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

**赏帮赚（ 3.20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 | 赏帮赚 |
| 版本 | 3.20 |
| 包名 | com.yjhb.android.feibang |
| 域名线索 | 80条 |
| URL线索 | 79条 |
| APP图标 |  |
| 分析日期 | 2025年6月8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 | xinstall\_0529094630\_v3.20.apk |
| 文件大小 | 22.73MB |
| MD5值 | dd2ac183fd8f7ccedbf1739378006443 |
| SHA1值 | 9325e285f67c4b8a4e5ae2136fd9e48f7003c76b |
| SHA256值 | 1c1ac113439846c0c7cae0a72985d4a2d437b4a0d73bfcc881e0122468d34a3c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 赏帮赚 |
| 包名 | com.yjhb.android.feibang |
| 主活动Activity | com.zx.core.code.activity.StartActivity |
| 安卓版本名称 | 3.20 |
| 安卓版本 | 320 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| fs.cl20 | 没有服务器地理信息. |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| wap.cmpassport.com | IP: 112.33.111.233  所属国家: China  地区: Anhui  城市: Hefei |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| applog.uc.cn | IP: 116.132.216.227  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| appsupport.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| sparegateway.shangbangzhuan.com | 没有服务器地理信息. |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| h5.17xianwan.com | IP: 47.110.214.234  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m.shangbangzhuan.com | IP: 124.95.170.217  所属国家: China  地区: Liaoning  城市: Shenyang |
| a.shangbangzuan.com | 没有服务器地理信息. |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| android.bugly.qq.com | IP: 124.95.225.169  所属国家: China  地区: Liaoning  城市: Shenyang |
| newwoly.jiutaoleyuan.com | IP: 47.95.11.4  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pre.shangbangzhuan.com | 没有服务器地理信息. |
| api-e189.21cn.com | IP: 222.93.106.185  所属国家: China  地区: Jiangsu  城市: Suzhou |
| webaddress.elided | 没有服务器地理信息. |
| sysdk.cl2009.com | IP: 101.133.104.19  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m.playmy.cn | IP: 101.71.43.46  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mclient.alipay.com | IP: 218.61.164.134  所属国家: China  地区: Liaoning  城市: Shenyang |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| image.cnamedomain.com | 没有服务器地理信息. |
| ucc.umeng.com | IP: 203.119.169.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| sy.cl2m.cn | IP: 106.14.53.48  所属国家: China  地区: Shanghai  城市: Shanghai |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| wappaygw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| cgi.connect.qq.com | IP: 60.28.215.27  所属国家: China  地区: Tianjin  城市: Tianjin |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| developer.umeng.com | IP: 59.82.31.154  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| h5.duomob.com | IP: 125.39.194.43  所属国家: China  地区: Tianjin  城市: Tianjin |
| wx.tenpay.com | IP: 210.22.240.151  所属国家: China  地区: Shanghai  城市: Shanghai |
| 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 |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| xinstall.top | IP: 222.141.5.16  所属国家: China  地区: Henan  城市: Luoyang |
| auth.wosms.cn | IP: 124.64.196.27  所属国家: China  地区: Beijing  城市: Beijing |
| errlog.umeng.com | IP: 223.109.148.142  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| render.alipay.com | IP: 124.95.153.221  所属国家: China  地区: Liaoning  城市: Shenyang |
| login.imgcache.qq.com | IP: 220.194.122.222  所属国家: China  地区: Tianjin  城市: Tianjin |
| imgcache.qq.com | IP: 59.83.212.232  所属国家: China  地区: Jiangsu  城市: Wuxi |
| plbslog.umeng.com | IP: 36.156.202.73  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| wsapi.253.com | IP: 47.116.191.137  所属国家: China  地区: Shanghai  城市: Shanghai |
| cgi.qplus.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 |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| loggw-exsdk.alipay.com | IP: 110.76.6.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| open.e.189.cn | IP: 42.123.76.75  所属国家: China  地区: Beijing  城市: Beijing |
| testh5.shangbangzhuan.com | IP: 101.28.133.120  所属国家: China  地区: Hebei  城市: Handan |
| 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 |
| gateway.shangbangzhuan.com | IP: 203.107.60.10  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| yuapi.duomob.com | IP: 47.107.116.106  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| gjapplog.ucweb.com | IP: 157.185.189.158  所属国家: Canada  地区: Ontario  城市: North York |
| ulogs.umengcloud.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| huatuocode.huatuo.qq.com | 没有服务器地理信息. |
| v5.shangbangzuan.com | IP: 47.119.175.7  所属国家: China  地区: Guangdong  城市: Shenzhen |
| wspeed.qq.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| likeinstall.cn | IP: 121.199.65.132  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pre-api.ads66.com | IP: 120.76.117.171  所属国家: China  地区: Guangdong  城市: Shenzhen |
| open.weixin.qq.com | IP: 220.196.132.78  所属国家: China  地区: Jiangsu  城市: Zhenjiang |
| mobilegw.alipay.com | IP: 203.209.255.238  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogsus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Singapore  地区: Singapore  城市: Singapore |
| picsum.photos | IP: 104.26.5.30  所属国家: United States of America  地区: California  城市: San Francisco |
| sdk-logs-prod.oss-cn-hangzhou.aliyuncs.com | IP: 101.67.61.184  所属国家: China  地区: Zhejiang  城市: Huzhou |
| t-api.ads66.com | IP: 47.104.82.180  所属国家: China  地区: Shandong  城市: Qingdao |
| ns.adobe.com | 没有服务器地理信息. |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Beijing  城市: Beijing |
| h5.m.taobao.com | IP: 125.38.11.98  所属国家: China  地区: Tianjin  城市: Tianjin |
| chuanyejinxuan.xyz | IP: 116.142.237.86  所属国家: China  地区: Beijing  城市: Beijing |
| fs.cl2009.com | IP: 47.101.5.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| preh5.shangbangzhuan.com | IP: 101.28.133.115  所属国家: China  地区: Hebei  城市: Handan |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.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 |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/cons/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/cons/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/cons/a.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/cons/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/cons/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/data/a.java |
| https://auth.wosms.cn/html/oauth/protocol2.html | com/chuanglan/shanyan\_sdk/OneKeyLoginManager.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/chuanglan/shanyan\_sdk/OneKeyLoginManager.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/chuanglan/shanyan\_sdk/OneKeyLoginManager.java |
| https://auth.wosms.cn/html/oauth/protocol2.html | com/chuanglan/shanyan\_sdk/view/ShanYanOneKeyActivity.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/chuanglan/shanyan\_sdk/view/ShanYanOneKeyActivity.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/chuanglan/shanyan\_sdk/view/ShanYanOneKeyActivity.java |
| https://wap.cmpassport.com/resources/html/contract.html | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | com/cmic/gen/sdk/view/GenLoginAuthActivity.java |
| https://wsapi.253.com/plat\_app/ | com/jingmeng/sdk/android/alive/constants/RequestUrls.java |
| http://schemas.android.com/apk/res/android | com/jingmeng/sdk/android/alive/ui/widget/GifImageView.java |
| https://wsapi.253.com/sdk-log/sdk/log/appLogReport | com/jingmeng/sdk/android/base/listener/CommonInterface.java |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/c.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/c.java |
| https://openmobile.qq.com/oauth2.0/me | com/tencent/connect/UnionInfo.java |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | com/tencent/connect/common/BaseApi.java |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | com/tencent/connect/common/BaseApi.java |
| https://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 |
| https://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 |
| https://imgcache.qq.com/qcloud/public/static// | com/tencent/liteav/login/ProfileManager.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://picsum.photos/id/%d/200/200 | com/tencent/qcloud/tim/uikit/modules/group/info/GroupInfoLayout.java |
| https://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html? | com/tencent/open/SocialApiIml.java |
| https://login.imgcache.qq.com | com/tencent/open/SocialApiIml.java |
| https://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://wspeed.qq.com/w.cgi | com/tencent/open/a/g.java |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | com/tencent/open/a/g.java |
| https://huatuocode.huatuo.qq.com | com/tencent/open/a/d.java |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/g.java |
| https://cgi.qplus.com/report/report | com/tencent/open/utils/l.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://gjapplog.ucweb.com/collect | com/uc/crashsdk/a/h.java |
| https://applog.uc.cn/collect | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com/api/crashsdk/validate | com/uc/crashsdk/a/d.java |
| https://ucc.umeng.com/v1/fetch | com/umeng/analytics/pro/ah.java |
| https://pslog.umeng.com/ablog | com/umeng/analytics/pro/ah.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/h.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.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://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://h5.17xianwan.com/dailybonus? | com/xianwan/sdklibrary/constants/Constants.java |
| https://h5.17xianwan.com/try/try\_cpl\_plus? | com/xianwan/sdklibrary/constants/Constants.java |
| https://h5.17xianwan.com/try/try\_list\_plus? | com/xianwan/sdklibrary/constants/Constants.java |
| https://h5.17xianwan.com/try/try\_cpl\_strategy.aspx? | com/xianwan/sdklibrary/constants/Constants.java |
| https://h5.17xianwan.com/try/try\_list\_plus?adlisttype=1 | com/xianwan/sdklibrary/constants/Constants.java |
| https://h5.17xianwan.com/try/try\_list\_plus?adlisttype=2 | com/xianwan/sdklibrary/constants/Constants.java |
| http://newwoly.jiutaoleyuan.com/?code=50000 | com/zx/core/code/v2/activity/TestPosterActivity.java |
| http://%s:%d/%s | com/zx/core/code/v2/activity/VideoActivity.java |
| https://gateway.shangbangzhuan.com/ | com/zx/core/code/v2/activity/EnvironmentActivity.java |
| https://m.shangbangzhuan.com/ | com/zx/core/code/v2/activity/EnvironmentActivity.java |
| https://v5.shangbangzuan.com/ | com/zx/core/code/v2/activity/EnvironmentActivity.java |
| https://testh5.shangbangzhuan.com/ | com/zx/core/code/v2/activity/EnvironmentActivity.java |
| https://preh5.shangbangzhuan.com/ | com/zx/core/code/v2/activity/EnvironmentActivity.java |
| https://gateway.shangbangzhuan.com/ | com/zx/core/code/activity/StartActivity.java |
| https://v5.shangbangzuan.com/ | com/zx/core/code/activity/ConsoleActivity.java |
| https://pre.shangbangzhuan.com/ | com/zx/core/code/activity/ConsoleActivity.java |
| https://gateway.shangbangzhuan.com/ | com/zx/core/code/activity/ConsoleActivity.java |
| http://sparegateway.shangbangzhuan.com | com/zx/core/code/activity/ConsoleActivity.java |
| http://chuanyejinxuan.xyz/commonImages/business\_icon.jpg | com/zx/core/code/activity/BusinessActivity.java |
| http://a.shangbangzuan.com:81 | com/zx/core/code/activity/ManagerCenterActivity\_ViewBinding.java |
| https://v5.shangbangzuan.com/ | com/yjhb/android/feibang/App.java |
| https://chuanyejinxuan.xyz | f/a/a/a/a/f/c/h2.java |
| https://gateway.shangbangzhuan.com/ | f/a/a/a/l/z.java |
| https://chuanyejinxuan.xyz | f/a/a/a/l/z.java |
| https://pre.shangbangzhuan.com/ | f/a/a/a/l/g0.java |
| https://gateway.shangbangzhuan.com/ | f/a/a/a/l/g0.java |
| https://v5.shangbangzuan.com/ | f/a/a/a/o/j0.java |
| https://testh5.shangbangzhuan.com/ | f/a/a/a/o/j0.java |
| https://m.shangbangzhuan.com/ | f/a/a/a/o/j0.java |
| https://v5.shangbangzuan.com/ | f/a/a/a/m/b.java |
| https://pre.shangbangzhuan.com/ | f/a/a/a/m/b.java |
| http://chuanyejinxuan.xyz/commonImages/business\_icon.jpg | f/a/a/a/c/s1.java |
| https://sy.cl2m.cn/flash/thin/accountInit/v3 | f/f/b/a/d.java |
| https://sy.cl2m.cn/flash/accountInit/v4 | f/f/b/a/d.java |
| https://wap.cmpassport.com/resources/html/contract.html | f/f/b/a/a.java |
| https://wap.cmpassport.com/resources/html/contract.html | f/f/b/f/t.java |
| https://auth.wosms.cn/html/oauth/protocol2.html | f/f/b/f/t.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | f/f/b/f/t.java |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | f/f/b/f/u.java |
| https://fs.cl2009.com/flash/thin/accountInit/v3 | f/f/b/f/r.java |
| https://fs.cl20 | f/f/b/f/r.java |
| https://auth.wosms.cn/html/oauth/protocol2.html | f/f/b/f/v.java |
| https://sysdk.cl2009.com/log/fdr/v3 | f/f/b/f/n.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | f/h/a/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | f/h/a/h.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | f/h/a/h.java |
| https://github.com/danikula/AndroidVideoCache/issues. | f/h/a/h.java |
| http://%s:%d/%s | f/h/a/k.java |
| https://h5.duomob.com/ | f/i/a/a/e/q.java |
| http://t-api.ads66.com/ | f/i/a/a/e/q.java |
| http://pre-api.ads66.com/ | f/i/a/a/e/q.java |
| https://yuapi.duomob.com/domains/list.json | f/i/b/b/g/b.java |
| https://yuapi.duomob.com/domains/fail\_log.php | f/i/b/b/b/a.java |
| https://wx.tenpay.com | f/i/b/b/a/m.java |
| https://wsapi.253.com/plat\_app/platform/app/commonSdk/querySdkUpdates | f/m/a/a/b/d/c.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | f/q/a/l0/a.java |
| https://sdk-logs-prod.oss-cn-hangzhou.aliyuncs.com | f/v/a/a/a.java |
| https://likeinstall.cn | f/v/a/a/f/c.java |
| https://xinstall.top | f/v/a/a/f/c.java |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | cn/com/chinatelecom/account/api/d/g.java |
| https://api-e189.21cn.com/gw/client/accountMsg.do | cn/com/chinatelecom/account/api/d/g.java |
| http://ns.adobe.com/xap/1.0/\u0000 | n/m/a/a.java |
| http://)?([\\w-]+\\.)+[\\w-]+(:\\d+)\*(/[\\w- | p/a/a/j/g.java |
| http://xml.apache.org/xslt | p/a/a/m/m.java |
| http://www.slf4j.org/codes.html | v/d/c.java |
| https://m.playmy.cn/View/Wall\_AdList.aspx? | jfq/wowan/com/myapplication/WowanIndex.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | 摸瓜V3引擎 |
| https://ucc.umeng.com/v1/fetch | 摸瓜V3引擎 |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| https://github.com/danikula/AndroidVideoCache/issues. | 摸瓜V3引擎 |
| https://h5.17xianwan.com/dailybonus? | 摸瓜V3引擎 |
| https://gjapplog.ucweb.com/collect | 摸瓜V3引擎 |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | 摸瓜V3引擎 |
| http://sparegateway.shangbangzhuan.com | 摸瓜V3引擎 |
| https://wsapi.253.com/plat\_app/platform/app/commonSdk/querySdkUpdates | 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 |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | 摸瓜V3引擎 |
| https://preh5.shangbangzhuan.com/ | 摸瓜V3引擎 |
| https://sysdk.cl2009.com/log/fdr/v3 | 摸瓜V3引擎 |
| https://wap.cmpassport.com/resources/html/contract.html | 摸瓜V3引擎 |
| https://mobilegw.alipay.com/mgw.htm | 摸瓜V3引擎 |
| https://m.shangbangzhuan.com/ | 摸瓜V3引擎 |
| http://xml.apache.org/xslt | 摸瓜V3引擎 |
| http://mclient.alipay.com/home/exterfaceAssign.htm | 摸瓜V3引擎 |
| https://mclient.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| http://wappaygw.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://h5.17xianwan.com/try/try\_cpl\_plus? | 摸瓜V3引擎 |
| https://mclient.alipay.com/home/exterfaceAssign.htm | 摸瓜V3引擎 |
| http://t-api.ads66.com/ | 摸瓜V3引擎 |
| https://render.alipay.com/p/s/i?scheme=%s | 摸瓜V3引擎 |
| https://errlog.umeng.com/upload | 摸瓜V3引擎 |
| https://picsum.photos/id/%d/200/200 | 摸瓜V3引擎 |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version? | 摸瓜V3引擎 |
| https://pslog.umeng.com/ablog | 摸瓜V3引擎 |
| https://likeinstall.cn | 摸瓜V3引擎 |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | 摸瓜V3引擎 |
| https://openmobile.qq.com/oauth2.0/m\_authorize? | 摸瓜V3引擎 |
| https://h5.17xianwan.com/try/try\_list\_plus? | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android(v | 摸瓜V3引擎 |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | 摸瓜V3引擎 |
| https://mcgw.alipay.com/sdklog.do | 摸瓜V3引擎 |
| http://image.cnamedomain.com | 摸瓜V3引擎 |
| https://openmobile.qq.com/v3/user/get\_info | 摸瓜V3引擎 |
| https://errlog.umeng.com/api/crashsdk/validate | 摸瓜V3引擎 |
| https://fs.cl2009.com/flash/thin/accountInit/v3 | 摸瓜V3引擎 |
| https://openmobile.qq.com/user/user\_login\_statis | 摸瓜V3引擎 |
| https://m.playmy.cn/View/Wall\_AdList.aspx? | 摸瓜V3引擎 |
| https://wappaygw.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | 摸瓜V3引擎 |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi | 摸瓜V3引擎 |
| https://v5.shangbangzuan.com/ | 摸瓜V3引擎 |
| https://openmobile.qq.com/oauth2.0/me | 摸瓜V3引擎 |
| https://open.e.189.cn/openapi/special/getTimeStamp.do | 摸瓜V3引擎 |
| https://mclient.alipay.com/cashier/mobilepay.htm | 摸瓜V3引擎 |
| http://pre-api.ads66.com/ | 摸瓜V3引擎 |
| http://mclient.alipay.com/service/rest.htm | 摸瓜V3引擎 |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | 摸瓜V3引擎 |
| http://chuanyejinxuan.xyz/commonImages/business\_icon.jpg | 摸瓜V3引擎 |
| https://github.com/danikula/AndroidVideoCache/issues/88. | 摸瓜V3引擎 |
| https://gateway.shangbangzhuan.com/ | 摸瓜V3引擎 |
| https://wspeed.qq.com/w.cgi | 摸瓜V3引擎 |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html? | 摸瓜V3引擎 |
| https://yuapi.duomob.com/domains/fail\_log.php | 摸瓜V3引擎 |
| https://github.com/danikula/AndroidVideoCache/issues/134. | 摸瓜V3引擎 |
| https://imgcache.qq.com/qcloud/public/static// | 摸瓜V3引擎 |
| http://mclient.alipay.com/cashier/mobilepay.htm | 摸瓜V3引擎 |
| https://fs.cl20 | 摸瓜V3引擎 |
| http://mobilegw.aaa.alipay.net/mgw.htm | 摸瓜V3引擎 |
| https://wx.tenpay.com | 摸瓜V3引擎 |
| https://pre.shangbangzhuan.com/ | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://yuapi.duomob.com/domains/list.json | 摸瓜V3引擎 |
| https://h5.m.taobao.com/mlapp/olist.html | 摸瓜V3引擎 |
| http://newwoly.jiutaoleyuan.com/?code=50000 | 摸瓜V3引擎 |
| https://testh5.shangbangzhuan.com/ | 摸瓜V3引擎 |
| http://a.shangbangzuan.com:81 | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#replay | 摸瓜V3引擎 |
| http://127.0.0.1 | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#multiple\_bindings | 摸瓜V3引擎 |
| HTTP://WEBADDRESS.ELIDED | 摸瓜V3引擎 |
| https://chuanyejinxuan.xyz | 摸瓜V3引擎 |
| https://auth.wosms.cn/html/oauth/protocol2.html | 摸瓜V3引擎 |
| https://h5.17xianwan.com/try/try\_cpl\_strategy.aspx? | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#version\_mismatch | 摸瓜V3引擎 |
| https://developer.umeng.com/docs/66632/detail/ | 摸瓜V3引擎 |
| https://xinstall.top | 摸瓜V3引擎 |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#StaticLoggerBinder | 摸瓜V3引擎 |
| https://api-e189.21cn.com/gw/client/accountMsg.do | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#unsuccessfulInit | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android00org.sufficientlysecure.htmltextview.HtmlTextView | 摸瓜V3引擎 |
| http://mobilegw.stable.alipay.net/mgw.htm | 摸瓜V3引擎 |
| https://wsapi.253.com/sdk-log/sdk/log/appLogReport | 摸瓜V3引擎 |
| https://huatuocode.huatuo.qq.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| http://www.slf4j.org/codes.html#substituteLogger | 摸瓜V3引擎 |
| http://developer.umeng.com/docs/66650/cate/66650 | 摸瓜V3引擎 |
| https://applog.uc.cn/collect | 摸瓜V3引擎 |
| http://oss.aliyuncs.com | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided | com/tencent/liteav/base/PiiElider.java |
| danikula@gmail.com | f/h/a/h.java |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=CN, ST=chongqing, L=chongqing, O=youjiuhubang, OU=youjiuhubang, CN=youjiuhubang 签名算法: rsassa\_pkcs1v15 有效期自: 2022-01-25 02:29:58+00:00 有效期至: 2047-01-19 02:29:58+00:00 发行人: C=CN, ST=chongqing, L=chongqing, O=youjiuhubang, OU=youjiuhubang, CN=youjiuhubang 序列号: 0x1409c801 哈希算法: sha256 md5值: fb06715c725907f075063cbece308e7a sha1值: 1c99d5ffc5563bf7c5f3bbb86b7b5b5cb179b5af sha256值: cbdfcf054a87cf02038a8b864be02cb16d2eb13dae7f1299c5a1fe15b18bfca6 sha512值: f8c1d272a01bc01b8f6b9f69349ed24dc639fd17e1aecc5a39de660e0757de1eaeab9c5cb2a24334b464d8f94381eb88befd58263fa61a1d0c478d9f74e05f33 公钥算法: rsa 密钥长度: 2048 指纹: 772d763ce11cbb4f4e0f463033fb246ce06a8cd7a039f7670d89d695116ba22f**

## **6. 硬编码敏感信息**

## **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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.READ\_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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.identifier.permission.OAID\_STATE\_DIALOG | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.zx.core.code.activity.StartActivity | **Schemes**: xio2cq783://, |
| com.zx.core.code.v2.activity.JDActivity | **Schemes**: jiubang://,  **Hosts:** pay.jd, |
| com.tencent.tauth.AuthActivity | **Schemes**: \ 101906140://, |

**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。**