MoGua

云家财富 1.0.0.APK 分析报告

APP名称:	云家财富

包名:	com.szsetk.yjcfapp
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: 云家财富.apk
文件大小: 5.11MB
MD5值: 2f73f2c1d58e860169a36da6fec7e8e0
SHA1值: a02dfe741a3a4f945e3e0ba52df2aff4d520990a
SHA256值: 5e651d482d71017c9ca079302acc8d6781e377fd6b11e383d40877679341ee1d

APP 信息

App名称: 云家财富
包名: com.szsetk.yjcfapp
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
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**: 223.5.5.5 **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://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=TLFK
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-02 15:20:54+00:00
有效期至: 2125-05-09 15:20:54+00:00
发行人: C=CN, O=COM, OU=IT, CN=TLFK

序列号: 0xbb49e5b
哈希算法: sha256
md5值: 3234e2606563adb8205025327644626c
sha1值: c632e80e68beae67dda0ea8de13c2e29336a4fa7
sha256值: 97dfcc170e4ee6452420d7c18fe47b95d4893703bdf41131a4c96c5a6a6ae7a5
sha512值: 1e67342801335e8506b07251bf235ce61856ec7b04e767050b0dd56ac9ab1381b50099976664ebb8b9bbb91620771d07a4692975e0fb12bc63a93497bafa1142
公钥算法: rsa
密钥长度: 2048
指纹: 2f7fc502cd5f1fbb881c18ec48f717b380a26fab0021f6de4f019ab3ff23c9ac

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	类型	详细情况

	险		
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.szsetk.yjcfapp.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
com.szsetk.yjcfapp.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: ltapp458993://,
