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

**金利国际（ 1.002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 | 金利国际 |
| 版本 | 1.002 |
| 包名 | com.jinliqph5.yule |
| 域名线索 | 29条 |
| URL线索 | 28条 |
| APP图标 |  |
| 分析日期 | 2024年9月18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 | jinli-v1.002-10001-1218.apk |
| 文件大小 | 41.89MB |
| MD5值 | 91af2b6e93032ceea1a190853cfe38bf |
| SHA1值 | f41cfb464cabeb3c56700e4a6308c841b238fd09 |
| SHA256值 | a4a6d930107737c8363b0fe0fda777a2d50dbc3c4d3d62d8f73f904d6d595c04 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| dragonbones.com | IP: 121.36.48.123 所属国家: China 地区: Beijing 城市: Beijing  |
| debugx5.qq.com | IP: 60.29.240.122 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  |
| 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  |
| static.oschina.net | IP: 218.28.104.157 所属国家: China 地区: Henan 城市: Zhengzhou  |
| bjuser.jpush.cn | IP: 122.9.9.237 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| qa1.api.universe.nqsf9emow.com | IP: 148.66.57.34 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| 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  |
| ahfc.gaoguosoft.com | IP: 168.76.254.150 所属国家: South Africa 地区: Free State 城市: Bloemfontein  |
| 192.168.188.126 | IP: 192.168.188.126 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ahfc.jineryansz.com | IP: 104.21.1.103 所属国家: United States of America 地区: California 城市: San Francisco  |
| tsis.jpush.cn | IP: 110.41.138.213 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| open.weixin.qq.com | IP: 220.196.139.154 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| cool.com | IP: 3.33.130.190 所属国家: United States of America 地区: Washington 城市: Seattle  |
| wup.imtt.qq.com | IP: 125.39.196.183 所属国家: China 地区: Tianjin 城市: Tianjin  |
| h5.all.nqsf9emow.com | IP: 148.66.57.34 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| 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  |
| 23.224.201.245 | IP: 23.224.201.245 所属国家: United States of America 地区: California 城市: Los Angeles  |
| 182.92.20.189 | IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 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**

## **6. 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"  |

## **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.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 |

## **10. 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**](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。**