyizhi" : "Hai mật khẩu đã nhập không nhất quán"  |
| "mimabunengweikong" : "Mật khẩu không được để trống"  |
| "mimaxiugaichenggong" : "Mật khẩu đã được thay đổi thành công"  |
| "password" : "Mật khẩu"  |
| "please\_zhifumima" : "Vui lòng nhập mật khẩu thanh toán"  |
| "private\_group" : "Nhóm thảo luận"  |
| "qingjietubaocunnindezhanghaohemima" : "Vui lòng chụp ảnh màn hình để lưu tài khoản và mật khẩu của bạn: Tài khoản: %s Mật khẩu: %s"  |
| "qingquerenxinmima" : "Vui lòng xác nhận mật khẩu mới"  |
| "qingshezhizhifumima" : "Đặt mật khẩu thanh toán"  |
| "qingshuruxinmima" : "Vui lòng nhập mật khẩu mới"  |
| "qingshuruyuanmima" : "Vui lòng nhập mật khẩu ban đầu"  |
| "qingshuruzhifumima" : "Vui lòng nhập mật khẩu thanh toán"  |
| "qingzaicishurumima" : "Vui lòng nhập lại mật khẩu của bạn"  |
| "qingzaicishuruquerenmima" : "Vui lòng nhập lại mật khẩu xác nhận"  |
| "querenmima" : "Xác nhận mật khẩu"  |
| "tuiroomkit\_mute\_user" : "Tắt tiếng"  |
| "tuiroomkit\_un\_mute\_user" : "Bỏ cấm"  |
| "wangjimima" : "quên mật khẩu"  |
| "xinmima" : "Mật khẩu mới"  |
| "xinmimabuyizhi" : "Mật khẩu mới không nhất quán"  |
| "xinmimaqueren" : "Xác nhận mật khẩu mới"  |
| "xiugaimima" : "Đổi mật khẩu"  |
| "xiugaizhifumima" : "Thay đổi mật khẩu thanh toán"  |
| "yuanmima" : "Mật khẩu gốc"  |
| "zhifumimashezhichenggong" : "Đã đặt mật khẩu thanh toán thành công"  |
| "zhifumimaxiugaichenggong" : "Mật khẩu thanh toán đã được thay đổi thành công"  |
| "appzhifumima" : "APP支付密码："  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "haimeiyoushezhizhifumima\_qingxianshezhizhifumima" : "还没有设置支付密码，请先设置支付密码"  |
| "haimeiyoushezhizhifumima\_shifoushezhi" : "还没有设置支付密码，是否设置？"  |
| "input\_password" : "请输入密码"  |
| "jizhumima" : "记住密码"  |
| "liangcimimabuyizhi\_qingjiancha" : "两次密码不一致，请检查"  |
| "liangcimimarushubuyizhi" : "两次密码输入不一致"  |
| "mimabunengweikong" : "密码不能为空"  |
| "mimaxiugaichenggong" : "密码修改成功"  |
| "password" : "密码"  |
| "please\_zhifumima" : "请输入支付密码"  |
| "private\_group" : "讨论组"  |
| "qingjietubaocunnindezhanghaohemima" : "请截图保存您的账号和密码： 账号：%s 密码：%s"  |
| "qingquerenxinmima" : "请确认新密码"  |
| "qingshezhizhifumima" : "设置支付密码"  |
| "qingshuruxinmima" : "请输入新密码"  |
| "qingshuruyuanmima" : "请输入原密码"  |
| "qingshuruzhifumima" : "请输入支付密码"  |
| "qingzaicishurumima" : "请再次输入密码"  |
| "qingzaicishuruquerenmima" : "请再次输入确认密码"  |
| "querenmima" : "确认密码"  |
| "tuiroomkit\_mute\_user" : "禁言"  |
| "tuiroomkit\_un\_mute\_user" : "取消禁言"  |
| "wangjimima" : "忘记密码"  |
| "xinmima" : "新密码"  |
| "xinmimabuyizhi" : "新密码不一致"  |
| "xinmimaqueren" : "新密码确认"  |
| "xiugaimima" : "修改密码"  |
| "xiugaizhifumima" : "修改支付密码"  |
| "yuanmima" : "原密码"  |
| "zhifumimashezhichenggong" : "支付密码设置成功"  |
| "zhifumimaxiugaichenggong" : "支付密码修改成功"  |
| "appzhifumima" : "APP payment password:"  |
| "contact\_no\_such\_user" : "This user does not exist"  |
| "haimeiyoushezhizhifumima\_qingxianshezhizhifumima" : "The payment password has not been set yet, please set the payment password first"  |
| "haimeiyoushezhizhifumima\_shifoushezhi" : "The payment password has not been set yet. Do you want to set it?"  |
| "input\_password" : "Please enter password, 6~20 letters or numbers"  |
| "jizhumima" : "Remember the password"  |
| "liangcimimabuyizhi\_qingjiancha" : "The two passwords are inconsistent, please check"  |
| "liangcimimarushubuyizhi" : "The two password inputs are inconsistent"  |
| "mimabunengweikong" : "Password cannot be empty"  |
| "mimaxiugaichenggong" : "Password changed successfully"  |
| "password" : "Password"  |
| "please\_zhifumima" : "Please enter the payment password"  |
| "private\_group" : "discussion group"  |
| "qingjietubaocunnindezhanghaohemima" : "Please take a screenshot to save your account and password: Account: %s Password: %s"  |
| "qingquerenxinmima" : "Please confirm the new password"  |
| "qingshezhizhifumima" : "Set payment password"  |
| "qingshuruxinmima" : "Please enter a new password"  |
| "qingshuruyuanmima" : "Please enter the original password"  |
| "qingshuruzhifumima" : "Please enter the payment password"  |
| "qingzaicishurumima" : "Please enter the password again"  |
| "qingzaicishuruquerenmima" : "Please enter the confirmation password again"  |
| "querenmima" : "Confirm password"  |
| "tuiroomkit\_mute\_user" : "Mute"  |
| "tuiroomkit\_un\_mute\_user" : "Unban"  |
| "wangjimima" : "forgot password"  |
| "xinmima" : "New password"  |
| "xinmimabuyizhi" : "New password is inconsistent"  |
| "xinmimaqueren" : "New password confirmation"  |
| "xiugaimima" : "Change password"  |
| "xiugaizhifumima" : "Change payment password"  |
| "yuanmima" : "Original password"  |
| "zhifumimashezhichenggong" : "The payment password is set successfully"  |
| "zhifumimaxiugaichenggong" : "Payment password changed successfully"  |

## **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.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.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.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.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\_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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.POS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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\_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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_MEDIA\_IMAGES | 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.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |
| 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.tydssdhali513kaiyuangf.www.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| demo.sample.txcode.addfile.ui.acitivity.StartUpActivity | **Schemes**: idolchat://, X://, fi3z0h7b://, **Hosts:** idolchatadd, idolchatshare,  |
| com.tencent.qcloud.tim.demo.main.MainNormalActivity | **Schemes**: pushscheme://, **Hosts:** com.tencent.qcloud, **Paths:** /detail,  |
| com.tencent.qcloud.tim.demo.main.MainMinimalistActivity | **Schemes**: pushscheme://, **Hosts:** com.tencent.qcloud, **Paths:** /detail,  |

**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。**