MoGua

金利国际 1.002.APK 分析报告

APP名称:	金利国际

包名:	com.jinliqph5.yule
域名线索:	29条
URL线索:	28条
邮箱线索:	0条
分析日期:	2025年10月29日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: jinli-v1.002-10001-1218.apk
文件大小: 41.89MB
MD5值: 91af2b6e93032ceea1a190853cfe38bf
SHA1值: f41cfb464cabeb3c56700e4a6308c841b238fd09
SHA256值: a4a6d930107737c8363b0fe0fda777a2d50dbc3c4d3d62d8f73f904d6d595c04

APP 信息

App名称: 金利国际
包名: com.jinliqph5.yule
主活动Activity: qponline.bwh5h5h5h5ngame.yule.MainActivity
安卓版本名称: 1.002
安卓版本: 1002

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 **纬度**: 39.142181 **经度**: 117.176102
dragonbones.com	**IP**: 121.36.48.123 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 60.29.240.122 **所属国家**: China **地区**: Tianjin

debugx5.qq.com	**城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
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
zaqz.vgcz3z99.xyz	没有服务器地理信息.
soft.tbs.imtt.qq.com	**IP**: 119.167.147.86 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
static.oschina.net	**IP**: 218.28.104.157 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
bjuser.jpush.cn	**IP**: 122.9.9.237 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
qa1.api.universe.nqsf9emow.com	**IP**: 148.66.57.34 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521

	经度: 114.157692
www.weilan246.com	没有服务器地理信息.
mdc.html5.qq.com	**IP**: 116.130.223.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ahfc.gaoguosoft.com	**IP**: 168.76.254.150 **所属国家**: South Africa **地区**: Free State **城市**: Bloemfontein **纬度**: -29.120939 **经度**: 26.213575
192.168.188.126	**IP**: 192.168.188.126 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

pms.mb.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
ahfc.jineryansz.com	**IP**: 104.21.1.103 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
tsis.jpush.cn	**IP**: 110.41.138.213 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
log.tbs.qq.com	**IP**: 124.95.231.218 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
open.weixin.qq.com	**IP**: 220.196.139.154 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
www.slf4j.org	**IP**: 195.15.222.169 **所属国家**: Switzerland **地区**: Geneve **城市**: Carouge **纬度**: 46.180931

	经度: 6.138709
cool.com	**IP**: 3.33.130.190 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
wup.imtt.qq.com	**IP**: 125.39.196.183 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
h5.all.nqsf9emow.com	**IP**: 148.66.57.34 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
mqqad.html5.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
qa1.api.api	没有服务器地理信息.
static2.bigstockphoto.com	**IP**: 13.33.30.69 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

23.224.201.245	**IP**: 23.224.201.245 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
182.92.20.189	**IP**: 182.92.20.189 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL**信息**	Url**所在文件**
https://tsis.jpush.cn	cn/jiguang/ae/i.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ab/b.java
http://182.92.20.189:9099/	cn/jiguang/p/a.java
https://static2.bigstockphoto.com/7/9/2/large2/297916114.jpg	com/jbl/quickpay/bean/PayInfoMsgBody.java
https://static.oschina.net/uploads/space/2015/0629/170157_rxDh_1767531.png	com/jbl/quickpay/export/UserInfo.java
http://cool.com/auth/index	com/jbl/quickpay/export/UserInfo.java
https://www.weilan246.com/images/weilan.jpg	com/jbl/quickpay/export/UserInfo.java
http://192.168.188.126:9501/im/image?serviceToken=	com/jbl/quickpay/export/UserInfo.java

https://www.weilan246.com/images/weilan.jpg	com/jbl/quickpay/export/ChatInfo.java
https://static.oschina.net/uploads/space/2015/0629/170157_rxDh_1767531.png	com/jbl/quickpay/export/ChatInfo.java
http://192.168.188.126:9501/im/image?serviceToken=	com/jbl/quickpay/export/ChatInfo.java
http://cool.com/auth/index?uid=1130610&account_type=2	com/jbl/quickpay/export/ChatInfo.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://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/i.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java

http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.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://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/a/a.java
http://www.slf4j.org/codes.html	org/c/c.java
http://h5.all.nqsf9emow.com:27799/api/app/	qponline/bwh5h5h5h5ngame/yule/b.java
http://ahfc.gaoguosoft.com:46013	qponline/bwh5h5h5h5ngame/yule/a.java
http://ahfc.jineryansz.com:46013	qponline/bwh5h5h5h5ngame/yule/a.java
http://23.224.201.245:46013	qponline/bwh5h5h5h5ngame/yule/a.java
http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	qponline/bwh5h5h5h5ngame/yule/a.java
https://github.com/egret-labs/resourcemanager/blob/master/docs/README.md	摸瓜V2引擎
http://qa$	摸瓜V2引擎
http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	摸瓜V2引擎
http://qa$	摸瓜V2引擎
http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	摸瓜V2引擎
http://qa$	摸瓜V2引擎

http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	摸瓜V2引擎
http://qa$	摸瓜V2引擎
http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	摸瓜V2引擎
http://qa$	摸瓜V2引擎
http://qa1.api.universe.nqsf9emow.com:27799	摸瓜V2引擎
http://qa$	摸瓜V2引擎
http://qa1.api.api_universe_swoole.nqsf9emow.com:27799	摸瓜V2引擎
https://zaqz.vgcz3z99.xyz/report	摸瓜V2引擎
http://dragonbones.com/\nSource	摸瓜V2引擎
https://github.com/DragonBones/	摸瓜V2引擎
https://github.com/DragonBones/Tools/	摸瓜V2引擎
https://github.com/imaya/zlib.js	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: False
v3 签名: False
找到 1 个唯一证书
主题: C=123, ST=123, L=123, O=123, OU=123, CN=123
签名算法: rsassa_pkcs1v15
有效期自: 2019-10-08 10:07:37+00:00
有效期至: 2044-10-01 10:07:37+00:00
发行人: C=123, ST=123, L=123, O=123, OU=123, CN=123
序列号: 0x4b00a962
哈希算法: sha256
md5值: 0b98abf9447cbd11f71aeb5402e903d7
sha1值: fc1dd30d6c9ff77bec3a7610670c4bace2f59c13
sha256值: 97e8729a40a3b0d8267acc670eae6f7c8db536dfc6cab730030d862b42508e1b
sha512值: fe9b4088ecf4b4a372e00e0f3226f946c7239cf7deab2855d2aa648b029b1dcc0cfdbff13771c8a9f285be165f9983f86225a37bfbe0d5a53ed2c891720800c8

🔑 硬编码敏感信息

可能的敏感信息
"alipay_pay_user" : "支付宝姓名"
"bank_pay_user" : "银行卡姓名"
"huabie_pay_user" : "收款人姓名"
"type_certificate" : "Certificate"
"wx_pay_user" : "微信姓名"
"type_certificate" : "Zertifikat"
"type_certificate" : "证书"
"type_certificate" : "Certifikát"

"type_certificate" : "Certifikát"
"type_certificate" : "Certificado"
"type_certificate" : "Сертификат"

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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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.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_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
com.jinliqph5.yule.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
qponline.bwh5h5h5h5ngame.yule.MainActivity	Schemes: tgm0zn://,

---

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。