MoGua

热江 1.0.5.APK 分析报告

APP名称:	热江

包名:	com.rxjh.yxaz
域名线索:	36条
URL线索:	28条
邮箱线索:	0条
分析日期:	2025年6月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 热血江湖.apk
文件大小: 95.64MB
MD5值: a0dfb4c3322625aa95a1b07be31b2f3c
SHA1值: 6dc1003d09b5c5fca2c84d81d9624cacbf6f230a
SHA256值: fd48d65540264d2355d8b464fb200ca99a3f91634c5a5ee165a7c4043c7b58cb

APP 信息

App名称: 热江
包名: com.rxjh.yxaz
主活动Activity: com.sjjh.view.JuHeSplashActivity
安卓版本名称: 1.0.5
安卓版本: 105

域名线索

域名	服务器信息
d.alipay.com	**IP**: 27.221.79.17 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
newapi.3975ad.com	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 223.109.148.178 **所属国家**: China **地区**: Jiangsu

ulogs.umeng.com	**城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
game.hio.cn	**IP**: 47.114.11.114 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
plbslog.umeng.com	**IP**: 36.156.202.68 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
sdk.youxin75.com	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
rxjhlogin.huanyumid.com	**IP**: 124.70.183.240 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
weixin.qq.com	**IP**: 140.207.122.206 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948

developer.umeng.com	**IP**: 59.82.29.163 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
pslog.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
test-game.hio.cn	**IP**: 47.111.206.81 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
alogus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668

	经度: 118.777992
ad.partner.gifshow.com	**IP**: 103.102.202.39 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
aaid.umeng.com	**IP**: 223.109.148.171 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
newapi.39center.com	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
astat.bugly.qcloud.com	**IP**: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
log.reyun.com	**IP**: 71.131.249.114 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 121.40.74.180 **所属国家**: China **地区**: Zhejiang

juhesdktest3.fgcq.info	**城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
adapitest.fgcq.info	**IP**: 121.40.74.180 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api.e.kuaishou.com	**IP**: 116.136.202.194 **所属国家**: China **地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
juhesdk.39api.com	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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 **纬度**: 37.774929 **经度**: -122.419418
sdkyouxin.fgcq.info	**IP**: 121.40.74.180 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

open.weixin.qq.com	**IP**: 220.196.154.28 **所属国家**: China **地区**: Jiangsu **城市**: Wuxi **纬度**: 31.569349 **经度**: 120.288788
pre-game.hio.cn	**IP**: 47.114.218.231 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
long.open.weixin.qq.com	**IP**: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
sdkyxue.fgcq.info	**IP**: 121.40.97.230 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
juhesdk.3975ad.com	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
websdk.8ah.cc	**IP**: 203.107.54.196 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou

	纬度: 30.293650 **经度**: 120.161583
ulogs.umengcloud.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
android.bugly.qq.com	**IP**: 124.95.225.169 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
www.slf4j.org	**IP**: 159.100.250.151 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790
report.3975ad.com	**IP**: 101.37.85.4 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
rqd.uu.qq.com	**IP**: 60.28.219.32 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

URL线索

URL信息	Url所在文件
https://api.e.kuaishou.com/rest/config/client/v1/open/globalId	a/a/a/a/c.java
https://ad.partner.gifshow.com/api/v2/sdk/log?token=dee6172daef74f0895c7d185956ac0a7	a/a/a/a/c.java
https://api.e.kuaishou.com/rest/config/client/v1/open/globalId	a/a/a/b/e.java
https://ad.partner.gifshow.com/api/v2/sdk/log?token=dee6172daef74f0895c7d185956ac0a7	a/a/a/b/e.java
https://api.e.kuaishou.com/rest/config/client/v1/open/sdkGatherConfig	a/a/a/b/e.java
https://sdkyxue.fgcq.info/?	com/example/universalsdk/UserCenter/UserCenterDialog.java
https://websdk.8ah.cc/?	com/example/universalsdk/UserCenter/UserCenterDialog.java
https://weixin.qq.com	com/example/universalsdk/UserCenter/UserCenterDialog.java
https://d.alipay.com	com/example/universalsdk/UserCenter/UserCenterDialog.java
https://weixin.qq.com	com/example/universalsdk/UserCenter/NewWebViewDialog.java
https://d.alipay.com	com/example/universalsdk/UserCenter/NewWebViewDialog.java
https://sdk	com/example/universalsdk/init/Controller/InitController.java
http://sdkyouxin.fgcq.info/sdk.php/	com/example/universalsdk/init/Controller/InitController.java
https://sdk.youxin75.com/sdk/NewLoveYouxin75?fromwap=1&transdata=	com/example/universalsdk/Pay/View/Payment.java

http://sdkyouxin.fgcq.info/sdk.php/NewLoveYouxin75?fromwap=1&transdata=	com/example/universalsdk/Pay/View/Payment.java
https://weixin.qq.com	com/example/universalsdk/Pay/View/Payment.java
https://d.alipay.com	com/example/universalsdk/Pay/View/Payment.java
https://test-game.hio.cn/events	com/hio/sdk/b/a/c/a.java
https://game.hio.cn/events	com/hio/sdk/b/a/c/a.java
https://pre-game.hio.cn/events	com/hio/sdk/b/a/c/a.java
https://d.alipay.com	com/sjjh/view/JuHeWebView.java
https://weixin.qq.com	com/sjjh/view/JuHeWebView.java
https://juhesdk.3975ad.com	com/sjjh/utils/JuHeConstants.java
https://newapi.3975ad.com/game/index/	com/sjjh/utils/JuHeConstants.java
https://newapi.3975ad.com/game/Package/check	com/sjjh/utils/JuHeConstants.java
https://juhesdk.39api.com	com/sjjh/utils/JuHeConstants.java
https://juhesdk	com/sjjh/utils/JuHeConstants.java
https://newapi.3975ad.com/	com/sjjh/utils/JuHeConstants.java
https://newapi.39center.com/	com/sjjh/utils/JuHeConstants.java
http://juhesdktest3.fgcq.info	com/sjjh/utils/JuHeConstants.java
http://juhesdktest3.fgcq.info/wap/pay/index	com/sjjh/utils/JuHeConstants.java
http://adapitest.fgcq.info/game/index/	com/sjjh/utils/JuHeConstants.java

http://adapitest.fgcq.info/game/Package/check	com/sjjh/utils/JuHeConstants.java
https://report.3975ad.com/sync_json/	com/hydata/tools/HyDataWebApi.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
http://log.reyun.com/	com/reyun/common/ReYunConst.java
http://log.reyun.com/receive/rest/heartbeat	com/reyun/sdk/ReYunGame.java
http://log.reyun.com/receive/pkginfo	com/reyun/utils/HttpNetworkUtil.java
http://log.reyun.com/receive/tkio/	com/reyun/utils/HttpNetworkUtil.java
http://log.reyun.com/receive/rest/	com/reyun/utils/HttpNetworkUtil.java
http://log.reyun.com/receive/track/	com/reyun/utils/HttpNetworkUtil.java
http://rxjhlogin.huanyumid.com/getLauncher.php	com/huanyu/cqssydb/UpdateActivity.java

http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.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://ulogs.umengcloud.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://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://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
https://juhesdk.3975ad.com/api/	摸瓜V2引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=13668, ST=13668, L=13668, O=13668, OU=13668, CN=13668
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-31 04:00:24+00:00
有效期至: 2123-05-07 04:00:24+00:00
发行人: C=13668, ST=13668, L=13668, O=13668, OU=13668, CN=13668
序列号: 0x92eb54c
哈希算法: sha256
md5值: cfe1880e87d2f672f44ef4e31b436f6c
sha1值: ca50f324344616763df08c9d631dc29695eb1423
sha256值: 10a6ab4a715be7a49e5db45cabe0cfc6ee375e5916e44fcfdd9bf26cf415b51f
sha512值: 9f0488c3b6a3f9df9aac9589f675d6bc6b5f80af1fc72017b608fa4cf6f99d3c54bdc5fc0922acf45390f4de3790d0ee112332f5ad873f1b0191d7e76d2235bb
公钥算法: rsa
密钥长度: 2048
指纹: a749a3d3a406594f73c92f169894a1a0aa0ca4b19022085c933a5a0429e96742

硬编码敏感信息

可能的敏感信息
"huanyu_enter_pwd" : "请输入密码"
"huanyu_enter_pwd_again" : "请再次输入密码"

"huanyu_enter_pwd_again" : "请再次输入密码"
"huanyu_enter_username" : "请输入用户名"
"huanyu_find_pwd_title" : "忘记密码"
"huanyu_forget_pwd" : "忘记密码"
"huanyu_no_password" : "密码不能为空"
"verifyUser" : "身份验证"

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

	是		

向手机申请的权限	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.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.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.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_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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.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.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.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.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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价

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.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
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.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.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.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

com.rxjh.yxaz.permission.xenv.RECEIVE	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
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.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.RESTART_PACKAGES	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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.webkit.permission.PLUGIN	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.sjjh.view.JuHeSplashActivity	Schemes: hysj.com.rxjh.yxaz://,