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

**惜蕊（ 1.0.1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 | 惜蕊 |
| 版本 | 1.0.1 |
| 包名 | com.xiruichat.app |
| 域名线索 | 132条 |
| URL线索 | 97条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | xirui-202506071042.apk |
| 文件大小 | 73.63MB |
| MD5值 | 5049a2f743211fd4169969554f869e37 |
| SHA1值 | fd8089e4e864ff1b9ef0b7794a910c01fe452f66 |
| SHA256值 | c340993721b7e66dded80b7c580810534505d7915c468c1d018aabf1d6cd1e6f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 惜蕊 |
| 包名 | com.xiruichat.app |
| 主活动Activity | com.xiruichat.app.activity.LauncherActivity |
| 安卓版本名称 | 1.0.1 |
| 安卓版本 | 2025052701 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| secure.checkout.visa.com | IP: 104.19.208.81  所属国家: United States of America  地区: California  城市: San Francisco |
| im.sdk.qcloud.com | IP: 42.236.6.83  所属国家: China  地区: Henan  城市: Zhengzhou |
| pipeline.qiniu.com | 没有服务器地理信息. |
| mcgw.alipay.com | IP: 111.202.5.210  所属国家: China  地区: Beijing  城市: Beijing |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| checkout.paypal.com | IP: 151.101.90.133  所属国家: United States of America  地区: California  城市: San Francisco |
| rtt2b.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipay.com | IP: 203.209.243.98  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.mytoday.net | IP: 13.248.169.48  所属国家: United States of America  地区: Washington  城市: Seattle |
| api-m.sandbox.paypal.com | IP: 151.101.91.1  所属国家: United States of America  地区: California  城市: San Francisco |
| 43.129.43.42 | IP: 43.129.43.42  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| apis.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| cmnsguider.yunos.com | IP: 203.119.169.246  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 162.14.13.104 | IP: 162.14.13.104  所属国家: China  地区: Beijing  城市: Beijing |
| developers.google.com | IP: 142.250.107.101  所属国家: United States of America  地区: California  城市: Mountain View |
| appapi.kbeky.cn | 没有服务器地理信息. |
| developers.braintreepayments.com | IP: 151.101.89.21  所属国家: United States of America  地区: California  城市: San Francisco |
| 162.14.17.129 | IP: 162.14.17.129  所属国家: China  地区: Beijing  城市: Beijing |
| sdk-im-1252463788.file.myqcloud.com | IP: 119.188.150.187  所属国家: China  地区: Shandong  城市: Jinan |
| api.share.mob.com | IP: 180.188.25.40  所属国家: China  地区: Zhejiang  城市: Taizhou |
| uri.paypal.com | 没有服务器地理信息. |
| www.paypal.com | IP: 151.101.89.21  所属国家: United States of America  地区: California  城市: San Francisco |
| rtt2c.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| graph.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| mta.oa.com | IP: 141.144.196.217  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| ue.indoorloc.map.qq.com | IP: 116.130.223.156  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| notify.bugsnag.com | IP: 35.186.205.6  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| api.weixin.qq.com | IP: 116.128.184.169  所属国家: China  地区: Shanghai  城市: Shanghai |
| 162.14.3.250 | IP: 162.14.3.250  所属国家: China  地区: Beijing  城市: Beijing |
| www.facebook.com | IP: 31.13.88.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| s1.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| s2.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| sdk-im-1252463788.cos.ap-hongkong.myqcloud.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| upload.twitter.com | IP: 202.160.128.203  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 162.14.11.59 | IP: 162.14.11.59  所属国家: China  地区: Beijing  城市: Beijing |
| s3-us-west-1.amazonaws.com | IP: 52.219.121.32  所属国家: United States of America  地区: California  城市: San Jose |
| b.stats.paypal.com | IP: 34.84.160.32  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| rtt2a.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| assets.staging.braintreepayments.com | IP: 184.105.254.110  所属国家: United States of America  地区: California  城市: Fremont |
| appapi-1333632706.cos.ap-nanjing.myqcloud.com | IP: 112.80.252.190  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| p3.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| twitter.com | IP: 172.66.0.227  所属国家: United States of America  地区: California  城市: San Francisco |
| p1.map.gtimg.com | IP: 60.221.17.184  所属国家: China  地区: Shanxi  城市: Taiyuan |
| xmlpull.org | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| 162.14.10.42 | IP: 162.14.10.42  所属国家: China  地区: Beijing  城市: Beijing |
| api.utag.mob.com | 没有服务器地理信息. |
| c.paypal.com | IP: 151.101.89.21  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| api.braintreegateway.com | IP: 3.122.176.248  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| api.twitter.com | IP: 162.125.8.1  所属国家: United States of America  地区: California  城市: San Francisco |
| confinfo.map.qq.com | IP: 220.194.120.95  所属国家: China  地区: Tianjin  城市: Tianjin |
| uplog.qbox.me | IP: 101.251.144.177  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| c.sandbox.paypal.com | IP: 151.101.91.1  所属国家: United States of America  地区: California  城市: San Francisco |
| wappaygw.alipay.com | IP: 111.202.5.210  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 |
| up.mob.com | IP: 60.191.231.227  所属国家: China  地区: Zhejiang  城市: Jinhua |
| 162.14.13.181 | IP: 162.14.13.181  所属国家: China  地区: Beijing  城市: Beijing |
| mta.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| upload.qq163.iego.cn | 没有服务器地理信息. |
| m0.map.gtimg.com | IP: 221.204.15.91  所属国家: China  地区: Shanxi  城市: Taiyuan |
| pingma.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| license.vod-pro.com | IP: 123.6.105.16  所属国家: China  地区: Henan  城市: Zhengzhou |
| qzs.qq.com | IP: 60.221.17.184  所属国家: China  地区: Shanxi  城市: Taiyuan |
| www.mob.com | IP: 180.188.26.28  所属国家: China  地区: Zhejiang  城市: Taizhou |
| pr.map.qq.com | IP: 116.130.224.82  所属国家: China  地区: Beijing  城市: Beijing |
| open.weixin.qq.com | IP: 116.128.171.214  所属国家: China  地区: Shanghai  城市: Shanghai |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| api.sandbox.braintreegateway.com | IP: 159.242.242.128  所属国家: United States of America  地区: California  城市: San Jose |
| lark.alipay.com | IP: 110.76.22.106  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| sandbox.secure.checkout.visa.com | IP: 104.16.97.27  所属国家: United States of America  地区: California  城市: San Francisco |
| yun-hl.3g.qq.com | IP: 125.36.181.143  所属国家: China  地区: Tianjin  城市: Tianjin |
| acs.amazonaws.com | 没有服务器地理信息. |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| www.paypalobjects.com | IP: 151.101.91.1  所属国家: United States of America  地区: California  城市: San Francisco |
| 162.14.6.156 | IP: 162.14.6.156  所属国家: China  地区: Beijing  城市: Beijing |
| s3.amazonaws.com | IP: 52.216.218.8  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| s3.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| h5.m.taobao.com | IP: 125.39.155.58  所属国家: China  地区: Tianjin  城市: Tianjin |
| alogus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cc.map.qq.com | IP: 125.36.181.144  所属国家: China  地区: Tianjin  城市: Tianjin |
| m1.map.gtimg.com | IP: 221.204.15.61  所属国家: China  地区: Shanxi  城市: Taiyuan |
| 162.14.19.159 | IP: 162.14.19.159  所属国家: China  地区: Beijing  城市: Beijing |
| p0.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| developer.umeng.com | IP: 59.82.31.160  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 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 |
| l.mob.com | IP: 180.188.25.40  所属国家: China  地区: Zhejiang  城市: Taizhou |
| m3.map.gtimg.com | IP: 221.204.15.61  所属国家: China  地区: Shanxi  城市: Taiyuan |
| www.myapp.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| analytics.map.qq.com | IP: 125.36.181.143  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.u.mob.com | 没有服务器地理信息. |
| mclient.alipay.com | IP: 218.61.164.135  所属国家: China  地区: Liaoning  城市: Shenyang |
| up-hl.3g.qq.com | IP: 112.64.235.44  所属国家: China  地区: Shanghai  城市: Shanghai |
| play.google.com | IP: 93.46.8.90  所属国家: Italy  地区: Lombardia  城市: Milan |
| api-m.paypal.com | IP: 151.101.91.1  所属国家: United States of America  地区: California  城市: San Francisco |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Singapore  地区: Singapore  城市: Singapore |
| p2.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| 162.14.3.17 | IP: 162.14.3.17  所属国家: China  地区: Beijing  城市: Beijing |
| uc.qbox.me | IP: 153.99.246.133  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| alogsus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| www.ngs.ac.uk | IP: 130.246.140.235  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Appleton |
| ulogs.umengcloud.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| s0.map.gtimg.com | IP: 42.236.6.64  所属国家: China  地区: Henan  城市: Zhengzhou |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.android.com | 没有服务器地理信息. |
| app.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| 10.0.2.2 | IP: 10.0.2.2  所属国家: -  地区: -  城市: - |
| up.sdk.mob.com | IP: 180.188.26.28  所属国家: China  地区: Zhejiang  城市: Taizhou |
| 162.14.19.114 | IP: 162.14.19.114  所属国家: China  地区: Beijing  城市: Beijing |
| sdk-im-1252463788.cos.accelerate.myqcloud.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| 162.14.19.46 | IP: 162.14.19.46  所属国家: China  地区: Beijing  城市: Beijing |
| rtt2.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| graph.facebook.com | IP: 98.159.108.71  所属国家: United States of America  地区: California  城市: Los Angeles |
| paygate-yf.meituan.com | IP: 101.236.69.63  所属国家: China  地区: Beijing  城市: Beijing |
| d55f1fc5.ngrok.io | IP: 18.177.76.42  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| h.trace.qq.com | IP: 113.56.189.246  所属国家: China  地区: Hubei  城市: Huangshi |
| dnsrepo-pub.alibaba.com | IP: 106.11.43.250  所属国家: China  地区: Beijing  城市: Beijing |
| 162.14.13.203 | IP: 162.14.13.203  所属国家: China  地区: Beijing  城市: Beijing |
| m2.map.gtimg.com | IP: 123.6.42.84  所属国家: China  地区: Henan  城市: Zhengzhou |
| 162.14.13.170 | IP: 162.14.13.170  所属国家: China  地区: Beijing  城市: Beijing |
| 162.14.20.148 | IP: 162.14.20.148  所属国家: China  地区: Beijing  城市: Beijing |
| new-api.meiqia.com | IP: 114.117.133.42  所属国家: China  地区: Beijing  城市: Beijing |
| apikey.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| 43.129.34.169 | IP: 43.129.34.169  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| ulogs.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://cc.map.qq.com/?get\_c3 | c/t/m/g/dd.java |
| https://up-hl.3g.qq.com/upreport | c/t/m/g/am.java |
| http://analytics.map.qq.com/?sf | c/t/m/g/ck.java |
| https://yun-hl.3g.qq.com/halleycloud | c/t/m/g/bt.java |
| http://ue.indoorloc.map.qq.com/?wl | c/t/m/g/dv.java |
| http://ue.indoorloc.map.qq.com/ | c/t/m/g/dv.java |
| http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile | cn/sharesdk/tencent/qq/a.java |
| http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk | cn/sharesdk/tencent/qq/a.java |
| http://www.myapp.com/down/ | cn/sharesdk/tencent/qq/f.java |
| https://graph.qq.com/oauth2.0/me | cn/sharesdk/tencent/qq/c.java |
| https://graph.qq.com/oauth2.0/m\_authorize?response\_type=token&client\_id= | cn/sharesdk/tencent/qq/c.java |
| https://graph.qq.com/user/get\_simple\_userinfo | cn/sharesdk/tencent/qq/c.java |
| http://openmobile.qq.com/api/check? | cn/sharesdk/tencent/qq/c.java |
| https://graph.qq.com | cn/sharesdk/tencent/qq/c.java |
| https://graph.qq.com/oauth2.0/m\_authorize?response\_type=token&client\_id= | cn/sharesdk/tencent/qzone/b.java |
| https://graph.qq.com/oauth2.0/me | cn/sharesdk/tencent/qzone/b.java |
| https://graph.qq.com/user/get\_simple\_userinfo | cn/sharesdk/tencent/qzone/b.java |
| https://graph.qq.com/photo/upload\_pic | cn/sharesdk/tencent/qzone/b.java |
| https://graph.qq.com | cn/sharesdk/tencent/qzone/b.java |
| https://api.twitter.com/oauth/request\_token | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/oauth/authorize?oauth\_token= | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/oauth/access\_token | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/1.1/users/show.json | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/1.1/friends/list.json | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/1.1/followers/list.json | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/1.1/statuses/update.json | cn/sharesdk/twitter/c.java |
| https://upload.twitter.com/1.1/media/upload.json | cn/sharesdk/twitter/c.java |
| https://api.twitter.com/1.1/statuses/update\_with\_media.json | cn/sharesdk/twitter/c.java |
| https://twitter.com/ | cn/sharesdk/twitter/Twitter.java |
| https://api.weixin.qq.com/sns/oauth2/access\_token | cn/sharesdk/wechat/utils/g.java |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token | cn/sharesdk/wechat/utils/g.java |
| https://api.weixin.qq.com/sns/userinfo | cn/sharesdk/wechat/utils/g.java |
| http://api.share.mob.com:80 | cn/sharesdk/framework/b/c.java |
| http://up.mob.com/upload/image | cn/sharesdk/framework/b/c.java |
| http://l.mob.com/url/shareSdkEncryptMapping.do | cn/sharesdk/framework/b/c.java |
| https://) | cn/sharesdk/framework/b/a.java |
| https://www.facebook.com/dialog/oauth? | cn/sharesdk/facebook/d.java |
| https://www.facebook.com/dialog/feed? | cn/sharesdk/facebook/d.java |
| https://graph.facebook.com/v2.8/me/feed | cn/sharesdk/facebook/d.java |
| https://graph.facebook.com/v2.8/me/photos | cn/sharesdk/facebook/d.java |
| https://graph.facebook.com/v2.8 | cn/sharesdk/facebook/d.java |
| https://graph.facebook.com/v2.8/ | cn/sharesdk/facebook/d.java |
| https://s3-us-west-1.amazonaws.com | com/amazonaws/services/s3/AmazonS3Client.java |
| http://10.0.2.2:20005 | com/amazonaws/services/s3/internal/Constants.java |
| http://s3.amazonaws.com/doc/2006-03-01/ | com/amazonaws/services/s3/internal/Constants.java |
| http://www.ngs.ac.uk/tools/jcepolicyfiles | com/amazonaws/services/s3/internal/crypto/EncryptionUtils.java |
| http://acs.amazonaws.com/groups/global/AllUsers | com/amazonaws/services/s3/model/GroupGrantee.java |
| http://acs.amazonaws.com/groups/global/AuthenticatedUsers | com/amazonaws/services/s3/model/GroupGrantee.java |
| http://acs.amazonaws.com/groups/s3/LogDelivery | com/amazonaws/services/s3/model/GroupGrantee.java |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermData | com/alibaba/pdns/g.java |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData | com/alibaba/pdns/g.java |
| http://10.0.2.2:3000/ | com/braintreepayments/api/BuildConfig.java |
| https://play.google.com/store/apps/details?id=com.venmo | com/braintreepayments/api/Venmo.java |
| https://secure.checkout.visa.com | com/braintreepayments/api/VisaCheckout.java |
| https://sandbox.secure.checkout.visa.com | com/braintreepayments/api/VisaCheckout.java |
| https://developers.google.com/android/reference/com/google/android/gms/wallet/WalletConstants | com/braintreepayments/api/AndroidPay.java |
| https://developers.braintreepayments.com/guides/client-sdk/android/v2 | com/braintreepayments/api/PayPal.java |
| https://api.sandbox.braintreegateway.com/ | com/braintreepayments/api/models/TokenizationKey.java |
| https://api.braintreegateway.com/ | com/braintreepayments/api/models/TokenizationKey.java |
| https://github.com/braintree/browser-switch-android | com/braintreepayments/browserswitch/BrowserSwitchFragment.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.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://mcgw.alipay.com/sdklog.do | com/alipay/sdk/packet/impl/c.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 |
| 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://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| https://new-api.meiqia.com/client/send\_msg | com/meiqia/core/d.java |
| https://new-api.meiqia.com/client/send\_msg | com/meiqia/core/h.java |
| https://new-api.meiqia.com/knowledge/questions/ | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/file\_downloaded | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/tickets\_v2/ | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/msg\_delivered | com/meiqia/core/h.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass\_message\_receipts | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/end\_conversation | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/queue/position | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/tickets\_v2/categories | com/meiqia/core/h.java |
| https://new-api.meiqia.com/upload?user\_id= | com/meiqia/core/h.java |
| https://new-api.meiqia.com/upload/oss/policies | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/inputting | com/meiqia/core/h.java |
| https://new-api.meiqia.com/conversation/ | com/meiqia/core/h.java |
| https://new-api.meiqia.com/sdk/init\_sdk\_user | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/device\_token | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/prechat-survey-msg | com/meiqia/core/h.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/unreceived\_mass\_messages | com/meiqia/core/h.java |
| https://new-api.meiqia.com/sdk/statistics | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/forms | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/attrs | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/ | com/meiqia/core/h.java |
| https://new-api.meiqia.com/scheduler | com/meiqia/core/h.java |
| https://new-api.meiqia.com/sdk/init | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/tickets\_v2 | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/tickets | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/msg\_read | com/meiqia/core/h.java |
| https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass\_messages/ | com/meiqia/core/h.java |
| https://new-api.meiqia.com/sdk/get\_dev\_client\_id | com/meiqia/core/h.java |
| https://new-api.meiqia.com/sdk/refresh\_push\_info | com/meiqia/core/h.java |
| https://new-api.meiqia.com/client/client\_events | com/meiqia/core/h.java |
| https://new-api.meiqia.com/mpush/copy/statistics | com/meiqia/core/h.java |
| https://notify.bugsnag.com | com/meiqia/core/a/e.java |
| http://meiqia.com/ | com/meiqia/core/a/e.java |
| https://new-api.meiqia.com/captchas | com/meiqia/meiqiasdk/util/HttpUtils.java |
| https://new-api.meiqia.com | com/meiqia/meiqiasdk/util/HttpUtils.java |
| http://api.u.mob.com | com/mob/MobUser.java |
| http://api.utag.mob.com/conf | com/mob/commons/utag/TagRequester.java |
| http://api.utag.mob.com/bdata | com/mob/commons/utag/UserTager.java |
| http://[host]:[port] | com/mob/commons/clt/MphClt.java |
| http://d55f1fc5.ngrok.io | com/mob/commons/clt/MphClt.java |
| http://up.sdk.mob.com | com/mob/commons/filesys/FileUploader.java |
| https://github.com/yyued/SVGAPlayer-Android | com/opensource/svgaplayer/SVGAParser.java |
| https://uri.paypal.com/services/payments/futurepayments\ | com/paypal/android/sdk/onetouch/core/BuildConfig.java |
| https://checkout.paypal.com/one-touch-login/\ | com/paypal/android/sdk/onetouch/core/BuildConfig.java |
| https://assets.staging.braintreepayments.com/one-touch-login/\ | com/paypal/android/sdk/onetouch/core/BuildConfig.java |
| https://www.paypal.com | com/paypal/android/sdk/onetouch/core/AuthorizationRequest.java |
| https://www.paypalobjects.com/webstatic/otc/otc-config.android.json | com/paypal/android/sdk/onetouch/core/config/ConfigManager.java |
| https://api-m.paypal.com/v1/ | com/paypal/android/sdk/onetouch/core/network/EnvironmentManager.java |
| https://api-m.sandbox.paypal.com/v1/ | com/paypal/android/sdk/onetouch/core/network/EnvironmentManager.java |
| https://uri.paypal.com/services/payments/futurepayments | com/paypal/android/sdk/onetouch/core/sdk/PayPalScope.java |
| https://uri.paypal.com/services/paypalattributes | com/paypal/android/sdk/onetouch/core/sdk/PayPalScope.java |
| http://%s | com/qiniu/android/common/Zone.java |
| https://uc.qbox.me | com/qiniu/android/common/AutoZone.java |
| http://uc.qbox.me | com/qiniu/android/common/AutoZone.java |
| https://uplog.qbox.me/log/3 | com/qiniu/android/collect/Config.java |
| https://pipeline.qiniu.com | com/qiniu/android/bigdata/Configuration.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 |
| 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://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.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://im.sdk.qcloud.com/download/plus/8.5.6864/ | com/tencent/imsdk/manager/LibraryDownloader.java |
| https://sdk-im-1252463788.cos.accelerate.myqcloud.com/download/plus/8.5.6864/ | com/tencent/imsdk/manager/LibraryDownloader.java |
| https://sdk-im-1252463788.file.myqcloud.com/download/plus/8.5.6864/ | com/tencent/imsdk/manager/LibraryDownloader.java |
| https://sdk-im-1252463788.cos.ap-hongkong.myqcloud.com/download/plus/8.5.6864/ | com/tencent/imsdk/manager/LibraryDownloader.java |
| https://confinfo.map.qq.com/confinfo?apikey= | com/tencent/mapsdk/rastercore/d.java |
| https://apikey.map.qq.com/mkey/index.php/mkey/check? | com/tencent/mapsdk/rastercore/a.java |
| https://rtt2.map.qq.com | com/tencent/mapsdk/rastercore/tile/b/f.java |
| https://rtt2a.map.qq.com | com/tencent/mapsdk/rastercore/tile/b/f.java |
| https://rtt2b.map.qq.com | com/tencent/mapsdk/rastercore/tile/b/f.java |
| https://rtt2c.map.qq.com | com/tencent/mapsdk/rastercore/tile/b/f.java |
| https://p0.map.gtimg.com/sateTiles | com/tencent/mapsdk/rastercore/tile/b/d.java |
| https://p1.map.gtimg.com/sateTiles | com/tencent/mapsdk/rastercore/tile/b/d.java |
| https://p2.map.gtimg.com/sateTiles | com/tencent/mapsdk/rastercore/tile/b/d.java |
| https://p3.map.gtimg.com/sateTiles | com/tencent/mapsdk/rastercore/tile/b/d.java |
| https://m0.map.gtimg.com/hwap | com/tencent/mapsdk/rastercore/tile/b/e.java |
| https://m1.map.gtimg.com/hwap | com/tencent/mapsdk/rastercore/tile/b/e.java |
| https://m2.map.gtimg.com/hwap | com/tencent/mapsdk/rastercore/tile/b/e.java |
| https://m3.map.gtimg.com/hwap | com/tencent/mapsdk/rastercore/tile/b/e.java |
| https://s0.map.gtimg.com/oversea | com/tencent/mapsdk/rastercore/tile/b/b.java |
| https://s1.map.gtimg.com/oversea | com/tencent/mapsdk/rastercore/tile/b/b.java |
| https://s2.map.gtimg.com/oversea | com/tencent/mapsdk/rastercore/tile/b/b.java |
| https://s3.map.gtimg.com/oversea | com/tencent/mapsdk/rastercore/tile/b/b.java |
| https://pr.map.qq.com/pingd? | com/tencent/mapsdk/rastercore/d/e.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://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 |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://ulogs.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com/unify\_logs | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://lark.alipay.com/yj131525/byt0wl/ufnf3i | com/umeng/commonsdk/statistics/internal/c.java |
| https://cmnsguider.yunos.com:443/genDeviceToken | com/umeng/commonsdk/statistics/idtracking/s.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://developer.umeng.com/docs/66632/detail/70018?um\_channel=sdk | com/umeng/analytics/b.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/h.java |
| https://apis.map.qq.com/ws/geocoder/v1/ | com/yunbao/common/http/CommonHttpUtil.java |
| https://apis.map.qq.com/ws/place/v1/search | com/yunbao/common/http/CommonHttpUtil.java |
| https://graph.qq.com/oauth2.0/me?access\_token= | com/yunbao/common/http/CommonHttpUtil.java |
| http://upload.qq163.iego.cn:8088/cam | com/yunbao/common/http/CommonHttpUtil.java |
| http://www.mytoday.net/api/public/?service=Video.uploadvideo | com/yunbao/common/upload/UploadFtpImpl.java |
| https://apis.map.qq.com/ws/staticmap/v2/?center= | com/yunbao/im/adapter/ImRoomAdapter.java |
| https://apis.map.qq.com/ws/staticmap/v2/?center= | com/yunbao/im/adapter/ImRoomTempAdapter.java |
| http://upload.qq163.iego.cn:8088/cam | com/yunbao/video/http/VideoHttpUtil.java |
| https://license.vod-pro.com/license/v2/1333632706\_1/v\_cube.license | com/xiruichat/app/AppContext.java |
| https://appapi-1333632706.cos.ap-nanjing.myqcloud.com/android.txt | com/xiruichat/app/activity/LauncherActivity.java |
| https://appapi-1333632706.cos.ap-nanjing.myqcloud.com/configan.txt | com/xiruichat/app/activity/LauncherActivity.java |
| https://appapi.kbeky.cn/ | com/xiruichat/app/activity/LauncherActivity.java |
| https://b.stats.paypal.com/counter.cgi | lib/android/paypal/com/magnessdk/a.java |
| https://c.paypal.com/r/v1/device/client-metadata | lib/android/paypal/com/magnessdk/a.java |
| https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes\_config\_android\_v4.json | lib/android/paypal/com/magnessdk/a.java |
| https://c.sandbox.paypal.com/r/v1/device/client-metadata | lib/android/paypal/com/magnessdk/a.java |
| https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes\_config\_android\_v4.json | lib/android/paypal/com/magnessdk/e.java |
| https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes\_config\_android\_v4.json | lib/android/paypal/com/magnessdk/network/c.java |
| https://c.paypal.com/r/v1/device/client-metadata | lib/android/paypal/com/magnessdk/network/c.java |
| https://c.sandbox.paypal.com/r/v1/device/client-metadata | lib/android/paypal/com/magnessdk/network/c.java |
| https://b.stats.paypal.com/counter.cgi | lib/android/paypal/com/magnessdk/network/c.java |
| https://c.paypal.com/r/v1/device/client-metadata | lib/android/paypal/com/magnessdk/network/i.java |
| https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes\_config\_android\_v4.json | lib/android/paypal/com/magnessdk/network/i.java |
| https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes\_config\_android\_v4.json | lib/android/paypal/com/magnessdk/network/j.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| https://github.com/vinc3m1 | 摸瓜V1引擎 |
| https://github.com/vinc3m1/RoundedImageView | 摸瓜V1引擎 |
| https://github.com/vinc3m1/RoundedImageView.git | 摸瓜V1引擎 |
| http://www.mob.com | 摸瓜V1引擎 |
| https://43.129.34.169/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.19.159/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.11.59/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.17.129/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.20.148/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.3.17/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.6.156/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.19.46/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.13.104/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://43.129.43.42/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.10.42/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.13.181/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://162.14.13.170/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| http://162.14.3.250/v4/ConfigGetSvc/GetOpenSSOIPList | lib/arm64-v8a/libImSDK.so |
| https://43.129.34.169/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.19.159/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.3.17/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.19.46/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.13.104/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.13.203/netcheck | lib/arm64-v8a/libImSDK.so |
| https://162.14.10.42/netcheck | lib/arm64-v8a/libImSDK.so |
| http://162.14.19.114/ | lib/arm64-v8a/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 |
| jrs@cs.berkeley | lib/arm64-v8a/libCNamaSDK.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222 | com/mob/commons/clt/DClt.java |
| 16222222222 | com/mob/commons/clt/DClt.java |
| 17222222222 | com/mob/commons/clt/DClt.java |
| 18222222222 | com/mob/commons/clt/DClt.java |
| 19222222222 | com/mob/commons/clt/DClt.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: CN=df, OU=df, O=ddf, L=beijing, ST=beijing, C=86 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-26 13:58:38+00:00 有效期至: 2050-03-20 13:58:38+00:00 发行人: CN=df, OU=df, O=ddf, L=beijing, ST=beijing, C=86 序列号: 0x1 哈希算法: sha256 md5值: c379bdc60e13266dcabfcb4e2db5a771 sha1值: 86b5bac2f6c1a906990d72fd5903b014624cc147 sha256值: c304d93cf396aff176b8c81b8d00d77f8c56623b9f746c5d7b33475ed685c82f sha512值: 8e8d38882c63db21374c497e3a3e10d0b5201b1b9494a1dc215052ef9ac0cdc09617780ec6e41aaab29269dbc90929a6073829562a5b5073ba0c01bcfdf73e30 公钥算法: rsa 密钥长度: 2048 指纹: 8481c01d53bfcc982a6cc461a77f5b992dbabd51b96f2229367b37cba520def6**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "auth\_my\_auth" : "我要认证" |
| "cash\_input\_bank\_user\_name" : "请输入持卡人姓名" |
| "chat\_gift\_user\_not\_auth" : "对方未认证" |
| "choose\_user" : "请选择用户" |
| "find\_pwd\_find" : "立即找回" |
| "find\_pwd\_forget" : "忘记密码" |
| "go\_auth" : "去认证" |
| "have\_auth" : "已认证" |
| "home\_user" : "用户" |
| "library\_roundedimageview\_author" : "Vince Mi" |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1" |
| "live\_input\_password" : "请输入房间密码" |
| "live\_set\_pwd" : "请设置房间密码" |
| "login\_auth\_cancle" : "授权取消" |
| "login\_auth\_failure" : "授权失败" |
| "login\_auth\_ing" : "正在授权登录" |
| "login\_auth\_success" : "登录成功" |
| "login\_forget\_pwd" : "忘记密码" |
| "match\_one\_key" : "一键匹配" |
| "mq\_auth\_code" : "验证码" |
| "not\_auth" : "未认证" |
| "rank\_auth\_tip" : "该用户还未认证~" |
| "reg\_input\_pwd\_1" : "请填写密码" |
| "reg\_input\_pwd\_2" : "请确认密码" |
| "search\_user\_name" : "搜索用户昵称" |
| "ssdk\_cmcc\_auth" : "手机认证服务由中国移动提供" |
| "ssdk\_cmcc\_login\_one\_key" : "本机号码一键登录" |
| "ssdk\_instapaper\_pwd" : "密码" |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权" |
| "video\_comment\_author" : "作者" |
| "mq\_auth\_code" : "CAPTCHA" |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile" |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login" |
| "ssdk\_instapaper\_pwd" : "Password" |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization" |
| "mq\_auth\_code" : "Kode verifikaso" |
| "mq\_auth\_code" : "Kod pengesahan" |
| "mq\_auth\_code" : "驗證碼" |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.NETWORK\_PROVIDER | 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| android.permission.RECEIVE\_USER\_PRESENT | 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.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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.braintreepayments.api.BraintreeBrowserSwitchActivity | **Schemes**: com.yunbao.shortvideo.braintree://, |
| cn.sharesdk.tencent.qq.ReceiveActivity | **Schemes**: tencent101577656://, |

**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。**