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

**夜色交友（ 4.2.0版本）   
APK分析报告**

## **1. 分析结果概述**

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

| 类别 | 内容 |
| --- | --- |
| APP名称 | 夜色交友 |
| 版本 | 4.2.0 |
| 包名 | com.huahua.dating |
| 域名线索 | 78条 |
| URL线索 | 44条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | -交.apk |
| 文件大小 | 63.41MB |
| MD5值 | 0dbe6f82a75e347137c46a7dfeff61ba |
| SHA1值 | c321b6820f4e9617a63e8a8dd3180a06f0e3631c |
| SHA256值 | 55b13caacead509793d030ab980f38291c1aea5bc621c7cb6085366a281d2882 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 夜色交友 |
| 包名 | com.huahua.dating |
| 主活动Activity | com.huahua.dating.ui.view.activity.SplashActivity |
| 安卓版本名称 | 4.2.0 |
| 安卓版本 | 420 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| play.google.com | IP: 59.24.3.174  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| developer.umeng.com | IP: 59.82.29.248  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| fusion.qq.com | IP: 116.130.229.204  所属国家: China  地区: Beijing  城市: Beijing |
| register.xmpush.global.xiaomi.com | IP: 47.237.96.1  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| metrics1.data.hicloud.com | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| openmobile.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| cgi.qplus.com | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| aaid.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pipeline.qiniu.com | 没有服务器地理信息. |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| mclient.alipay.com | IP: 1.190.42.122  所属国家: China  地区: Heilongjiang  城市: Harbin |
| norma-external-collect.meizu.com | 没有服务器地理信息. |
| www.google.com | IP: 31.13.68.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| store.hispace.hicloud.com | IP: 49.4.47.241  所属国家: China  地区: Guangdong  城市: Guangzhou |
| onepass.geetest.com | IP: 103.143.17.142  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| ulogs.umengcloud.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 223.6.6.6 | IP: 223.6.6.6  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.xmpush.xiaomi.com | IP: 123.125.102.209  所属国家: China  地区: Beijing  城市: Beijing |
| alogsus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| auth.wosms.cn | IP: 124.64.196.28  所属国家: China  地区: Beijing  城市: Beijing |
| resolver.msg.xiaomi.net | IP: 110.43.0.169  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| exoplayer.dev | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| stackoverflow.com | IP: 172.64.155.249  所属国家: United States of America  地区: California  城市: San Francisco |
| opencloud.wostore.cn | IP: 210.22.123.92  所属国家: China  地区: Shanghai  城市: Shanghai |
| login.imgcache.qq.com | IP: 124.166.237.88  所属国家: China  地区: Shanxi  城市: Taiyuan |
| playready.directtaps.net | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| daily.m.zzx9.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com | IP: 84.201.210.37  所属国家: Poland  地区: Lubelskie  城市: Lublin |
| h.trace.qq.com | IP: 113.56.189.246  所属国家: China  地区: Hubei  城市: Huangshi |
| es5.github.io | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.qiniu.com | IP: 175.17.21.215  所属国家: China  地区: Jilin  城市: Changchun |
| www.computerhope.com | IP: 172.67.0.39  所属国家: United States of America  地区: California  城市: San Francisco |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| mobilegw.alipay.com | IP: 203.209.255.238  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| dashif.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| 8.8.8.8 | IP: 8.8.8.8  所属国家: United States of America  地区: California  城市: Mountain View |
| plbslog.umeng.com | IP: 36.156.202.75  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| grs.dbankcloud.asia | IP: 49.4.35.251  所属国家: China  地区: Guangdong  城市: Guangzhou |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| appgallery.cloud.huawei.comhttps | 没有服务器地理信息. |
| wspeed.qq.com | 没有服务器地理信息. |
| www.baidu.com | IP: 110.242.70.57  所属国家: China  地区: Hebei  城市: Baoding |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| metrics2.data.hicloud.com | IP: 80.158.38.48  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| grs.dbankcloud.com | IP: 60.28.200.159  所属国家: China  地区: Tianjin  城市: Tianjin |
| java.oracle.com | IP: 23.210.26.31  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| aomedia.org | IP: 54.234.18.200  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| www.oracle.com | IP: 23.219.69.212  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.mob.com | IP: 180.188.26.28  所属国家: China  地区: Zhejiang  城市: Taizhou |
| cdn.ronghub.com | IP: 60.221.18.41  所属国家: China  地区: Shanxi  城市: Taiyuan |
| appgallery.cloud.huawei.com | IP: 49.4.35.16  所属国家: China  地区: Guangdong  城市: Guangzhou |
| grs.dbankcloud.cn | IP: 49.4.40.185  所属国家: China  地区: Guangdong  城市: Guangzhou |
| bugreport.sun.com | IP: 23.208.227.240  所属国家: Japan  地区: Osaka  城市: Ibaraki |
| auth.snapchat.com | IP: 74.125.20.121  所属国家: United States of America  地区: California  城市: Mountain View |
| www.tutorialspoint.com | IP: 3.173.219.78  所属国家: United States of America  地区: Washington  城市: Seattle |
| 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 |
| wap.cmpassport.com | IP: 112.33.111.233  所属国家: China  地区: Anhui  城市: Hefei |
| wappaygw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| open.weixin.qq.com | IP: 140.207.176.25  所属国家: China  地区: Shanghai  城市: Shanghai |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| ulogs.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100  所属国家: Singapore  地区: Singapore  城市: Singapore |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://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://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://onepass.geetest.com | com/geetest/onelogin/o/f.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/geetest/onelogin/l/e.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/geetest/onelogin/l/e.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/geetest/onelogin/l/e.java |
| https://onepass.geetest.com | com/geetest/onepassv2/bean/a.java |
| https://onepass.geetest.com | com/geetest/onepassv2/c/b.java |
| https://api-push.meizu.com/garcia/api/server/getPublicKey | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.in.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| http://norma-external-collect.meizu.com/android/exchange/getpublickey.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| http://norma-external-collect.meizu.com/push/android/external/add.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/o1oo/o1oo.java |
| https://api-push.in.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/o1oo/o1oo.java |
| https://api-push.meizu.com/garcia/api/client/log/upload | com/meizu/cloud/pushsdk/platform/o1oo/o1oo.java |
| https://github.com/yyued/SVGAPlayer-Android | com/opensource/svgaplayer/o1o11o.java |
| https://223.6.6.6/dns-query | com/qiniu/android/storage/GlobalConfiguration.java |
| https://8.8.8.8/dns-query | com/qiniu/android/storage/GlobalConfiguration.java |
| https://www.qiniu.com | com/qiniu/android/storage/GlobalConfiguration.java |
| https://www.baidu.com | com/qiniu/android/storage/GlobalConfiguration.java |
| https://www.google.com | com/qiniu/android/storage/GlobalConfiguration.java |
| https://pipeline.qiniu.com | com/qiniu/android/bigdata/Configuration.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 |
| https://openmobile.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://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| http://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/auth/a.java |
| https://openmobile.qq.com/v3/user/get\_info | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | com/tencent/connect/auth/AuthAgent.java |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | com/tencent/connect/auth/AuthAgent.java |
| https://openmobile.qq.com/user/user\_login\_statis | 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://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| http://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| http://login.imgcache.qq.com | com/tencent/open/SocialApiIml.java |
| http://login.imgcache.qq.com/open/mobile/request/sdk\_request.html? | com/tencent/open/SocialApiIml.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group | com/tencent/open/SocialOperation.java |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind | com/tencent/open/SocialOperation.java |
| https://huatuocode.huatuo.qq.com | com/tencent/open/a/d.java |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/f.java |
| http://cgi.qplus.com/report/report | com/tencent/open/utils/k.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/c.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/b.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://developer.umeng.com/docs/119267/detail/182050 | com/umeng/commonsdk/debug/UMLogCommon.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file= | com/xiaomi/mipush/sdk/OO010O.java |
| https://api.xmpush.xiaomi.com/upload/app\_log?file= | com/xiaomi/mipush/sdk/OO010O.java |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file= | com/xiaomi/mipush/sdk/o1oo.java |
| http://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/o0.java |
| https://register.xmpush.global.xiaomi.com | com/xiaomi/push/service/O0OOoO1.java |
| https://fr.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/O0OOoO1.java |
| https://ru.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/O0OOoO1.java |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| https://play.google.com/store | 摸瓜V1引擎 |
| https://appgallery.cloud.huawei.com/app/ | 摸瓜V1引擎 |
| https://play.google.com/store/apps/details?id= | 摸瓜V1引擎 |
| https://appgallery.cloud.huawei.com | 摸瓜V1引擎 |
| http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. | 摸瓜V1引擎 |
| http://www.mob.com/about/policy>http://www.mob.com/about/policy</a> | 摸瓜V1引擎 |
| https://www.mob.com | 摸瓜V1引擎 |
| https://store.hispace.hicloud.com/hwmarket/api/ | 摸瓜V1引擎 |
| http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If | 摸瓜V1引擎 |
| http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a> | 摸瓜V1引擎 |
| http://' | 摸瓜V2引擎 |
| https://cdn.ronghub.com/sight\_msg.png' | 摸瓜V2引擎 |
| https://cdn.ronghub.com/lbs\_msg.png'></div><div | 摸瓜V2引擎 |
| https://metrics1.data.hicloud.com:6447 | 摸瓜V2引擎 |
| https://metrics-dra.dt.hicloud.com:6447 | 摸瓜V2引擎 |
| https://metrics2.data.hicloud.com:6447 | 摸瓜V2引擎 |
| https://metrics5.data.hicloud.com:6447 | 摸瓜V2引擎 |
| https://grs.dbankcloud.com | 摸瓜V2引擎 |
| https://grs.dbankcloud.cn | 摸瓜V2引擎 |
| https://grs.dbankcloud.eu | 摸瓜V2引擎 |
| https://grs.dbankcloud.asia | 摸瓜V2引擎 |
| http://schemas.android.com/apk/res/android((layout/fragment\_main\_child\_live\_stream\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android$$layout/im\_item\_greet\_activity\_list\_0 | 摸瓜V3引擎 |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | 摸瓜V3引擎 |
| http://www.mob.com/about/policy | 摸瓜V3引擎 |
| http://es5.github.io/#x15.4.4.21 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##io.rong.imkit.widget.AsyncImageView | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://mobilegw.stable.alipay.net/mgw.htm | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/public\_fragment\_action\_dialog\_0 | 摸瓜V3引擎 |
| https://www.oracle.com/javase/jmc | 摸瓜V3引擎 |
| https://api-push.in.meizu.com/garcia/api/client/ | 摸瓜V3引擎 |
| https://www.oracle.com/technetwork/java/javase/downloads | 摸瓜V3引擎 |
| https://aomedia.org/emsg/ID3 | 摸瓜V3引擎 |
| https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\_Objects/String/startsWith | 摸瓜V3引擎 |
| https://openmobile.qq.com/oauth2.0/me | 摸瓜V3引擎 |
| https://metrics1.data.hicloud.com:6447 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android//layout/mine\_conversation\_type\_dialog\_fragment\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##layout/room\_item\_public\_msg\_emoji\_0 | 摸瓜V3引擎 |
| http://www.computerhope.com/forum/index.php?topic=76293.0 | 摸瓜V3引擎 |
| http://www.mob.com/about/policy/en | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android%%layout/mine\_activity\_edit\_character\_0 | 摸瓜V3引擎 |
| https://auth.wosms.cn | 摸瓜V3引擎 |
| https://api-push.meizu.com | 摸瓜V3引擎 |
| http://stackoverflow.com/a/15123777 | 摸瓜V3引擎 |
| http://dashif.org/guidelines/trickmode | 摸瓜V3引擎 |
| http://stackoverflow.com/questions/1026069/capitalize-the-first-letter-of-string-in-javascript | 摸瓜V3引擎 |
| http://mobilegw.aaa.alipay.net/mgw.htm | 摸瓜V3引擎 |
| https://auth.snapchat.com/oauth2/api/user.bitmoji.avatar | 摸瓜V3引擎 |
| https://openmobile.qq.com/v3/user/get\_info | 摸瓜V3引擎 |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | 摸瓜V3引擎 |
| http://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | 摸瓜V3引擎 |
| https://wspeed.qq.com/w.cgi | 摸瓜V3引擎 |
| http://dashif.org/guidelines/last-segment-number | 摸瓜V3引擎 |
| http://login.imgcache.qq.com/open/mobile/request/sdk\_request.html? | 摸瓜V3引擎 |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signatur | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/item\_live\_stream\_public\_voice\_0 | 摸瓜V3引擎 |
| https://store.hispace.hicloud.com/hwmarket/api/ | 摸瓜V3引擎 |
| http://java.oracle.com/ | 摸瓜V3引擎 |
| http://stackoverflow.com/a/1465386/4224163 | 摸瓜V3引擎 |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| edge.ds-c7110-microsoft.global.dns.qwilted-cds.cqloud.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android))io.rong.imkit.plugin.image.HackyViewPager | 摸瓜V3引擎 |
| http://www.mob.com/policy/en | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android((layout/im\_item\_other\_side\_info\_message\_0 | 摸瓜V3引擎 |
| https://grs.dbankcloud.eu | 摸瓜V3引擎 |
| https://huatuocode.huatuo.qq.com | 摸瓜V3引擎 |
| https://appgallery.cloud.huawei.com | 摸瓜V3引擎 |
| https://appgallery.cloud.huawei.com((https://appgallery.cloud.huawei.com/app/88https://auth.snapchat | 摸瓜V3引擎 |
| https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\_Objects/Array/Reduce | 摸瓜V3引擎 |
| https://www.mob.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android%%layout/im\_fragment\_sub\_con\_stranger\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android%%layout/multi\_live\_item\_icons\_layout\_0 | 摸瓜V3引擎 |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread | 摸瓜V3引擎 |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | 摸瓜V3引擎 |
| http://developer.umeng.com/docs/66650/cate/66650 | 摸瓜V3引擎 |
| https://metrics-dra.dt.hicloud.com:6447 | 摸瓜V3引擎 |
| https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\_Objects/String/Trim | 摸瓜V3引擎 |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | 摸瓜V3引擎 |
| http://login.imgcache.qq.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##layout/im\_fragment\_image\_send\_tip\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android$$layout/room\_item\_chatroom\_backound\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android%%layout/mine\_fragment\_bind\_phone\_tip\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##io.rong.imkit.widget.AsyncImageView))io.rong.imkit.widge | 摸瓜V3引擎 |
| http://www.tutorialspoint.com/javascript/array\_map.htm | 摸瓜V3引擎 |
| https://api-push.meizu.com/garcia/api/server/getPublicKey | 摸瓜V3引擎 |
| https://grs.dbankcloud.asia | 摸瓜V3引擎 |
| https://pipeline.qiniu.com | 摸瓜V3引擎 |
| http://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html? | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android((layout/fragment\_video\_card\_newer\_guide\_0 | 摸瓜V3引擎 |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android$$layout/im\_dialog\_fragment\_un\_reply\_0 | 摸瓜V3引擎 |
| http://bugreport.sun.com/bugreport/ | 摸瓜V3引擎 |
| http://www.mob.com/policy/zh | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android//layout/im\_call\_error\_intimacy\_dialog\_fragment\_0 | 摸瓜V3引擎 |
| http://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | 摸瓜V3引擎 |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind | 摸瓜V3引擎 |
| https://developer.mozilla.org/en/docs/Web/JavaScript/Reference/Global\_Objects/String/endsWith | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/119267/detail/182050 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/room\_vip\_gift\_dialog\_fragment\_0 | 摸瓜V3引擎 |
| https://grs.dbankcloud.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/dialog\_sign\_in\_receive\_reward\_0 | 摸瓜V3引擎 |
| http://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | 摸瓜V3引擎 |
| https://api-push.meizu.com/garcia/api/client/log/upload | 摸瓜V3引擎 |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android((layout/im\_item\_sub\_conversation\_others\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##layout/im\_dialog\_notification\_tip\_0 | 摸瓜V3引擎 |
| http://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | 摸瓜V3引擎 |
| https://onepass.geetest.com | 摸瓜V3引擎 |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android11layout/room\_fragment\_live\_broadcast\_preparation\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##ivFullMic | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/activity\_watch\_imgs\_with\_chat\_0 | 摸瓜V3引擎 |
| https://metrics5.data.hicloud.com:6447 | 摸瓜V3引擎 |
| https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\_Objects/Array/filter | 摸瓜V3引擎 |
| https://openmobile.qq.com/user/user\_login\_statis | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android))layout/fragment\_dialog\_pickup\_countdown\_0 | 摸瓜V3引擎 |
| https://metrics2.data.hicloud.com:6447 | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/66632/detail/ | 摸瓜V3引擎 |
| https://api-push.meizu.com/garcia/api/client/ | 摸瓜V3引擎 |
| http://www.oracle.com/technetwork/java/javase/documentation/index.html | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/im\_fragment\_greet\_eidt\_dialog\_0 | 摸瓜V3引擎 |
| https://mobilegw.alipay.com/mgw.htm | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android&&layout/im\_item\_sub\_conversation\_list\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android11layout/im\_intimacy\_introduction\_dialog\_fragment\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android##layout/im\_fragment\_sub\_con\_others\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android%%layout/fragment\_dialog\_video\_dating\_0 | 摸瓜V3引擎 |
| https://daily.m.zzx9.cn | 摸瓜V3引擎 |
| http://stackoverflow.com/questions/1068834/object-comparison-in-javascript | 摸瓜V3引擎 |
| https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global\_Objects/Array/indexOf | 摸瓜V3引擎 |
| https://wap.cmpassport.com/resources/html/contract.html | 摸瓜V3引擎 |
| https://grs.dbankcloud.cn | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://appgallery.cloud.huawei.com/app/ | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android((layout/im\_fragment\_call\_gallery\_dialog\_0 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android((layout/im\_fragment\_friendship\_fund\_tip\_0 | 摸瓜V3引擎 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=ZheJiang, L=HangZhou, O=flashwhale, OU=flashwhale, CN=flashwhale 签名算法: rsassa\_pkcs1v15 有效期自: 2020-04-29 08:27:47+00:00 有效期至: 2045-04-23 08:27:47+00:00 发行人: C=CN, ST=ZheJiang, L=HangZhou, O=flashwhale, OU=flashwhale, CN=flashwhale 序列号: 0x62861e43 哈希算法: sha256 md5值: b8f4cefccb48953c0cb072b6b540d8f0 sha1值: 02486ae5433143052d4ec04b10e9b0f4c01f11e2 sha256值: b7d077a1621d19430dd06493df9e8cd83398409caed1a8f02f4e5b804ad2606b sha512值: ef051e193644fb95d6c0488e64c4c3a9bba2ad845a276e7b169971c84b07ff51eab9546f97a916defb4d601c5d58d64d40c0d24229a7d1eb4a4ba52a299b2bba**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_auth\_checking" : "审核中" |
| "account\_auth\_id" : "身份证号：" |
| "account\_auth\_name" : "姓名：" |
| "account\_auth\_now" : "立即认证" |
| "account\_auth\_ok" : "已认证" |
| "account\_auth\_tip\_female" : "提高曝光，收益翻倍" |
| "account\_auth\_tip\_male" : "提高曝光，优先推荐" |
| "account\_authenticateNow" : "立即认证" |
| "account\_go\_authenticate" : "去认证" |
| "account\_id\_auth" : "身份认证" |
| "account\_manual\_auth" : "人工认证" |
| "account\_my\_auth" : "我的认证" |
| "account\_real\_name\_auth" : "实名认证" |
| "account\_start\_del\_user" : "开始注销" |
| "account\_un\_authentication\_desc" : "为了提供更高级的服务， 需要验证身份信息" |
| "account\_un\_authentication\_reviewing\_desc" : "身份验证正在审核中" |
| "gt\_one\_login\_auth\_btn" : "一键登录" |
| "im\_private\_look\_detail" : "查看个人主页" |
| "mine\_auth" : "认证" |
| "mine\_face\_auth\_reviewing" : "审核中" |
| "mine\_face\_auth\_unqualified" : "不合格" |
| "mine\_go\_auth" : "去认证" |
| "mine\_has\_auth" : "已认证" |
| "mine\_has\_auth\_reviewing" : "审核中" |
| "mine\_keep\_secret" : "保密" |
| "mine\_my\_auth" : "我的认证" |
| "mine\_not\_auth" : "未认证" |
| "mine\_real\_name\_auth" : "实名认证" |
| "mine\_real\_name\_auth\_for\_recharge\_msg" : "为了确保您的账户安全请完成 实名认证" |
| "mobcommon\_authorize\_dialog\_accept" : "Accept" |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject" |
| "mobcommon\_authorize\_dialog\_reject" : "Reject" |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use" |
| "mobdemo\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/about/policy>http://www.mob.com/about/policy</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。" |
| "mobdemo\_authorize\_dialog\_title" : "服务授权" |
| "public\_auth\_now" : "立即认证" |
| "public\_authorize\_to\_obtain\_phonenumber" : "并授权获取本机号码" |
| "public\_secret" : "保密" |
| "rc\_authorities\_fileprovider" : ".FileProvider" |
| "rc\_conversation\_list\_my\_private\_conversation" : "我的私人会话" |
| "rc\_emoji\_hear\_no\_monkey" : "不听" |
| "rc\_emoji\_see\_no\_monkey" : "不看" |
| "room\_all\_mic\_user" : "全麦用户" |
| "room\_go\_auth" : "去认证" |
| "room\_go\_auth\_name" : "去实名" |
| "room\_please\_complete\_name\_authentication\_first" : "请先完成实名认证" |
| "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" |
| "teenager\_mode\_forget\_password" : "忘记密码？请联系客服微信：%1$s 账号ID：%2$s" |
| "gt\_one\_login\_auth\_btn" : "one-click login" |
| "mobcommon\_authorize\_dialog\_accept" : "Accept" |
| "mobcommon\_authorize\_dialog\_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click <a href=http://www.mob.com/policy/en>http://www.mob.com/policy/en</a>. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject" |
| "mobcommon\_authorize\_dialog\_reject" : "Reject" |
| "mobcommon\_authorize\_dialog\_title" : "Terms of Use" |
| "mobdemo\_authorize\_dialog\_content" : "In order to provide you with Mobservice related products and services, please check our privacy policy in detail, see details<a href=http://www.mob.com/about/policy/en>http://www.mob.com/about/policy/en</a>.If you agree with our privacy policy, please click accept. If you disagree with our privacy policy, please click reject." |
| "mobdemo\_authorize\_dialog\_title" : "service authority" |
| "rc\_conversation\_list\_my\_private\_conversation" : "My private conversation" |
| "rc\_emoji\_hear\_no\_monkey" : "Hear-No-Monkey" |
| "rc\_emoji\_see\_no\_monkey" : "See-No-Monkey" |
| "ssdk\_cmcc\_auth" : "Provided by China Mobile" |
| "ssdk\_cmcc\_login\_one\_key" : "PhoneNum Login" |
| "ssdk\_instapaper\_pwd" : "Password" |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization" |
| "gt\_one\_login\_auth\_btn" : "一鍵登錄" |
| "mobcommon\_authorize\_dialog\_accept" : "同意" |
| "mobcommon\_authorize\_dialog\_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见<a href=http://www.mob.com/policy/zh>http://www.mob.com/policy/zh</a>。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。" |
| "mobcommon\_authorize\_dialog\_reject" : "拒绝" |
| "mobcommon\_authorize\_dialog\_title" : "服务授权" |

## **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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收 | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.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.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.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.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.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\_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.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.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.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.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.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.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.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。 |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huahua.dating.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huahua.dating.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| com.huahua.dating.permission.RONG\_ACCESS\_RECEIVER | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.huahua.dating.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.huahua.dating.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.huahua.dating.ui.view.activity.MainActivity | **Schemes**: hhdatingapp://, |
| com.huahua.dating.ui.view.activity.TeenagerModeActivity | **Schemes**: hhdatingapp://, |
| com.huahua.account.ui.view.activity.IdentityAuthActivity | **Schemes**: hhauthenticatecall://, |
| com.huahua.pay.ui.view.PayActivity | **Schemes**: sandcash://,  **Hosts:** scpay, |
| cn.sharesdk.tencent.qq.ReceiveActivity | **Schemes**: tencent1110990371://, |

**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。**