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

**消除星星乐（ 2.4.8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 | 消除星星乐 |
| 版本 | 2.4.8 |
| 包名 | com.pfu.xcxxl.vivo |
| 域名线索 | 70条 |
| URL线索 | 81条 |
| APP图标 |  |
| 分析日期 | 2025年8月27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 | 消除星星乐.apk |
| 文件大小 | 58.93MB |
| MD5值 | 62ec2f486593da19ab865e6d896ff86c |
| SHA1值 | d95c0ccfc9e05b91c36d394819c3435bf7b2657e |
| SHA256值 | 908d03d9cb321cf5ef535c44a74712e85839da30f7851e9b81043030ee4fa0ee |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 消除星星乐 |
| 包名 | com.pfu.xcxxl.vivo |
| 主活动Activity | com.pfu.xcxxl.permission.PermissionActivity |
| 安卓版本名称 | 2.4.8 |
| 安卓版本 | 1248 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| m.worldwy.cn | IP: 47.98.211.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h5.jfydgame.com | IP: 47.110.167.79 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| usrsysjoint.vivo.com.cn | IP: 123.126.38.57 所属国家: China 地区: Beijing 城市: Beijing  |
| 100000189777.retail.n.weimob.com | IP: 212.64.63.139 所属国家: China 地区: Beijing 城市: Beijing  |
| www.facebook.com | IP: 108.160.167.174 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| adsdk.vivo.com.cn | IP: 123.125.243.253 所属国家: China 地区: Beijing 城市: Beijing  |
| ulog-sdk.gifshow.com | IP: 103.102.202.158 所属国家: China 地区: Beijing 城市: Beijing  |
| open.e.kuaishou.com | IP: 116.136.162.35 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| purl.eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| risk-fp-openapi.vivo.com.cn | IP: 101.237.1.44 所属国家: China 地区: Shanghai 城市: Shanghai  |
| i.snssdk.com | IP: 61.182.131.160 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| topic.vivo.com.cn | IP: 42.236.8.94 所属国家: China 地区: Henan 城市: Zhengzhou  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| cdn.jsdelivr.net | IP: 104.16.88.20 所属国家: United States of America 地区: California 城市: San Francisco  |
| joint-account.vivo.com.cn | IP: 61.156.44.10 所属国家: China 地区: Shandong 城市: Xintai  |
| www.samsungapps.com | IP: 52.48.119.222 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| open.weixin.qq.com | IP: 223.167.82.219 所属国家: China 地区: Shanghai 城市: Shanghai  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| s.e.kuaishou.com | IP: 103.102.202.80 所属国家: China 地区: Beijing 城市: Beijing  |
| qzs.qq.com | IP: 119.188.155.60 所属国家: China 地区: Shandong 城市: Jinan  |
| appstore.vivo.com.cn | IP: 115.56.90.63 所属国家: China 地区: Henan 城市: Jiaozuo  |
| sdk.e.qq.com | IP: 220.194.116.72 所属国家: China 地区: Tianjin 城市: Tianjin  |
| shop.vivo.com.cn | IP: 115.56.90.190 所属国家: China 地区: Henan 城市: Jiaozuo  |
| apps.bytesfield.com | IP: 121.29.30.191 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| ssp.vivo.com.cn | IP: 115.56.90.190 所属国家: China 地区: Henan 城市: Jiaozuo  |
| eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| win.gdt.qq.com | IP: 220.194.116.80 所属国家: China 地区: Tianjin 城市: Tianjin  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| heycam.github.io | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| appdetailh5.vivo.com.cn | IP: 101.72.251.93 所属国家: China 地区: Hebei 城市: Langfang  |
| ro.usdk.vivo.com.cn | IP: 101.72.224.58 所属国家: China 地区: Hebei 城市: Langfang  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| qzs.gdtimg.com | IP: 60.221.73.196 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.cocos.com | IP: 125.39.165.87 所属国家: China 地区: Tianjin 城市: Tianjin  |
| promotion-partner.kuaishou.com | IP: 103.107.219.8 所属国家: China 地区: Beijing 城市: Beijing  |
| f.up.vivo.com.cn | IP: 39.97.158.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tdid.m.qq.com | IP: 60.29.240.40 所属国家: China 地区: Tianjin 城市: Tianjin  |
| pslog.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ucc.umeng.com | IP: 203.119.169.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apps.oceanengine.com | IP: 42.236.86.222 所属国家: China 地区: Henan 城市: Zhengzhou  |
| qzonestyle.gtimg.cn | IP: 119.167.180.241 所属国家: China 地区: Shandong 城市: Qingdao  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| imgcache.qq.com | IP: 61.49.23.182 所属国家: China 地区: Beijing 城市: Beijing  |
| apps.samsung.com | IP: 123.157.77.120 所属国家: China 地区: Zhejiang 城市: Zhoushan  |
| static.yximgs.com | IP: 114.66.246.207 所属国家: China 地区: Beijing 城市: Beijing  |
| wifi.vivo.com.cn | IP: 61.156.44.10 所属国家: China 地区: Shandong 城市: Xintai  |
| joint.vivo.com.cn | IP: 101.72.251.93 所属国家: China 地区: Hebei 城市: Langfang  |
| st-offlinegame.vivo.com.cn | IP: 123.125.243.228 所属国家: China 地区: Beijing 城市: Beijing  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| sf6-ttcdn-tos.pstatp.com | IP: 103.3.115.129 所属国家: China 地区: Zhejiang 城市: Taizhou  |
| aaid.umeng.com | IP: 223.109.148.171 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.khronos.org | IP: 104.236.24.254 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| v.gdt.qq.com | IP: 220.194.116.38 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.saxproject.org | IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pay.vivo.com.cn | IP: 101.237.1.85 所属国家: China 地区: Shanghai 城市: Shanghai  |
| graph.facebook.com | IP: 202.160.128.203 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| api.dhhdft.cn | IP: 47.98.211.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| androidquery.appspot.com | IP: 69.50.221.20 所属国家: United States of America 地区: Arizona 城市: Phoenix  |
| gamegateway.vivo.com.cn | IP: 116.136.133.140 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| api.twitter.com | IP: 74.86.151.167 所属国家: United States of America 地区: California 城市: San Jose  |
| st-onlinegame.vivo.com.cn | IP: 123.125.243.229 所属国家: China 地区: Beijing 城市: Beijing  |
| dom.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://androidquery.appspot.com  | com/androidquery/service/MarketService.java  |
| https://api.twitter.com/oauth/access\_token  | com/androidquery/auth/TwitterHandle.java  |
| https://api.twitter.com/oauth/authorize  | com/androidquery/auth/TwitterHandle.java  |
| https://api.twitter.com/oauth/request\_token  | com/androidquery/auth/TwitterHandle.java  |
| https://graph.facebook.com/oauth/authorize  | com/androidquery/auth/FacebookHandle.java  |
| https://www.facebook.com/connect/login\_success.html  | com/androidquery/auth/FacebookHandle.java  |
| https://graph.facebook.com/oauth/authorize?  | com/androidquery/auth/FacebookHandle.java  |
| https://graph.facebook.com/me  | com/androidquery/auth/FacebookHandle.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/d/a.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/d/a.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/i/c.java  |
| https://m.worldwy.cn:8091/api/V5\_Medium  | com/game/officialad/e/d.java  |
| https://m.worldwy.cn:8091/api/Device  | com/game/officialad/e/d.java  |
| https://m.worldwy.cn:8091/api/Total  | com/game/officialad/e/d.java  |
| https://api.dhhdft.cn:8092/api/V5\_Medium  | com/game/officialad/e/d.java  |
| https://api.dhhdft.cn:8092/api/Device  | com/game/officialad/e/d.java  |
| https://api.dhhdft.cn:8092/api/Total  | com/game/officialad/e/d.java  |
| http://xml.apache.org/xslt  | com/game/officialad/utils/GCAdLogUtil.java  |
| http://xml.apache.org/xslt  | com/game/officialad/utils/GCLogUtil.java  |
| https://static.yximgs.com/udata/pkg/commercial\_res\_test/ks\_so-TachikomaArm64v8aRelease-3.3.13.apk  | com/kwad/c/a/a.java  |
| https://static.yximgs.com/udata/pkg/commercial\_res\_test/ks\_so-TachikomaArmeabiv7aRelease-3.3.13.apk  | com/kwad/c/a/a.java  |
| https://promotion-partner.kuaishou.com/rest/n/promotion/p?adid=7348&imei=\_\_IMEI2\_\_&idfa=\_\_IDFA2\_\_&oaid=\_\_OAID\_\_&ip=\_\_IP\_\_&mac=\_\_MAC2\_\_&androidId=\_\_ANDROIDID2\_\_&callback=\_\_CALLBACK\_\_&siteSet=XXX  | com/kwad/components/core/ec/model/EcKwaiInfo.java  |
| https://open.e.kuaishou.com  | com/kwad/sdk/b.java  |
| https://s.e.kuaishou.com  | com/kwad/sdk/b.java  |
| https://open.e.kuaishou.com/rest/e/v3/open/sdk2  | com/kwad/sdk/api/loader/Loader.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArm64v8aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-appStatusArmeabiv7aRelease-3.3.14.apk  | com/kwad/sdk/collector/d.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/kwad/sdk/core/videocache/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/kwad/sdk/core/videocache/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/kwad/sdk/core/videocache/h.java  |
| http://%s:%d/%s  | com/kwad/sdk/core/videocache/f.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArm64v8aRelease-3.3.23.apk  | com/kwad/sdk/crash/f.java  |
| https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks\_so-exceptionArmeabiv7aRelease-3.3.23.apk  | com/kwad/sdk/crash/f.java  |
| https://ulog-sdk.gifshow.com/rest/log/sdk/file/token  | com/kwad/sdk/crash/report/upload/c.java  |
| https://ulog-sdk.gifshow.com/rest/log/sdk/file/upload  | com/kwad/sdk/crash/report/upload/b.java  |
| http://apps.samsung.com/appquery/appDetail.as?appId=  | com/kwad/sdk/utils/d.java  |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | com/kwai/filedownloader/services/a.java  |
| https://gamegateway.vivo.com.cn/gateway/developer/game/publish/v1/getOnlineVersion  | com/pfu/xcxxl/vivo/XcXxlActivity.java  |
| https://h5.jfydgame.com/proto/wuxi-agreement.html  | com/pfu/xcxxl/permission/PermissionActivity.java  |
| https://h5.jfydgame.com/proto/wuxi-privacy.html  | com/pfu/xcxxl/permission/PermissionActivity.java  |
| https://sdk.e.qq.com/activate  | com/qq/e/comm/b/a.java  |
| https://sdk.e.qq.com/launch  | com/qq/e/comm/b/a.java  |
| http://sdk.e.qq.com  | com/qq/e/comm/plugin/B/g.java  |
| http://sdk.e.qq.com/disp  | com/qq/e/comm/plugin/B/g.java  |
| http://sdk.e.qq.com/click  | com/qq/e/comm/plugin/B/g.java  |
| http://sdk.e.qq.com/msg  | com/qq/e/comm/plugin/B/g.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/tempMob.html  | com/qq/e/comm/plugin/E/d.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/videoPlay.html  | com/qq/e/comm/plugin/E/d.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/videoPlay.js  | com/qq/e/comm/plugin/E/d.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/tempMob.js  | com/qq/e/comm/plugin/E/d.java  |
| https://qzs.gdtimg.com/union/res/union\_temp\_v2/page/ANTempMob/tempMob.package.json  | com/qq/e/comm/plugin/E/d.java  |
| http://%s/%s  | com/qq/e/comm/plugin/C/a.java  |
| http://%s:%d/%s  | com/qq/e/comm/plugin/G/g.java  |
| http://%s:%d/%s  | com/qq/e/comm/plugin/G/e.java  |
| http://v.gdt.qq.com/gdt\_stats.fcg  | com/qq/e/comm/plugin/H/v/e.java  |
| http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android01/download.html  | com/qq/e/comm/plugin/apkmanager/v/a.java  |
| http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/android03/js-release/%s/native.js  | com/qq/e/comm/plugin/gdtnativead/k.java  |
| https://100000189777.retail.n.weimob.com/saas/retail/100000189777/21036777/goods/detail,https://46a79741.fyeds3.com/  | com/qq/e/comm/plugin/model/RewardADData.java  |
| http://qzs.qq.com/union/res/union\_cdn/page/images/loading\_2x.gif  | com/qq/e/comm/plugin/r/m/i.java  |
| http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkSplashAdLogo.png  | com/qq/e/comm/plugin/util/C0651h.java  |
| http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkNativeAdLogo.png  | com/qq/e/comm/plugin/util/C0651h.java  |
| http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkRewardAdLogo.png  | com/qq/e/comm/plugin/util/C0651h.java  |
| http://imgcache.qq.com/qzone/biz/gdt/dev/sdk/cdn/resources/common/SdkRewardBrowseAdLogo.png  | com/qq/e/comm/plugin/util/C0651h.java  |
| http://win.gdt.qq.com/win\_notice.fcg  | com/qq/e/comm/plugin/util/C0657n.java  |
| https://sdk.e.qq.com/mediation?version=1  | com/qq/e/comm/plugin/x/d/d.java  |
| https://sdk.e.qq.com/mediation?version=2  | com/qq/e/comm/plugin/x/d/d.java  |
| https://i.snssdk.com/  | com/ss/android/downloadad/api/constant/AdBaseConstants.java  |
| https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html  | com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java  |
| https://apps.oceanengine.com/customer/api/app/pkg\_info?  | com/ss/android/downloadlib/addownload/compliance/b.java  |
| https://www.samsungapps.com/appquery/appDetail.as?appId=  | com/ss/android/downloadlib/g/h.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://tdid.m.qq.com?mc=2  | com/tencent/turingfd/sdk/ams/au/C0679j.java  |
| https://errlogos.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/i.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/c/b.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/c/b.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.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://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://adsdk.vivo.com.cn  | com/vivo/ad/a.java  |
| http://www.w3.org/ns/ttml  | com/vivo/google/android/exoplayer3/p4.java  |
| https://wifi.vivo.com.cn/generate\_204  | com/vivo/ic/dm/p/a.java  |
| http://appstore.vivo.com.cn/appinfo/downloadApkFile?id=69112&stype=3&v\_d\_s\_f=yes&app\_version=1021&imei=865407010000009&model=vivo+X7Plus&elapsedtime=285813496&cs=0&av=23&an=6.0.1&u=150100434a4e42345207c969b41a4300&nt=WIFI&sourword=%E7%B3%97%E4%BA%8B%E7%99%BE%E7%A7%91&listpos=99&page\_index=5&target=local&cfrom=35&related=-1&update=-1&module\_id=2&v\_d\_f\_f=final&tryTime=1&s=2%7C3134493712  | com/vivo/ic/minidownload/MiniDownloader.java  |
| https://adsdk.vivo.com.cn  | com/vivo/mobilead/manager/c.java  |
| https://adsdk.vivo.com.cn  | com/vivo/mobilead/manager/f.java  |
| https://ssp.vivo.com.cn  | com/vivo/mobilead/model/a.java  |
| https://risk-fp-openapi.vivo.com.cn/deviceprofile/v4  | com/vivo/mobilead/util/q0.java  |
| https://risk-fp-openapi.vivo.com.cn/v3/cloudconf  | com/vivo/mobilead/util/q0.java  |
| https://adsdk.vivo.com.cn  | com/vivo/mobilead/util/w.java  |
| https://adsdk.vivo.com.cn  | com/vivo/mobilead/util/k0.java  |
| https://adsdk.vivo.com.cn/videoplay  | com/vivo/mobilead/util/k0.java  |
| https://shop.vivo.com.cn/wap  | com/vivo/mobilead/util/j.java  |
| https://adsdk.vivo.com.cn  | com/vivo/mobilead/web/VivoADSDKWebView.java  |
| https://adsdk.vivo.com.cn/clickinh5  | com/vivo/mobilead/web/VivoADSDKWebView.java  |
| https://joint.vivo.com.cn/game-subaccount-login  | com/vivo/sdkplugin/a.java  |
| https://topic.vivo.com.cn/joint/TP32em3gbsibi0/index.html  | com/vivo/sdkplugin/h/i.java  |
| http://ro.usdk.vivo.com.cn  | com/vivo/unionsdk/l.java  |
| http://f.up.vivo.com.cn  | com/vivo/unionsdk/l.java  |
| https://pay.vivo.com.cn  | com/vivo/unionsdk/l.java  |
| https://joint-account.vivo.com.cn  | com/vivo/unionsdk/l.java  |
| https://joint.vivo.com.cn  | com/vivo/unionsdk/l.java  |
| https://joint.vivo.com.cn/ops/allowChannelInfo  | com/vivo/unionsdk/a/f.java  |
| https://joint.vivo.com.cn/game-subaccount-login  | com/vivo/unionsdk/c/i.java  |
| https://usrsysjoint.vivo.com.cn/realNameAuth/isAuthed  | com/vivo/unionsdk/c/d.java  |
| https://appdetailh5.vivo.com.cn/detail/1873310  | com/vivo/unionsdk/cmd/JumpUtils.java  |
| https://pay.vivo.com.cn/vcoin/wap/cashier  | com/vivo/unionsdk/d/a.java  |
| https://st-offlinegame.vivo.com.cn  | com/vivo/unionsdk/i/a.java  |
| https://st-onlinegame.vivo.com.cn  | com/vivo/unionsdk/i/a.java  |
| http://xmlpull.org/v1/doc/features.html  | com/zk/adengine/lk\_sdk/c.java  |
| http://eligrey.com  | Mogua Engine V2  |
| https://github.com/dsamarin  | Mogua Engine V2  |
| https://github.com/eligrey/Blob.js/blob/master/LICENSE.md  | Mogua Engine V2  |
| http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml  | Mogua Engine V2  |
| https://dom.spec.whatwg.org/  | Mogua Engine V2  |
| https://heycam.github.io/webidl/  | Mogua Engine V2  |
| https://github.com/taylorhakes  | Mogua Engine V2  |
| https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE  | Mogua Engine V2  |
| https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js  | Mogua Engine V2  |
| http://www.cocos.com  | Mogua Engine V2  |
| https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB\_texture\_float.txt  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml';  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace';  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html  | Mogua Engine V2  |
| http://www.w3.org/TR/REC-DOM-Level-1/ecma-script-language-binding.html  | Mogua Engine V2  |
| http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/ecma-script-binding.html  | Mogua Engine V2  |
| http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/core.html  | Mogua Engine V2  |
| http://www.w3.org/TR/REC-DOM-Level-1/level-one-core.html  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/')  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml')  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml'  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/';  | Mogua Engine V2  |
| http://www.cocos.com  | Mogua Engine V2  |
| https://www.cocos.com/  | Mogua Engine V2  |
| https://apps.bytesfield.com/download/basic/cur/edbc800db3b5b52103a1005826e95969f31bf4a7  | Mogua Engine V2  |
| https://h5.jfydgame.com/proto/agreement.html  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| .apk@classes.dex  | com/kuaishou/weapon/p0/C0196.java  |
| danikula@gmail.com  | com/kwad/sdk/core/videocache/h.java  |
| .apk@classes.dex  | com/tencent/turingfd/sdk/ams/au/p0.java  |
| wxjw2020@sina.com  | Mogua Engine V2  |
| -iuwv@7.q1 sl@lfv.klt  | Mogua Engine V2  |
| yr@v.hգfi 0@8.xb  | Mogua Engine V2  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13888888888  | Mogua Engine V2  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=pfu 签名算法: rsassa\_pkcs1v15 有效期自: 2013-07-23 02:32:08+00:00 有效期至: 2112-06-29 02:32:08+00:00 发行人: CN=pfu 序列号: 0x790ee4d6 哈希算法: sha256 md5值: fa540f8fbc53dfe062b8f8c37423c119 sha1值: 6c297528376485a05716ec0cd57db6609b738a7a sha256值: de8854bfb6558ea5c1e66b50374a8443f9e8aa568ef37ff75d4d033f0df97d98 sha512值: df007471cb0c5fe06559f3d6ea8fec5aa5075d1f5c9711c8c3bc470c02fe3cf66ef54c7611724c5d87e3088b8ffcd53366e85d56ac59e727d15e07c388e4d1c2 公钥算法: rsa 密钥长度: 2048 指纹: 8adbf1956ecbbe09b1060a892bd5730bfc2c413d539e80d1b602a3196686a14f**

## **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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| vivo.game.permission.OPEN\_JUMP\_INTENTS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.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.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_REPLACED | 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 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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 |
| 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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.pfu.xcxxl.vivo.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.pfu.xcxxl.permission.PermissionActivity | **Schemes**: game://, **Hosts:** com.pfu.xcxxl.vivo,  |
| com.vivo.unionsdk.ui.UnionActivity | **Schemes**: vivounion://, **Hosts:** union.vivo.com, **Paths:** /openjump,  |

**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。**