MoGua

智天国库 1.0.0.APK 分析报告

APP名称:	智天国库

包名:	cc.zhitianguoku.wapc8c
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: x463405-adr-v100-vKw.apk
文件大小: 3.78MB
MD5值: 8152f513fc3aea9cd75df438fa402a0a
SHA1值: fa86f833a066fe2500ec1bc54d3417c642cb8620
SHA256值: 9736fcff8fc6f6e8dab9cdd9477b638e63dce5968764d941bbb4317b0f828610

APP 信息

App名称: 智天国库
包名: cc.zhitianguoku.wapc8c
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=RZLX
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-16 05:40:32+00:00
有效期至: 2125-06-22 05:40:32+00:00
发行人: C=CN, O=COM, OU=IT, CN=RZLX

序列号: 0x2640a7f3
哈希算法: sha256
md5值: f012d41100b00456a6a56adeda970936
sha1值: 5bf8cb4050174042ec8b1d38ed3d3e059adbe368
sha256值: 64947e656c2135f64409b146ede499bfd404e25591a742da6f14f6e96525c2c1
sha512值: b838774b6fcef689ce5bd706d6a02de47ebf0f0f14f00968a6843289f0e4cbb73108f9b825dc4b977fe9241392d130666fae93381396bb9ead36b443d1b8cd64
公钥算法: rsa
密钥长度: 2048
指纹: c904f48f1bd631c76dab1f7ca8051d9f0cc7e611c5c409454de3348d310ad65f

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	类型	详细情况

	危险		
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。
cc.zhitianguoku.wapc8c.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
cc.zhitianguoku.wapc8c.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: ltapp464405://,
