MoGua

中华国货 1.0.APK 分析报告

APP名称:	中华国货

包名:	z9sg9.w_iyh
域名线索:	16条
URL线索:	13条
邮箱线索:	1条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 中华国货.apk
文件大小: 1.9MB
MD5值: e72545a279c25ece01c2cf5140750f58
SHA1值: 0aa97ef8bf65ac67a023fd08800d353ea9cf1654
SHA256值: 81205eab6ab9768e95a9283656bcd0db0b7620ae21063d71163a4fcee9e94dfd

APP 信息

App名称: 中华国货
包名: z9sg9.w_iyh
主活动Activity: o_b7.kiz3.xgj_.p3pl
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
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
ulogs.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alogus.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu

	城市: Nanjing **纬度**: 32.061668 **经度**: 118.777992
developer.umeng.com	IP: 59.82.29.163 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
alogsus.umeng.com	IP: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
pslog.umeng.com	IP: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
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

tbs.imtt.qq.com	**IP**: 119.188.150.244 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
github.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ulogs.umengcloud.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
debugx5.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
plbslog.umeng.com	**IP**: 36.156.202.78 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221

	经度: 119.435600
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
utoken.umeng.com	**IP**: 223.109.148.139 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

URL线索

URL信息	Url所在文件
https://utoken.umeng.com/api/updateZdata/v4	com/umeng/umzid/ZIDManager.java
https://utoken.umeng.com/api/postZdata/v4	com/umeng/umzid/ZIDManager.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java

https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://alogus.umeng.com	com/umeng/commonsdk/stateless/a.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.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://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/k.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://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://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	l1/q.java

邮箱线索

邮箱地址	所在文件
x5tbs@tencent.com	com/tencent/smtt/sdk/X5Downloader.java

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=admindm21is, ST=admindm21is, L=admindm21is, O=admindm21is, OU=admindm21is, CN=admindm21is
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-06 08:48:08+00:00
有效期至: 2125-04-12 08:48:08+00:00
发行人: C=admindm21is, ST=admindm21is, L=admindm21is, O=admindm21is, OU=admindm21is, CN=admindm21is
序列号: 0x7e756ca0
哈希算法: sha256
md5值: 2631ac214c08a841ee7beeb15908458d
sha1值: 261bb27016f8a792e722db05bd97d0e92b226960
sha256值: 1579b7d8b64aae0b6c148f1f55103295e4ebbe0bf0787aaedb6812ccecb844ee
sha512值: 6c36ae7bb9d6bfe570d4c493fc74015c50ca264d01ebbb8b7d97ac4b651c9f98cb53ed0a7056bcacb31106cd6b132e95686f61b37450fe5821eeedb2f3acc72e
公钥算法: rsa

密钥长度: 1024
指纹: 0fe2ff7519abfdb3aaf0585ee2532ba39d647e79ce0ff7f22ac493ee6daebdf6

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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.MICROPHONE	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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_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.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_SETTINGS	未知	Unknown permission	Unknown permission from android reference
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.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.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
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.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
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
z9sg9.w_iyh.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
o_b7.kiz3.xgj_.p3pl	Schemes: http://, https://, about://, javascript://, inline://, tbopen://, a://, Hosts: o_b7.kiz3.browser, Mime Types: text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml, Path Prefixes: /index.html,