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

**国投机构（ null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 | 国投机构 |
| 版本 | null |
| 包名 | moidri.jgsgojjj.ousukn.jbj |
| 域名线索 | 15条 |
| URL线索 | 21条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | base2.apk |
| 文件大小 | 26.22MB |
| MD5值 | d128a85ae7061a5372872f045e404968 |
| SHA1值 | 6b7c7878e5c3d3e24a19af3e581b134c484c606f |
| SHA256值 | 4dbb55a9f20ae0773b32817b3a305dacc48643834b4cbc6e2234dd89148e9173 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 国投机构 |
| 包名 | moidri.jgsgojjj.ousukn.jbj |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | null |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cfg.imtt.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| ns.adobe.com | 没有服务器地理信息. |
| mdc.html5.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 |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| tbsrecovery.imtt.qq.com | IP: 60.28.172.40  所属国家: China  地区: Tianjin  城市: Tianjin |
| ask.dcloud.net.cn | IP: 123.125.244.13  所属国家: China  地区: Beijing  城市: Beijing |
| tbs.imtt.qq.com | IP: 119.188.44.221  所属国家: China  地区: Shandong  城市: Jinan |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| er.dcloud.io | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| m3w.cn | IP: 123.6.37.172  所属国家: China  地区: Henan  城市: Zhengzhou |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/l.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/o.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/o.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/o.java |
| https://tbsrecovery.imtt.qq.com/getconfig | com/tencent/smtt/utils/o.java |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs | com/tencent/smtt/utils/d.java |
| https://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.java |
| https://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| http://ns.adobe.com/xap/1.0/\u0000 | io/dcloud/common/util/ExifInterface.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://er.dcloud.io/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://er.dcloud.net.cn/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.java |
| https://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |

### **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: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=chengdu, ST=chengdu, L=chengdu, O=wf1714011920333, OU=fh1714011920333, CN=bjbv 签名算法: rsassa\_pkcs1v15 有效期自: 2024-04-25 02:25:20+00:00 有效期至: 2074-04-13 02:25:20+00:00 发行人: C=chengdu, ST=chengdu, L=chengdu, O=wf1714011920333, OU=fh1714011920333, CN=bjbv 序列号: 0x4e6655df 哈希算法: sha1 md5值: 4297bf447eb602a45ea6b90fede1a14d sha1值: 541da53562bf5eb57115f56325c098db4a6f981a sha256值: 57f6dd28aef543b21b606688eaea4300272d80adf9a14e718cd70f531abf1815 sha512值: 7f174c3e4aed976c7af1c58613733f9b1ea3375079bdb2a6b0a6f3ac62698aa3791546969494e071f6b8f489dd2d34c7ab9d7ee47e3bcc0f3ff181648d456975 公钥算法: rsa 密钥长度: 1024 指纹: 954c8ff26641f69a383ddf90b1bf929bfd089268d544fbf4031cdd306a220fa9**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.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.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.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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| moidri.jgsgojjj.ousukn.jbj\_com.huawei.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| moidri.jgsgojjj.ousukn.jbj\_com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| moidri.jgsgojjj.ousukn.jbj\_com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**