MoGua

精准扶贫 1.0.0.APK 分析报告

APP名称:	精准扶贫

包名:	com.youlihexin.jzfpapp
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年5月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 精准扶贫[1].apk
文件大小: 5.11MB
MD5值: 32c262519e27a059954a8f2bcd8efbd3
SHA1值: 237367003876359e9e675f2d449c20520422978d
SHA256值: 8e3919b09a8c75b1d425d696447a8b80d702aaad91d1e93693a05ef4a9f5a7fc

APP 信息

App名称: 精准扶贫
包名: com.youlihexin.jzfpapp
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	服务器信息
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
www.baidu.com	**IP**: 110.242.70.57 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
1.12.12.12	**IP**: 1.12.12.12 **所属国家**: China

1.12.12.12	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

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

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, O=COM, OU=IT, CN=GZDM
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-19 07:30:27+00:00
有效期至: 2125-04-25 07:30:27+00:00

发行人: C=CN, O=COM, OU=IT, CN=GZDM
序列号: 0x196c7e6e
哈希算法: sha256
md5值: ce1469bdab2c9bf903d068f2d93bf517
sha1值: b0e6faf857b1f05fc6144c4dc053326b73648820
sha256值: aa195e2b898d818a84ecdeed6c4484325ffd3e9fc50841190efc4ac86262af64
sha512值: dbcd5d305fd8ebe3dd51f2dba8fdc2fe19b6f186fe06d3870ee96092b441c0ff2e01d8d682d1d6403a408cc6f1d3693320b9ec86ba103f8210120e50825c39b2
公钥算法: rsa
密钥长度: 2048
指纹: 347c1eab77d2b8df44cfb50e55c8e5a8eb4c8737365657dc37cb785dae8ce7a9

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

	是否		

向手机申请的权限	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。
com.youlihexin.jzfpapp.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
com.youlihexin.jzfpapp.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

活动(ACTIVITY)	**通信**(INTENT)

com.lt.app.JumpActivity	Schemes: ltapp456302://,
