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

**国联尊宝（ 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 | 国联尊宝 |
| 版本 | null |
| 包名 | gkhfDhj.xufjidhuasfhh5.hlahfjkm |
| 域名线索 | 6条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年7月5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 | 国联尊宝\_gkhfDhj.xufjidhuasfhh5.hlahfjkm\_3334c9bdacc26b5dc2345c287bdc6297.apk |
| 文件大小 | 28.48MB |
| MD5值 | d1b22d52217d9bfb7d5cda19af3bcb56 |
| SHA1值 | a18bdc4ec3ff9b8600724082a3b55bd40fc0def3 |
| SHA256值 | a54f684b43cb54a144ba86f6a694fbe42bfbe8e83bec20b36bc256c959f9cdbd |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 国联尊宝 |
| 包名 | gkhfDhj.xufjidhuasfhh5.hlahfjkm |
| 主活动Activity | com.westpm.hlahl.ui.activity.SplashActivity |
| 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 |
| --- | --- |
| 172.20.10.4 | IP: 172.20.10.4  所属国家: -  地区: -  城市: - |
| 139.199.2.238 | IP: 139.199.2.238  所属国家: China  地区: Beijing  城市: Beijing |
| 52.196.130.254 | IP: 52.196.130.254  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 119.45.235.110 | IP: 119.45.235.110  所属国家: China  地区: Beijing  城市: Beijing |
| www.migu.cn | IP: 117.135.165.90  所属国家: China  地区: Shanghai  城市: Shanghai |
| 3.112.244.253 | IP: 3.112.244.253  所属国家: Japan  地区: Tokyo  城市: Tokyo |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://172.20.10.4:8080/food | com/westpm/hlahl/util/Constant.java |
| https://www.migu.cn/ilndex.html | com/westpm/hlahl/ui/activity/webActivity.java |
| https://52.196.130.254:51000/loong/ | com/westpm/hlahl/ui/activity/H5Activity.java |
| https://3.112.244.253:51000/loong/ | com/westpm/hlahl/ui/activity/H5Activity.java |
| https://139.199.2.238:12338/loong/ | com/westpm/hlahl/ui/activity/H5Activity.java |
| https://119.45.235.110:12338/loong/ | com/westpm/hlahl/ui/activity/H5Activity.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 123456789@qq.com | com/westpm/hlahl/ui/activity/OpeningActivity.java |

### **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=hknkrcqwedigqjp, ST=nxkbunjkhfmpown, L=htpvwzmcojuuswn, O=pmn1748567362483, OU=eai1748567362483, CN=Xpzo1748567362483 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-30 01:09:22+00:00 有效期至: 2075-05-18 01:09:22+00:00 发行人: C=hknkrcqwedigqjp, ST=nxkbunjkhfmpown, L=htpvwzmcojuuswn, O=pmn1748567362483, OU=eai1748567362483, CN=Xpzo1748567362483 序列号: 0x23849f1a 哈希算法: sha1 md5值: 38f55a6a7af762dd44e4effd19813f40 sha1值: 9e796346391efdb80945146ed6d151a10ae03898 sha256值: 559573ad6d3732531f253a1b49f2f10452302027b9263643db31838de740c681 sha512值: 1b227723b43279218009d2436f0832876c16bed6485ee13d187aa7350bba67fa9f72358cdc6000d342e780f0c6d4a4236d35bef8c02190e67d839e288624f47f 公钥算法: rsa 密钥长度: 1024 指纹: a221e5fda79b08b5a66f3b3335819b7510f8e4f66c5356bb590ad2f77f29cbc2**

## **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.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.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.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.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.NETWORK\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.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。 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.WRITE\_SETTINGS | 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 |

## **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。**