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

**小辣椒（ 1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 | 小辣椒 |
| 版本 | 1 |
| 包名 | com.pro.gnewp |
| 域名线索 | 119条 |
| URL线索 | 86条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 小辣椒.apk |
| 文件大小 | 137.96MB |
| MD5值 | 114a9bce55789ee6db302befa7eab866 |
| SHA1值 | 4a5204614cc15089332a03ceb77a6e8c653061f6 |
| SHA256值 | 722c83d76b4f697e068857683f269e1a30e7ec5ec736ebe68d73e8b11a9202a4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小辣椒 |
| 包名 | com.pro.gnewp |
| 主活动Activity | com.pro.gnewp.activity.SplashActivity |
| 安卓版本名称 | 1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| rsf.qiniu.com | IP: 124.160.115.103 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| data.facegl.com | IP: 47.104.165.23 所属国家: China 地区: Shandong 城市: Qingdao  |
| rsf-as0.qiniu.com | IP: 116.196.140.63 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| fusion.qiniuapi.com | IP: 27.221.14.166 所属国家: China 地区: Shandong 城市: Qingdao  |
| rs-z2.qiniu.com | IP: 120.83.145.14 所属国家: China 地区: Guangdong 城市: Foshan  |
| fusion.qq.com | IP: 116.130.229.204 所属国家: China 地区: Beijing 城市: Beijing  |
| up-z2.qiniup.com | IP: 163.142.153.211 所属国家: China 地区: Guangdong 城市: Foshan  |
| upload-z2.qiniup.com | IP: 120.83.145.4 所属国家: China 地区: Guangdong 城市: Foshan  |
| qyspare.chatchat.vip | IP: 45.199.32.231 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| guoek.sevenghosts.cn | IP: 103.7.141.50 所属国家: China 地区: Hubei 城市: Shiyan  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| rsf.qbox.me | IP: 101.251.144.177 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| free-qvm-z0-xs.qiniup.com | IP: 100.103.4.62 所属国家: - 地区: - 城市: -  |
| api-as0.qiniu.com | IP: 116.196.140.68 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| appcashier256.95516.com | IP: 220.194.105.87 所属国家: China 地区: Tianjin 城市: Tianjin  |
| uc.qbox.me | IP: 101.251.144.177 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| up-as0.qiniu.com | IP: 154.41.93.11 所属国家: Canada 地区: Quebec 城市: Montreal  |
| m.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tsis.jpush.cn | IP: 110.41.23.105 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| graph.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| rs-z2.qbox.me | IP: 163.142.153.214 所属国家: China 地区: Guangdong 城市: Foshan  |
| vodreport.qcloud.com | IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| upload-z1.qiniup.com | IP: 110.242.48.22 所属国家: China 地区: Hebei 城市: Baoding  |
| rs.qbox.me | IP: 101.251.144.179 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| adiu.amap.com | IP: 110.253.189.146 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| qvs.qiniuapi.com | IP: 122.195.131.81 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| api-na0.qiniu.com | IP: 116.196.140.64 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| authsdk.tillusory.com | IP: 47.122.23.250 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| iovip-z1.qbox.me | IP: 110.242.48.24 所属国家: China 地区: Hebei 城市: Baoding  |
| up-as0.qiniup.com | IP: 154.41.93.11 所属国家: Canada 地区: Quebec 城市: Montreal  |
| lbs.amap.com | IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| rsf-z2.qbox.me | IP: 163.142.153.214 所属国家: China 地区: Guangdong 城市: Foshan  |
| rs-as0.qiniu.com | IP: 116.196.140.66 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| sandcash.mixienet.com.cn | IP: 203.107.86.172 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| bjuser.jpush.cn | IP: 122.9.5.30 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.weixin.qq.com | IP: 112.65.193.153 所属国家: China 地区: Shanghai 城市: Shanghai  |
| rs.qiniu.com | IP: 153.99.246.130 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing  |
| api-z2.qiniu.com | IP: 163.142.153.217 所属国家: China 地区: Guangdong 城市: Foshan  |
| linking.qiniuapi.com | IP: 114.230.94.210 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| up-z2.qiniu.com | IP: 120.83.145.4 所属国家: China 地区: Guangdong 城市: Foshan  |
| qzs.qq.com | IP: 221.204.14.52 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| mobilegw.alipay.com | IP: 203.209.250.8 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.1-liao.com | IP: 72.52.179.174 所属国家: United States of America 地区: Michigan 城市: Lansing  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-s.qiniu.com | 没有服务器地理信息.  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| api-cn.faceplusplus.com | IP: 60.205.234.99 所属国家: China 地区: Beijing 城市: Beijing  |
| com.thoughtworks.xstream | 没有服务器地理信息.  |
| up-na0.qiniu.com | IP: 148.153.188.134 所属国家: United States of America 地区: Texas 城市: Dallas  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| pili.qiniuapi.com | IP: 110.242.48.43 所属国家: China 地区: Hebei 城市: Baoding  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| rs-as0.qbox.me | IP: 116.196.140.67 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| rsf-na0.qiniu.com | IP: 116.196.140.68 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| rsf-na0.qbox.me | IP: 116.196.140.66 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| pipeline.qiniu.com | 没有服务器地理信息.  |
| rsf-z2.qiniu.com | IP: 163.142.153.217 所属国家: China 地区: Guangdong 城市: Foshan  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| iovip-z2.qbox.me | IP: 163.142.153.211 所属国家: China 地区: Guangdong 城市: Foshan  |
| open.weixin.qq.com | IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api.qiniu.com | IP: 124.160.115.102 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-us.faceplusplus.com | IP: 3.96.36.235 所属国家: Canada 地区: Quebec 城市: Montreal  |
| iovip.qbox.me | IP: 112.82.212.155 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| iovip-as0.qbox.me | IP: 154.41.93.9 所属国家: Canada 地区: Quebec 城市: Montreal  |
| www.bt.cn | IP: 157.255.129.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| up-z1.qiniup.com | IP: 110.242.48.121 所属国家: China 地区: Hebei 城市: Baoding  |
| argus.agoralab.co | IP: 218.24.90.145 所属国家: China 地区: Liaoning 城市: Shenyang  |
| up-z1.qiniu.com | IP: 110.242.48.122 所属国家: China 地区: Hebei 城市: Baoding  |
| apiinit.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| rtc.qiniuapi.com | IP: 110.242.48.50 所属国家: China 地区: Hebei 城市: Baoding  |
| tb.53kf.com | IP: 101.66.249.253 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| paygate-yf.meituan.com | IP: 101.236.69.63 所属国家: China 地区: Beijing 城市: Beijing  |
| appcashier.test.95516.com | IP: 180.95.171.99 所属国家: China 地区: Gansu 城市: Jinchang  |
| rs-na0.qbox.me | IP: 116.196.140.66 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| mobile.unionpay.com | 没有服务器地理信息.  |
| rsf-as0.qbox.me | IP: 116.196.140.63 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| iovip-na0.qbox.me | IP: 148.153.188.136 所属国家: United States of America 地区: Texas 城市: Dallas  |
| restapi.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h5.m.taobao.com | IP: 221.194.162.215 所属国家: China 地区: Hebei 城市: Langfang  |
| sms.qiniuapi.com | IP: 121.52.255.244 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| mclient.alipay.com | IP: 116.142.245.227 所属国家: China 地区: Beijing 城市: Beijing  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| www.tensorflow.org | IP: 142.250.73.142 所属国家: United States of America 地区: California 城市: Mountain View  |
| cgi.connect.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| free-qvm-z1-zz.qiniup.com | IP: 121.29.19.112 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| upload-na0.qiniup.com | IP: 116.196.140.63 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| up.qiniu.com | IP: 153.99.246.140 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| 4.ipw.cn | IP: 43.161.219.160 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| up.qiniup.com | IP: 112.82.212.151 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| upload-as0.qiniup.com | IP: 154.41.93.9 所属国家: Canada 地区: Quebec 城市: Montreal  |
| pu.qbox.me | IP: 153.99.246.133 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| rsf-z1.qiniu.com | IP: 110.242.48.33 所属国家: China 地区: Hebei 城市: Baoding  |
| 182.92.20.189 | IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing  |
| up-na0.qiniup.com | IP: 148.153.188.137 所属国家: United States of America 地区: Texas 城市: Dallas  |
| vod2.qcloud.com | IP: 111.206.147.172 所属国家: China 地区: Beijing 城市: Beijing  |
| wappaygw.alipay.com | IP: 116.142.245.205 所属国家: China 地区: Beijing 城市: Beijing  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mcgw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| rs-z1.qbox.me | IP: 121.29.19.114 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| picsum.photos | IP: 172.67.74.163 所属国家: United States of America 地区: California 城市: San Francisco  |
| rs-na0.qiniu.com | IP: 116.196.140.64 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| upload.qiniup.com | IP: 153.99.246.142 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| res.openinstall.com | IP: 8.137.76.62 所属国家: China 地区: Sichuan 城市: Chengdu  |
| api-z1.qiniu.com | IP: 110.242.48.33 所属国家: China 地区: Hebei 城市: Baoding  |
| rs-z1.qiniu.com | IP: 110.242.48.33 所属国家: China 地区: Hebei 城市: Baoding  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| wb.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| rsf-z1.qbox.me | IP: 121.29.19.114 所属国家: China 地区: Hebei 城市: Shijiazhuang  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://tsis.jpush.cn  | cn/jiguang/ad/i.java  |
| http://182.92.20.189:9099/  | cn/jiguang/o/c.java  |
| https://bjuser.jpush.cn/v1/appawake/status  | cn/jiguang/aa/b.java  |
| https://authsdk.tillusory.com/app/v1/auth/init  | cn/tillusory/sdk/net/a.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://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/cons/a.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | 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://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/packet/impl/c.java  |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&  | com/alipay/sdk/data/a.java  |
| https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\  | com/alipay/test/a.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/services/a/dd.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/services/a/bh.java  |
| http://restapi.amap.com/v3  | com/amap/api/services/a/i.java  |
| https://restapi.amap.com/v3  | com/amap/api/services/a/i.java  |
| http://restapi.amap.com/v4  | com/amap/api/services/a/i.java  |
| https://restapi.amap.com/v4  | com/amap/api/services/a/i.java  |
| http://yuntuapi.amap.com  | com/amap/api/services/a/i.java  |
| https://yuntuapi.amap.com  | com/amap/api/services/a/i.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/services/a/i.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/services/a/i.java  |
| http://restapi.amap.com  | com/amap/api/services/a/bn.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/amap/api/services/a/bg.java  |
| http://restapi.amap.com/v3/iasdkauth  | com/amap/api/services/a/bg.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/services/a/ba.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/services/a/ba.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/services/a/ba.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/services/a/ba.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/bl.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/di.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/di.java  |
| http://restapi.amap.com  | com/loc/t.java  |
| http://restapi.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restapi.amap.com/v3/config/district?  | com/loc/a.java  |
| http://restapi.amap.com/v3/place/around?  | com/loc/a.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/dn.java  |
| http://restapi.amap.com/v3/geocode/regeo  | com/loc/dd.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/db.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/loc/m.java  |
| http://restapi.amap.com/v3/iasdkauth  | com/loc/m.java  |
| https://api-cn.faceplusplus.com/sdk/v3/auth  | com/meihu/beautylibrary/utils/h.java  |
| https://api-us.faceplusplus.com/sdk/v3/auth  | com/meihu/beautylibrary/utils/h.java  |
| https://github.com/yyued/SVGAPlayer-Android  | com/opensource/svgaplayer/SVGAParser.java  |
| http://guoek.sevenghosts.cn/app/  | com/pro/gnewp/BuildConfig.java  |
| https://www.bt.cn/Api/getIpAddress  | com/pro/gnewp/net/AudioVideoRequester.java  |
| https://vodreport.qcloud.com/ugcupload  | com/pro/gnewp/videoupload/impl/UGCReport.java  |
| https://vod2.qcloud.com/v3/index.php?Action=  | com/pro/gnewp/videoupload/impl/UGCClient.java  |
| http://guoek.sevenghosts.cn/app/app/  | com/pro/gnewp/constant/ChatApi.java  |
| http://guoek.sevenghosts.cn/app/share/  | com/pro/gnewp/constant/ChatApi.java  |
| http://www.1-liao.com  | com/pro/gnewp/constant/ChatApi.java  |
| https://www.bt.cn/Api/getIpAddress  | com/pro/gnewp/constant/ChatApi.java  |
| https://4.ipw.cn/api/ip/myip?json  | com/pro/gnewp/constant/ChatApi.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token  | com/pro/gnewp/constant/ChatApi.java  |
| https://api.weixin.qq.com/sns/userinfo  | com/pro/gnewp/constant/ChatApi.java  |
| http://qyspare.chatchat.vip/app/getProtectAppVersion.html  | com/pro/gnewp/constant/ChatApi.java  |
| https://tb.53kf.com/code/client/10188492/1?device=android  | com/pro/gnewp/activity/KeFuWebViewActivity.java  |
| https://sandcash.mixienet.com.cn/h5/?  | com/pay/paytypelibrary/PayUtil.java  |
| http://linking.qiniuapi.com  | com/qiniu/linking/LinkingVodManager.java  |
| http://linking.qiniuapi.com  | com/qiniu/linking/LinkingDeviceManager.java  |
| https://uc.qbox.me  | com/qiniu/storage/Region.java  |
| http://api-%s.qiniu.com/sisyphus/fetch?id=%s  | com/qiniu/storage/BucketManager.java  |
| http://pu.qbox.me:10200  | com/qiniu/storage/BucketManager.java  |
| http://%s/%s/%s.m3u8  | com/qiniu/streaming/UrlFactory.java  |
| http://%s/%s/%s.flv  | com/qiniu/streaming/UrlFactory.java  |
| http://%s/%s/%s.jpg  | com/qiniu/streaming/UrlFactory.java  |
| http://pili.qiniuapi.com  | com/qiniu/streaming/StreamingManager.java  |
| http://qvs.qiniuapi.com  | com/qiniu/qvs/TemplateManager.java  |
| http://qvs.qiniuapi.com  | com/qiniu/qvs/NameSpaceManager.java  |
| http://qvs.qiniuapi.com  | com/qiniu/qvs/StreamManager.java  |
| https://pipeline.qiniu.com  | com/qiniu/bigdata/Configuration.java  |
| http://rtc.qiniuapi.com  | com/qiniu/rtc/RtcAppManager.java  |
| http://rtc.qiniuapi.com  | com/qiniu/rtc/RtcRoomManager.java  |
| http://fusion.qiniuapi.com  | com/qiniu/cdn/CdnManager.java  |
| https://sms.qiniuapi.com  | com/qiniu/sms/Configuration.java  |
| https://uc.qbox.me  | com/qiniu/common/AutoZone.java  |
| http://up.qiniu.com  | com/qiniu/common/AutoZone.java  |
| http://up-z1.qiniu.com  | com/qiniu/common/AutoZone.java  |
| http://up-z2.qiniu.com  | com/qiniu/common/AutoZone.java  |
| http://up-na0.qiniu.com  | com/qiniu/common/AutoZone.java  |
| http://up-as0.qiniu.com  | com/qiniu/common/AutoZone.java  |
| http://rs.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rs.qbox.me  | com/qiniu/common/Zone.java  |
| http://rsf.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rsf.qbox.me  | com/qiniu/common/Zone.java  |
| http://api.qiniu.com  | com/qiniu/common/Zone.java  |
| https://api.qiniu.com  | com/qiniu/common/Zone.java  |
| http://upload.qiniup.com  | com/qiniu/common/Zone.java  |
| https://upload.qiniup.com  | com/qiniu/common/Zone.java  |
| http://up.qiniup.com  | com/qiniu/common/Zone.java  |
| https://up.qiniup.com  | com/qiniu/common/Zone.java  |
| http://iovip.qbox.me  | com/qiniu/common/Zone.java  |
| https://iovip.qbox.me  | com/qiniu/common/Zone.java  |
| http://free-qvm-z0-xs.qiniup.com  | com/qiniu/common/Zone.java  |
| https://free-qvm-z0-xs.qiniup.com  | com/qiniu/common/Zone.java  |
| http://upload-z1.qiniup.com  | com/qiniu/common/Zone.java  |
| https://upload-z1.qiniup.com  | com/qiniu/common/Zone.java  |
| http://up-z1.qiniup.com  | com/qiniu/common/Zone.java  |
| https://up-z1.qiniup.com  | com/qiniu/common/Zone.java  |
| http://iovip-z1.qbox.me  | com/qiniu/common/Zone.java  |
| https://iovip-z1.qbox.me  | com/qiniu/common/Zone.java  |
| http://rs-z1.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rs-z1.qbox.me  | com/qiniu/common/Zone.java  |
| http://rsf-z1.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rsf-z1.qbox.me  | com/qiniu/common/Zone.java  |
| http://api-z1.qiniu.com  | com/qiniu/common/Zone.java  |
| https://api-z1.qiniu.com  | com/qiniu/common/Zone.java  |
| http://free-qvm-z1-zz.qiniup.com  | com/qiniu/common/Zone.java  |
| https://free-qvm-z1-zz.qiniup.com  | com/qiniu/common/Zone.java  |
| http://upload-z2.qiniup.com  | com/qiniu/common/Zone.java  |
| https://upload-z2.qiniup.com  | com/qiniu/common/Zone.java  |
| http://up-z2.qiniup.com  | com/qiniu/common/Zone.java  |
| https://up-z2.qiniup.com  | com/qiniu/common/Zone.java  |
| http://iovip-z2.qbox.me  | com/qiniu/common/Zone.java  |
| https://iovip-z2.qbox.me  | com/qiniu/common/Zone.java  |
| http://rs-z2.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rs-z2.qbox.me  | com/qiniu/common/Zone.java  |
| http://rsf-z2.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rsf-z2.qbox.me  | com/qiniu/common/Zone.java  |
| http://api-z2.qiniu.com  | com/qiniu/common/Zone.java  |
| https://api-z2.qiniu.com  | com/qiniu/common/Zone.java  |
| http://upload-na0.qiniup.com  | com/qiniu/common/Zone.java  |
| https://upload-na0.qiniup.com  | com/qiniu/common/Zone.java  |
| http://up-na0.qiniup.com  | com/qiniu/common/Zone.java  |
| https://up-na0.qiniup.com  | com/qiniu/common/Zone.java  |
| http://iovip-na0.qbox.me  | com/qiniu/common/Zone.java  |
| https://iovip-na0.qbox.me  | com/qiniu/common/Zone.java  |
| http://rs-na0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rs-na0.qbox.me  | com/qiniu/common/Zone.java  |
| http://rsf-na0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rsf-na0.qbox.me  | com/qiniu/common/Zone.java  |
| http://api-na0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://api-na0.qiniu.com  | com/qiniu/common/Zone.java  |
| http://upload-as0.qiniup.com  | com/qiniu/common/Zone.java  |
| https://upload-as0.qiniup.com  | com/qiniu/common/Zone.java  |
| http://up-as0.qiniup.com  | com/qiniu/common/Zone.java  |
| https://up-as0.qiniup.com  | com/qiniu/common/Zone.java  |
| http://iovip-as0.qbox.me  | com/qiniu/common/Zone.java  |
| https://iovip-as0.qbox.me  | com/qiniu/common/Zone.java  |
| http://rs-as0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rs-as0.qbox.me  | com/qiniu/common/Zone.java  |
| http://rsf-as0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://rsf-as0.qbox.me  | com/qiniu/common/Zone.java  |
| http://api-as0.qiniu.com  | com/qiniu/common/Zone.java  |
| https://api-as0.qiniu.com  | com/qiniu/common/Zone.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  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.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/d.java  |
| http://qzs.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| http://qzs.qq.com  | com/tencent/open/SocialApiIml.java  |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/f.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/b/d.java  |
| https://picsum.photos/id/%d/200/200  | com/tencent/qcloud/tim/uikit/modules/group/info/GroupInfoLayout.java  |
| http://mta.qq.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://mta.oa.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/wxop/stat/common/StatConstants.java  |
| https://graph.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | com/tencent/connect/share/QQShare.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | com/tencent/connect/share/QzoneShare.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/b/a/a.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/b/a/e.java  |
| http://com.thoughtworks.xstream/sax/property/configured-xstream  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/source-object-list  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://xml.org/sax/features/namespaces  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/configured-xstream\  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/sax/property/source-object-list\  | com/thoughtworks/xstream/io/xml/SaxWriter.java  |
| http://com.thoughtworks.xstream/XStreamSource/feature  | com/thoughtworks/xstream/io/xml/TraxSource.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/UPPayAssistEx.java  |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin\  | com/unionpay/mobile/android/utils/c.java  |
| https://res.openinstall.com/%s.dnc  | io/openinstall/sdk/j.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| https://github.com/opencv/opencv/issues/16739  | lib/armeabi-v7a/libTiSDK.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libagora-crypto.so  |
| http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk-jni.so  |
| http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk-jni.so  |
| http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| http://s  | lib/armeabi-v7a/libagora-rtc-sdk.so  |
| https://appcashier256.95516.com/gateway/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/conf  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/conf  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/hft  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/hft  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/gateway/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://data.facegl.com/appapi/auth/index  | lib/armeabi-v7a/libfacegl.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libfacegl.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libfuai.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libfuai.so  |
| https://github.com/opencv/opencv/issues/16739  | lib/armeabi-v7a/libfuai.so  |
| https://github.com/opencv/opencv/issues/6293  | lib/armeabi-v7a/liblmktrack.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libnative.so  |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libqcOpenSSL.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libuptsmaddon.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libuptsmaddonmi.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| tt01@2x.png  | com/pro/gnewp/im/ConfigHelper.java  |
| null@null.xml  | com/thoughtworks/xstream/persistence/FilePersistenceStrategy.java  |
| ftp@example.com  | lib/armeabi-v7a/libfacegl.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | com/faceunity/wrapper/faceunity.java  |
| 15060355040  | com/unionpay/UPPayAssistEx.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **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=485200, ST=kih, L=ftygh, O=njkl, OU=drfcg, CN=uhjkhv 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-01 06:41:20+00:00 有效期至: 2050-05-26 06:41:20+00:00 发行人: C=485200, ST=kih, L=ftygh, O=njkl, OU=drfcg, CN=uhjkhv 序列号: 0x6c1e6d41 哈希算法: sha256 md5值: b91fc5fcd31870f54dd981a0997ccbbf sha1值: 31f46bff3a61999b0ddb2462150750f01bea5c65 sha256值: 5b0d00f5cea5c9c88b2fc702b117620fd643178ef36dbad5aceb0762d5ec7d51 sha512值: 24b62ac0be49957e7cc3866e5cfaab5fa172fdc75bf7aa71fc060c3ba936f752db0bf4d888168134810b9839e8b74651ad318cca8f009e5ea05fb9b77c5793a2 公钥算法: rsa 密钥长度: 2048 指纹: d1ade2e15575acc5bdf18efdeece0512804fee1b5f399f5a9b334f00f6a6faa9**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_password" : "账号密码登录"  |
| "active\_user" : "活跃用户:"  |
| "chat\_user" : "聊友:"  |
| "forget\_password" : "忘记密码?"  |
| "input\_password" : "输入密码"  |
| "need\_independent\_password" : "启动未成年模式,需要设置独立密码"  |
| "online\_user" : "当前在线用户: 5562次"  |
| "password" : "密 码:"  |
| "phone\_private" : "私密(不公开)"  |
| "please\_input\_active\_user" : "请输入您的活跃用户"  |
| "please\_input\_long\_password" : "密码长度不够"  |
| "please\_input\_password" : "请输入密码"  |
| "private\_agree" : "《隐私政策》"  |
| "private\_chat\_switch" : "私信聊天"  |
| "private\_detail" : "隐私政策"  |
| "private\_image" : "私密照片"  |
| "private\_video" : "私密视频"  |
| "swtich\_off\_alert\_private" : "关闭后你将收不到私聊消息"  |
| "token\_invalid" : "登录失效，请重新登录"  |
| "verify\_password" : "验证密码"  |
| "wrong\_password" : "密码不正确,请重新输入"  |

## **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.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.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.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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| com.pro.chat.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.pro.gnewp.permission.JPUSH\_MESSAGE | 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.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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.pro.gnewp.activity.SplashActivity | **Schemes**: jy02ck://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent://,  |

**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。**