MoGua

红旗资本 null.APK 分析报告

APP名称:	红旗资本

包名:	net.hongqiziben.m
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年6月21日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 红旗[1].apk
文件大小: 4.39MB
MD5值: 69a027d601db37eb18145d785976432d
SHA1值: b69296c43d5f3917ea2db1428296f4bc6194d60f
SHA256值: 8af1f35c6e88bee3570028fd2b20348f91c63fa6eb80a19dc1441b9c2a2aa6ee

APP 信息

App名称: 红旗资本
包名: net.hongqiziben.m
主活动Activity: com.lt.app.MainActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
1.12.12.12	**IP**: 1.12.12.12 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.baidu.com	**IP**: 110.242.69.21 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
dns.alidns.com	**IP**: 223.6.6.6 **所属国家**: China **地区**: Zhejiang

	城市: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
https://dns.alidns.com/dns-query	m3/r.java
https://1.12.12.12/dns-query	m3/r.java
https://www.baidu.com/favicon.ico?\	l3/h1.java

邮箱线索

手机线索

签名证书

无法读取代码签名证书.

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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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。
net.hongqiziben.m.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference

net.hongqiziben.m.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.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

应用内通信
