MoGua

火星直播 1.9.8.APK 分析报告

APP名称:	火星直播
包名:	com.xiaojie.tv
域名线索:	38条
URL线索:	30条
邮箱线索:	2条
分析日期:	2025年8月10日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.xiaochang.easylive.apk
文件大小: 7.74MB
MD5值: 0427bef20cdff246fa2935f40612eede
SHA1值: dd02f256c9f01f685a9b99f6849991cc2c194962
SHA256值: e4f903562e0d16a539c9476a3fa021768ed0e9da3c72f107c61d1dfde41fc869

APP 信息

App名称: 火星直播
包名: com.xiaojie.tv
主活动Activity: com.tv.core.main.LiveActivity
安卓版本名称: 1.9.8
安卓版本: 147

域名线索

域名	服务器信息
napi.tvmars.com	**IP**: 123.57.134.70 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
facebook.github.io	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
fb.me	**IP**: 157.240.31.35 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.374031 **经度**: 4.889690

px-intl.ucweb.com	**IP**: 157.185.188.1 **所属国家**: United States of America **地区**: California **城市**: Monrovia **纬度**: 34.142773 **经度**: -117.999565
errlog.umeng.com	**IP**: 223.109.148.143 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.openssl.org	**IP**: 23.13.92.35 **所属国家**: Malaysia **地区**: Selangor **城市**: Cyberjaya **纬度**: 2.922500 **经度**: 101.654999
schemas.android.com	没有服务器地理信息.
123.56.103.89	**IP**: 123.56.103.89 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
px.ucweb.com	**IP**: 106.8.139.15 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810001 **经度**: 114.879440
klink.volceapplog.com	**IP**: 117.34.47.240 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
ulogs.umengcloud.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
stackoverflow.com	**IP**: 151.101.1.69 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
developer.umeng.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423

alink.volceapplog.com	**IP**: 58.58.80.223 **所属国家**: China **地区**: Shandong **城市**: Yantai **纬度**: 37.533329 **经度**: 121.400002
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
aaid.umeng.com	**IP**: 218.91.197.68 **所属国家**: China **地区**: Jiangsu **城市**: Nantong **纬度**: 32.030281 **经度**: 120.874718
cdn.tvmars.com	**IP**: 150.138.98.117 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
xmlpull.org	**IP**: 74.50.61.58 **所属国家**: United States of America **地区**: Texas **城市**: Dallas **纬度**: 32.814899 **经度**: -96.879204
127.0.0.1	**IP**: 127.0.0.1 **所属国家**: **-** **地区**: **-** **城市**: **-** **纬度**: 0.000000 **经度**: 0.000000
api.tvmars.com	**IP**: 123.56.103.89 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
tobapplog.volceapplog.com	**IP**: 182.40.60.243 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

alogus.umeng.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ulogs.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ouplog.umeng.com	**IP**: 47.246.110.94 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
jquery.org	**IP**: 104.17.20.100 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
abtest.volceapplog.com	**IP**: 117.34.47.240 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.560280
ns.adobe.com	没有服务器地理信息.
sizzlejs.com	**IP**: 104.18.230.48 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
pslog.umeng.com	**IP**: 59.82.29.163 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
feross.org	**IP**: 50.116.11.184 **所属国家**: United States of America **地区**: California **城市**: Fremont **纬度**: 37.548271 **经度**: -121.988571
jquery.com	**IP**: 104.18.213.12 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
toblog.volceapplog.com	**IP**: 58.58.80.217 **所属国家**: China **地区**: Shandong **城市**: Yantai **纬度**: 37.533329 **经度**: 121.400002
databyterangers.com.cn	没有服务器地理信息.
alogsus.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.iluqi.com	**IP**: 8.218.4.6 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
errlogos.umeng.com	**IP**: 47.246.110.18 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
plbslog.umeng.com	**IP**: 36.156.202.68 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

URL线索

URL**信息**	Url**所在文件**
http://127.0.0.1:	p000/r20.java
http://%s/api/v1/plugin?module=sce	p000/r20.java
http://%s/act?tag=plugin&ver=1	p000/r20.java
http://%s:%s/playlist/huoxing/ticket/channels	p000/j80.java
http://127.0.0.1:9981/playlist/huoxing/ticket/channels	p000/j80.java
http://api.tvmars.com	p000/ff0.java
http://api.iluqi.com	p000/ff0.java
http://123.56.103.89	p000/ff0.java

http://ns.adobe.com/xap/1.0/\u0000	p000/z8.java
http://cdn.tvmars.com/new/config.json?tm=%s	p000/za0.java
https://klink.volceapplog.com/service/2/device_register/	p000/qu.java
https://klink.volceapplog.com/service/2/device_update	p000/qu.java
https://klink.volceapplog.com/service/2/app_alert_check/	p000/qu.java
https://toblog.volceapplog.com/service/2/app_log/	p000/qu.java
https://tobapplog.volceapplog.com/service/2/app_log/	p000/qu.java
https://toblog.volceapplog.com/service/2/profile/	p000/qu.java
https://toblog.volceapplog.com/service/2/log_settings/	p000/qu.java
https://abtest.volceapplog.com/service/2/abtest_config/	p000/qu.java
https://alink.volceapplog.com/service/2/attribution_data	p000/qu.java
https://alink.volceapplog.com/service/2/alink_data	p000/qu.java
http://127.0.0.1:9981/playlist/huoxing/ticket/channels	p000/i80.java
https://databyterangers.com.cn	p000/iz.java
http://xmlpull.org/v1/doc/features.html	p000/w60.java
http://127.0.0.1	p000/r.java
http://schemas.android.com/apk/res/android	p000/r.java
http://xmlpull.org/v1/doc/features.html	p000/r.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://px-intl.ucweb.com	com/uc/crashsdk/a/h.java
https://px.ucweb.com	com/uc/crashsdk/a/h.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
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.ja
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.ja

https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
http://api.tvmars.com	com/xiaojie/tv/MyApplication.java
http://napi.tvmars.com	com/xiaojie/tv/MyApplication.java
http://cdn.tvmars.com/new/agreement.txt?tm=%s	com/xiaojie/tv/product/ProductAgreementView.java
http://cdn.tvmars.com/new/faq.txt?tm=%s	com/xiaojie/tv/product/ProductFAQView.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.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://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
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
http://%s:%d	Mogua Engine V1
http://xxx	Mogua Engine V1
http://jquery.com/	Mogua Engine V2
http://sizzlejs.com/	Mogua Engine V2
http://jquery.org/license	Mogua Engine V2
https://fb.me/react-spread-deprecation	Mogua Engine V2
http://facebook.github.io/react/docs/error-decoder.html?invariant=	Mogua Engine V2
https://fb.me/react-special-props)	Mogua Engine V2
https://github.com/facebook/react/issues/3236).	Mogua Engine V2

https://fb.me/react-legacyfactory	Mogua Engine V2
https://fb.me/react-warning-keys	Mogua Engine V2
https://fb.me/react-warning-dont-call-proptypes	Mogua Engine V2
https://fb.me/react-devtools	Mogua Engine V2
https://fb.me/react-minification	Mogua Engine V2
https://fb.me/react-warning-polyfills	Mogua Engine V2
https://fb.me/react-event-pooling	Mogua Engine V2
https://fb.me/react-refs-must-have-owner).	Mogua Engine V2
http://www.w3.org/1999/xhtml	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
https://fb.me/react-invariant-dangerously-set-inner-html	Mogua Engine V2
https://fb.me/react-controlled-components	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	Mogua Engine V2
https://fb.me/react-unknown-prop%s	Mogua Engine V2
https://fb.me/invalid-aria-prop%s	Mogua Engine V2
https://github.com/zertosh/loose-envify)	Mogua Engine V2
http://stackoverflow.com/questions/30030031)	Mogua Engine V2
https://github.com/reactjs/react-redux/releases/tag/v2.0.0	Mogua Engine V2
http://feross.org>	Mogua Engine V2
http://127.0.0.1:%d/play?enc=base64&url=%s&%s	lib/armeabi-v7a/libsce.so
http://127.0.0.1	lib/armeabi-v7a/libsce.so
http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd	lib/armeabi-v7a/libsce.so
http://www.w3.org/1999/xhtml	lib/armeabi-v7a/libsce.so
http://%s/recommend?format=1	lib/armeabi-v7a/libsce.so
http://%s),	lib/armeabi-v7a/libsce.so
http://%s/channel/config? groupId=%s&type=%s&module=cde&version=%s&geo=%s&isp=%d&country=%d&province=%d&city=%d&area=%d&appid=%d&mac=%s&hwtype=%s&custid=%s&p2pLimitParam=%s&appPackage=%s&appChannel=%s&ver=%s	lib/armeabi-v7a/libsce.so

http://%s:%d	lib/armeabi-v7a/libsce.so
http://%s:%d%s/	lib/armeabi-v7a/libsce.so
http://%s:%u	lib/armeabi-v7a/libsce.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
feross@feross.org	Mogua Engine V2
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

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

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=86, ST=Beijing, L=China, O=xiaojie, OU=xiaojie, CN=xiaojie
签名算法: rsassa_pkcs1v15
有效期自: 2014-11-06 02:50:27+00:00
有效期至: 2039-10-31 02:50:27+00:00
发行人: C=86, ST=Beijing, L=China, O=xiaojie, OU=xiaojie, CN=xiaojie
序列号: 0x545ae1f3
哈希算法: sha1
md5值: 009e52b98af9a1d68ecc8aee35cd334e
sha1值: 3c0bf79984be580648f15faae4f22c234eed46c5
sha256值: 695020bfa763b529bc69d48431a8541e56657fc22119f0fc1c542765b453b8bb
sha512值: 46bd49685b305b26b83934f6cddab35cab35411dcf2d5d17854a6fe11225a1d0bc1fd9a04c6abb1d5cbcabecb673c1d16ea5fb8cc5d2c4fdd2bea84a326747d5
公钥算法: rsa
密钥长度: 1024
指纹: 634c04247c7e8676533751eb4aa0c4ed96bf7460fbc5bc544471bc24e499e885

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.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.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.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_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.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.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.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

应用内通信