



MoGua

国联尊宝 null.APK 分析报告



APP名称:

国联尊宝

包名: gkhfDhj.xufjidhuasfhh5.hlahfjkm

域名线索: 6条

URL线索: 3条

邮箱线索: 1条

分析日期: 2025年7月2日

分析平台: [摸瓜APK反编译平台](#)

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: a54f684b43cb54a144ba86f6a694fbe42bfbe8e83bec20b36bc256c959f9cddb

i APP 信息

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:

🔍 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: - 纬度: 0.000000 经度: 0.000000
139.199.2.238	IP: 139.199.2.238 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
52.196.130.254	IP: 52.196.130.254 所属国家: Japan 地区: Tokyo

	城市: Tokyo 纬度: 35.689499 经度: 139.692322
119.45.235.110	IP: 119.45.235.110 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.migu.cn	IP: 117.135.165.90 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
3.112.244.253	IP: 3.112.244.253 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322

 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/ilIndex.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

 邮箱线索

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

 手机线索

 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=nxkbunjkfhmpown, L=httpwzmcojuuswn, 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=nxkbunjkfhmpown, L=httpwzmcojuuswn, 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

硬编码敏感信息

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.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
--	----	--------------------	---

应用内通信

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。