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

**福彩阁（ 1.0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 | 福彩阁 |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 105条 |
| URL线索 | 89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 | 424\_3fgUsbx.apk |
| 文件大小 | 75.59MB |
| MD5值 | 8f6c160e91eb668eef27ce51f8e02d58 |
| SHA1值 | 786671db9f66896a4412a3582e0494d396ca4c0d |
| SHA256值 | 2b02a389733823ce6e349704d718c38f1fd16ecc6ff63170b8351b6e97373ae8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 福彩阁 |
| 包名 |  |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | [] |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| playready.directtaps.net | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| merchant.5upay.com | IP: 123.56.64.111 所属国家: China 地区: Beijing 城市: Beijing  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| m.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| ce3e75d5.jpush.cn | IP: 120.233.118.169 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| login.imgcache.qq.com | IP: 220.194.122.222 所属国家: China 地区: Tianjin 城市: Tianjin  |
| register.xmpush.global.xiaomi.com | IP: 47.237.96.1 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| mdc.html5.qq.com | IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing  |
| wallet.95516.com | IP: 116.196.139.42 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| 10.10.10.61 | IP: 10.10.10.61 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| fusion.qq.com | IP: 116.130.229.204 所属国家: China 地区: Beijing 城市: Beijing  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| new.api.ad.xiaomi.com | 没有服务器地理信息.  |
| dev-merchant.5upay.com | IP: 172.24.3.120 所属国家: - 地区: - 城市: -  |
| www.wh.com | IP: 216.137.39.98 所属国家: United States of America 地区: California 城市: Los Angeles  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| www.eclipse.org | IP: 198.41.30.198 所属国家: Canada 地区: Ontario 城市: Brampton  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| www.sina.com.hk | IP: 199.16.156.38 所属国家: United States of America 地区: Georgia 城市: Atlanta  |
| push.statics | 没有服务器地理信息.  |
| appsupport.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| bjuser.jpush.cn | IP: 122.9.5.30 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.5.com | 没有服务器地理信息.  |
| h5.m.taobao.com | IP: 125.39.155.58 所属国家: China 地区: Tianjin 城市: Tianjin  |
| qa-webox-api.5upay.com | 没有服务器地理信息.  |
| mcgw.alipay.com | IP: 116.196.141.48 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| resolver.msg.xiaomi.net | IP: 110.43.0.41 所属国家: China 地区: Beijing 城市: Beijing  |
| www.huawei.com | IP: 120.52.95.238 所属国家: China 地区: Hebei 城市: Langfang  |
| 10.10.10.176 | IP: 10.10.10.176 所属国家: - 地区: - 城市: -  |
| uat-webox-api.5upay.com | 没有服务器地理信息.  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| wappaygw.alipay.com | IP: 116.196.141.52 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| open.weixin.qq.com | IP: 220.196.132.78 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| ip.chinaz.com | IP: 123.129.219.142 所属国家: China 地区: Shandong 城市: Jinan  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.inkscape.org | IP: 140.211.9.79 所属国家: United States of America 地区: Oregon 城市: Eugene  |
| www.5upay.com | IP: 118.26.164.135 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| loggw-exsdk.alipay.com | IP: 110.76.6.92 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 182.92.20.189 | IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing  |
| g.cn | IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing  |
| acs.amazonaws.com | 没有服务器地理信息.  |
| d.alipay.com | IP: 116.196.141.47 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| www.qq.com | IP: 221.198.70.47 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.xmpush.xiaomi.com | IP: 123.125.102.209 所属国家: China 地区: Beijing 城市: Beijing  |
| www.4.com | 没有服务器地理信息.  |
| wspeed.qq.com | 没有服务器地理信息.  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| www.2.com | 没有服务器地理信息.  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| uat-merchant.5upay.com | IP: 172.16.12.112 所属国家: - 地区: - 城市: -  |
| wiki.eclipse.org | IP: 198.41.30.195 所属国家: Canada 地区: Ontario 城市: Brampton  |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| mclient.alipay.com | IP: 124.95.170.204 所属国家: China 地区: Liaoning 城市: Shenyang  |
| tsis.jpush.cn | IP: 110.41.23.105 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| app.mi.com | IP: 221.194.175.44 所属国家: China 地区: Hebei 城市: Langfang  |
| webox.5upay.com | IP: 47.95.113.116 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  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| idmb.register.xmpush.global.xiaomi.com | IP: 20.219.205.9 所属国家: India 地区: Maharashtra 城市: Pune  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| pv.sohu.com | IP: 123.125.244.28 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| dev-webox-api.ehking.com | 没有服务器地理信息.  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| 34.150.84.57 | IP: 34.150.84.57 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.3.com | 没有服务器地理信息.  |
| netty.io | IP: 172.67.130.186 所属国家: United States of America 地区: California 城市: San Francisco  |
| render.alipay.com | IP: 124.165.219.237 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.google.com | IP: 31.13.94.41 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| grs.dbankcloud.cn | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| tools.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| sodipodi.sourceforge.net | IP: 104.18.13.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.ip.sb | IP: 172.67.75.172 所属国家: United States of America 地区: California 城市: San Francisco  |
| 169.254.169.254 | IP: 169.254.169.254 所属国家: - 地区: - 城市: -  |
| qa-merchant.5upay.com | IP: 172.24.3.124 所属国家: - 地区: - 城市: -  |
| xrcf0530.s3.ap-southeast-1.amazonaws.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| cn.register.xmpush.xiaomi.com | IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| astat.bugly.qcloud.com | IP: 119.28.121.133 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dev-sdk.ehking.com | 没有服务器地理信息.  |
| www.geetest.com | IP: 116.196.155.61 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| cgi.qplus.com | 没有服务器地理信息.  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobilegw.alipay.com | IP: 203.209.243.27 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| vfx.mtime.cn | IP: 121.29.9.33 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| static.geetest.com | IP: 60.28.220.193 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  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://tsis.jpush.cn  | cn/jiguang/ao/i.java  |
| https://bjuser.jpush.cn/v1/appawake/status  | cn/jiguang/ai/b.java  |
| http://182.92.20.189:9099/  | cn/jiguang/r/a.java  |
| https://ce3e75d5.jpush.cn/wi/cjc4sa  | cn/jiguang/aj/d.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://render.alipay.com/p/s/i?scheme=%s  | com/alipay/sdk/app/OpenAuthTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| http://g.cn/generate\_204  | com/ehking/sdk/wepay/utlis/CheckWifiLoginTask.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | com/ehking/sdk/wepay/utlis/NetUtils.java  |
| https://wallet.95516.com/s/wl/webV3/activity/yhtzB/insB2c/html/b2cIndex.html?institutionId=E00000295038  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://webox.5upay.com/  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/constant/Constants.java  |
| https://qa-webox-api.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://qa-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://qa-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://webox.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-webox-api.5upay.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://uat-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-webox-api.ehking.com/  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| https://dev-merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/ehking/sdk/wepay/interfaces/WalletPay.java  |
| http://app.mi.com/detail/163525?ref=search  | com/getmessage/lite/presenter/AboutUsPresenter.java  |
| http://www.huawei.com  | com/getmessage/lite/view/TestActivity.java  |
| http://www.qq.com  | com/getmessage/lite/view/TestActivity.java  |
| http://www.sina.com.hk  | com/getmessage/lite/view/TestActivity.java  |
| http://www.google.com  | com/getmessage/lite/view/TestActivity.java  |
| http://vfx.mtime.cn/Video/2019/03/21/mp4/190321153853126488.mp4  | com/getmessage/lite/view/TestActivity.java  |
| http://10.10.10.176:80  | com/getmessage/module\_base/model/bean/HttpServerConfigEntity.java  |
| http://www.2.com  | com/getmessage/module\_base/model/bean/HttpServerConfigEntity.java  |
| http://www.3.com  | com/getmessage/module\_base/model/bean/HttpServerConfigEntity.java  |
| http://www.4.com  | com/getmessage/module\_base/model/bean/HttpServerConfigEntity.java  |
| http://www.5.com  | com/getmessage/module\_base/model/bean/HttpServerConfigEntity.java  |
| https://d.alipay.com  | com/getmessage/module\_base/web/WebViewHelper.java  |
| https://d.alipay.com  | com/getmessage/module\_base/web/x5WebViewHelper.java  |
| http://www.geetest.com/first\_page  | com/geetest/sdk/views/GT3GeetestButton.java  |
| https://push.statics  | com/meizu/cloud/pushsdk/networking/http/HttpURLConnectionCall.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/api/PushAPI.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/api/PushAPI.java  |
| https://dev-sdk.ehking.com/callback  | com/payeasenet/wepay/ui/viewModel/OrderPayModel.java  |
| https://dev-sdk.ehking.com/onlinepay/notify\_V3  | com/payeasenet/wepay/ui/viewModel/OrderPayModel.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | com/payeasenet/wepay/utlis/NetUtils.java  |
| https://merchant.5upay.com/webox/agreement/privacyPolicy.html  | com/payeasenet/wepay/constant/Constants.java  |
| https://merchant.5upay.com/webox/agreement/serviceAgreement.html  | com/payeasenet/wepay/constant/Constants.java  |
| https://www.5upay.com/  | com/payeasenet/wepay/constant/Constants.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://127.0.0.1/android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/j.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/m.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/m.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd'  | com/github/siyamed/shapeimageview/path/parser/SvgToPath.java  |
| http://www.inkscape.org/namespaces/inkscape'  | com/github/siyamed/shapeimageview/path/parser/SvgToPath.java  |
| https://tools.ietf.org/html/rfc7540  | io/netty/handler/codec/http2/HttpConversionUtil.java  |
| https://wiki.eclipse.org/Jetty/Feature/NPN  | io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java  |
| http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html  | io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java  |
| https://netty.io/wiki/forked-tomcat-native.html  | io/netty/handler/ssl/OpenSsl.java  |
| https://www.openssl.org/docs/man1.0.2/apps/verify.html.  | io/netty/handler/ssl/OpenSslCertificateException.java  |
| https://netty.io/wiki/sslcontextbuilder-and-private-key.html  | io/netty/handler/ssl/PemReader.java  |
| https://netty.io/wiki/reference-counted-objects.html  | io/netty/util/ResourceLeakDetector.java  |
| http://pv.sohu.com/cityjson  | p/a/y/e/a/s/e/net/kd0.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | p/a/y/e/a/s/e/net/kd0.java  |
| http://ip.chinaz.com/getip.aspx  | p/a/y/e/a/s/e/net/kd0.java  |
| https://xrcf0530.s3.ap-southeast-1.amazonaws.com/fcg\_0630  | p/a/y/e/a/s/e/net/l50.java  |
| https://34.150.84.57:24465  | p/a/y/e/a/s/e/net/l50.java  |
| https://127.0.0.1/fhim-Proxy.txt  | p/a/y/e/a/s/e/net/l50.java  |
| http://xmlpull.org/v1/doc/features.html  | p/a/y/e/a/s/e/net/in2.java  |
| http://m.alipay.com/?action=h5quit  | p/a/y/e/a/s/e/net/w2.java  |
| https://mobilegw.alipay.com/mgw.htm  | p/a/y/e/a/s/e/net/w2.java  |
| https://mcgw.alipay.com/sdklog.do  | p/a/y/e/a/s/e/net/w2.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | p/a/y/e/a/s/e/net/w2.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | p/a/y/e/a/s/e/net/w2.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | p/a/y/e/a/s/e/net/w2.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | p/a/y/e/a/s/e/net/w2.java  |
| http://www.slf4j.org/codes.html  | p/a/y/e/a/s/e/net/cs3.java  |
| http://xml.apache.org/xslt  | p/a/y/e/a/s/e/net/n62.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | p/a/y/e/a/s/e/net/sn2.java  |
| https://127.0.0.1/cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | p/a/y/e/a/s/e/net/cd2.java  |
| http://new.api.ad.xiaomi.com/logNotificationAdActions  | p/a/y/e/a/s/e/net/dk2.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | p/a/y/e/a/s/e/net/z2.java  |
| http://www.slf4j.org/codes.html  | p/a/y/e/a/s/e/net/bs3.java  |
| http://xmlpull.org/v1/doc/features.html  | p/a/y/e/a/s/e/net/yn2.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | p/a/y/e/a/s/e/net/tm.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | p/a/y/e/a/s/e/net/tm.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | p/a/y/e/a/s/e/net/tm.java  |
| http://%s:%d/%s  | p/a/y/e/a/s/e/net/vm.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | p/a/y/e/a/s/e/net/vm.java  |
| http://%1$s/gslb/?ver=4.0  | p/a/y/e/a/s/e/net/mk2.java  |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file=  | p/a/y/e/a/s/e/net/gh2.java  |
| https://api.xmpush.xiaomi.com/upload/app\_log?file=  | p/a/y/e/a/s/e/net/gh2.java  |
| https://wspeed.qq.com/w.cgi  | p/a/y/e/a/s/e/net/ic2.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | p/a/y/e/a/s/e/net/ic2.java  |
| http://cgi.qplus.com/report/report  | p/a/y/e/a/s/e/net/hd2.java  |
| https://huatuocode.huatuo.qq.com  | p/a/y/e/a/s/e/net/fc2.java  |
| https://login.imgcache.qq.com/open/mobile/request/sdk\_request.html?  | p/a/y/e/a/s/e/net/yb2.java  |
| https://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | p/a/y/e/a/s/e/net/yb2.java  |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | p/a/y/e/a/s/e/net/yb2.java  |
| https://login.imgcache.qq.com  | p/a/y/e/a/s/e/net/yb2.java  |
| https://static.geetest.com/static/appweb/app3-index.html  | p/a/y/e/a/s/e/net/j30.java  |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file=  | p/a/y/e/a/s/e/net/ih2.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | p/a/y/e/a/s/e/net/kb2.java  |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | p/a/y/e/a/s/e/net/kb2.java  |
| https://openmobile.qq.com/oauth2.0/me  | p/a/y/e/a/s/e/net/za2.java  |
| http://xmlpull.org/v1/doc/features.html  | p/a/y/e/a/s/e/net/zn2.java  |
| http://xmlpull.org/v1/doc/features.html  | p/a/y/e/a/s/e/net/ym2.java  |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | p/a/y/e/a/s/e/net/eb2.java  |
| http://resolver.msg.xiaomi.net/psc/?t=a  | p/a/y/e/a/s/e/net/er2.java  |
| http://acs.amazonaws.com/groups/s3/LogDelivery  | p/a/y/e/a/s/e/net/zw1.java  |
| http://acs.amazonaws.com/groups/global/AllUsers  | p/a/y/e/a/s/e/net/zw1.java  |
| http://acs.amazonaws.com/groups/global/AuthenticatedUsers  | p/a/y/e/a/s/e/net/zw1.java  |
| http://169.254.169.254  | p/a/y/e/a/s/e/net/fy1.java  |
| https://cn.register.xmpush.xiaomi.com  | p/a/y/e/a/s/e/net/gs2.java  |
| https://register.xmpush.global.xiaomi.com  | p/a/y/e/a/s/e/net/gs2.java  |
| https://fr.register.xmpush.global.xiaomi.com  | p/a/y/e/a/s/e/net/gs2.java  |
| https://ru.register.xmpush.global.xiaomi.com  | p/a/y/e/a/s/e/net/gs2.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | p/a/y/e/a/s/e/net/gs2.java  |
| http://%s:%d/%s  | p/a/y/e/a/s/e/net/rm.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | p/a/y/e/a/s/e/net/ac2.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | p/a/y/e/a/s/e/net/ac2.java  |
| http://10.10.10.61:8889  | p/a/y/e/a/s/e/net/y21.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | p/a/y/e/a/s/e/net/ob2.java  |
| http://fusion.qq.com/cgi-bin/qzapps/unified\_jump?appid=%1$s&from=%2$s&isOpenAppID=1  | p/a/y/e/a/s/e/net/qb2.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | p/a/y/e/a/s/e/net/cb2.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | p/a/y/e/a/s/e/net/cb2.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | p/a/y/e/a/s/e/net/cb2.java  |
| https://openmobile.qq.com/v3/user/get\_info  | p/a/y/e/a/s/e/net/cb2.java  |
| http://pv.sohu.com/cityjson  | p/a/y/e/a/s/e/net/m11.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | p/a/y/e/a/s/e/net/m11.java  |
| http://ip.chinaz.com/getip.aspx  | p/a/y/e/a/s/e/net/m11.java  |
| https://api.ip.sb/geoip  | p/a/y/e/a/s/e/net/m11.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://www.wh.com/.well-known/assetlinks.json  | 摸瓜V1引擎  |
| 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  |
| 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  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| permission@gmail.com  | p/a/y/e/a/s/e/net/zu2.java  |
| danikula@gmail.com  | p/a/y/e/a/s/e/net/tm.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13000000000  | com/ehking/sdk/wepay/constant/Constants.java  |
| 18222222222  | com/tencent/smtt/sdk/j.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**无法读取代码签名证书.**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Enter\_your\_login\_password" : "输入登录密码"  |
| "Please\_enter\_your\_login\_password" : "请输入登录密码"  |
| "WeChat\_authorization\_failed" : "微信授权失败"  |
| "agree\_to\_authorize" : "同意授权"  |
| "authorization\_succeeded" : "授权成功"  |
| "easy\_password" : "密码过于简单"  |
| "encryption\_to\_retrieve\_password" : "密保找回密码"  |
| "enter\_password" : "输入小程序码"  |
| "fail\_pwd\_input" : "密码为6到16位数字和字母的组合"  |
| "fail\_pwd\_input\_identical" : "两次输入密码不一致"  |
| "fail\_pwd\_login\_input" : "密码格式不正确"  |
| "fill\_in\_user\_name" : "填写用户名"  |
| "forget\_password" : "忘记密码"  |
| "frgot\_password" : "忘记密码"  |
| "group\_no\_private\_instructions" : "开启后，群成员点击群内其他成员头像没有反应"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "login\_input\_password" : "请输入密码,6~20位字母或数字"  |
| "login\_input\_user" : "请输入用户名"  |
| "login\_user" : "用户名"  |
| "mark\_auth" : "提醒:后续只能绑定该持卡人的银行卡"  |
| "no\_private\_chat" : "禁止私聊"  |
| "please\_enter\_your\_payment\_password" : "请输入支付密码"  |
| "please\_input\_pwd\_ward" : "请输入支付密码，以验证身份"  |
| "please\_select\_secret\_protection\_problem" : "请选择密保问题："  |
| "public\_private\_group" : "是否为公开群组"  |
| "pwd" : "小程序"  |
| "register\_user" : "用户名"  |
| "retrieve\_password" : "找回密码"  |
| "secret" : "保密"  |
| "secret\_protection\_question" : "密保问题"  |
| "select\_secret\_protection\_problem" : "选择密保问题"  |
| "set\_pay\_password" : "设置支付密码"  |
| "use\_pwd" : "使用密码"  |
| "username\_is\_not\_bound\_to\_secret\_security" : "用户名未绑定密保，无法找回密码"  |
| "Enter\_your\_login\_password" : "‏‮输入登录密码‬‏"  |
| "Please\_enter\_your\_login\_password" : "‏‮请输入登录密码‬‏"  |
| "WeChat\_authorization\_failed" : "‏‮微信授权失败‬‏"  |
| "agree\_to\_authorize" : "‏‮同意授权‬‏"  |
| "authorization\_succeeded" : "‏‮授权成功‬‏"  |
| "easy\_password" : "‏‮密码过于简单‬‏"  |
| "encryption\_to\_retrieve\_password" : "‏‮密保找回密码‬‏"  |
| "enter\_password" : "‏‮输入小程序码‬‏"  |
| "fail\_pwd\_input" : "‏‮密码为6到16位数字和字母的组合‬‏"  |
| "fail\_pwd\_input\_identical" : "‏‮两次输入密码不一致‬‏"  |
| "fail\_pwd\_login\_input" : "‏‮密码格式不正确‬‏"  |
| "fill\_in\_user\_name" : "‏‮填写用户名‬‏"  |
| "forget\_password" : "‏‮忘记密码‬‏"  |
| "frgot\_password" : "‏‮忘记密码‬‏"  |
| "group\_no\_private\_instructions" : "‏‮开启后，群成员点击群内其他成员头像没有反应‬‏"  |
| "library\_roundedimageview\_author" : "‏‮Vince‬‏ ‏‮Mi‬‏"  |
| "library\_roundedimageview\_authorWebsite" : "‏‮https://github.com/vinc3m1‬‏"  |
| "login\_input\_password" : "‏‮请输入密码,6~20位字母或数字‬‏"  |
| "login\_input\_user" : "‏‮请输入用户名‬‏"  |
| "login\_user" : "‏‮用户名‬‏"  |
| "mark\_auth" : "‏‮提醒:后续只能绑定该持卡人的银行卡‬‏"  |
| "no\_private\_chat" : "‏‮禁止私聊‬‏"  |
| "please\_enter\_your\_payment\_password" : "‏‮请输入支付密码‬‏"  |
| "please\_input\_pwd\_ward" : "‏‮请输入支付密码，以验证身份‬‏"  |
| "please\_select\_secret\_protection\_problem" : "‏‮请选择密保问题：‬‏"  |
| "public\_private\_group" : "‏‮是否为公开群组‬‏"  |
| "pwd" : "‏‮小程序‬‏"  |
| "register\_user" : "‏‮用户名‬‏"  |
| "retrieve\_password" : "‏‮找回密码‬‏"  |
| "secret" : "‏‮保密‬‏"  |
| "secret\_protection\_question" : "‏‮密保问题‬‏"  |
| "select\_secret\_protection\_problem" : "‏‮选择密保问题‬‏"  |
| "set\_pay\_password" : "‏‮设置支付密码‬‏"  |
| "use\_pwd" : "‏‮使用密码‬‏"  |
| "username\_is\_not\_bound\_to\_secret\_security" : "‏‮用户名未绑定密保，无法找回密码‬‏"  |
| "Enter\_your\_login\_password" : "[输入登录密码 one two three]"  |
| "Please\_enter\_your\_login\_password" : "[请输入登录密码 one two three]"  |
| "WeChat\_authorization\_failed" : "[微信授权失败 one two three]"  |
| "agree\_to\_authorize" : "[同意授权 one two]"  |
| "authorization\_succeeded" : "[授权成功 one two]"  |
| "easy\_password" : "[密码过于简单 one two three]"  |
| "encryption\_to\_retrieve\_password" : "[密保找回密码 one two three]"  |
| "enter\_password" : "[输入小程序码 one two three]"  |
| "fail\_pwd\_input" : "[密码为6到16位数字和字母的组合 one two three four five]"  |
| "fail\_pwd\_input\_identical" : "[两次输入密码不一致 one two three four]"  |
| "fail\_pwd\_login\_input" : "[密码格式不正确 one two three]"  |
| "fill\_in\_user\_name" : "[填写用户名 one two three]"  |
| "forget\_password" : "[忘记密码 one two]"  |
| "frgot\_password" : "[忘记密码 one two]"  |
| "group\_no\_private\_instructions" : "[开启后，群成员点击群内其他成员头像没有反应 one two three four five six seven]"  |
| "library\_roundedimageview\_author" : "[νîñçé Ḿî one two]"  |
| "library\_roundedimageview\_authorWebsite" : "[ĥţţþš://ĝîţĥûɓ.çöḿ/Vîñç3ḿ1 one two three four]"  |
| "login\_input\_password" : "[请输入密码,6~20位字母或数字 one two three four five]"  |
| "login\_input\_user" : "[请输入用户名 one two three]"  |
| "login\_user" : "[用户名 one two]"  |
| "mark\_auth" : "[提醒:后续只能绑定该持卡人的银行卡 one two three four five six]"  |
| "no\_private\_chat" : "[禁止私聊 one two]"  |
| "please\_enter\_your\_payment\_password" : "[请输入支付密码 one two three]"  |
| "please\_input\_pwd\_ward" : "[请输入支付密码，以验证身份 one two three four five]"  |
| "please\_select\_secret\_protection\_problem" : "[请选择密保问题： one two three]"  |
| "public\_private\_group" : "[是否为公开群组 one two three]"  |
| "pwd" : "[小程序 one two]"  |
| "register\_user" : "[用户名 one two]"  |
| "retrieve\_password" : "[找回密码 one two]"  |
| "secret" : "[保密 one two]"  |
| "secret\_protection\_question" : "[密保问题 one two]"  |
| "select\_secret\_protection\_problem" : "[选择密保问题 one two three]"  |
| "set\_pay\_password" : "[设置支付密码 one two three]"  |
| "use\_pwd" : "[使用密码 one two]"  |
| "username\_is\_not\_bound\_to\_secret\_security" : "[用户名未绑定密保，无法找回密码 one two three four five]"  |

## **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**

## **10. 应用内通信**

**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。**