MoGua

国窖传奇 1.0.3.APK 分析报告

APP名称:	国窖传奇

包名:	x83.x17.x124.x27
域名线索:	3条
URL线索:	2条
邮箱线索:	0条
分析日期:	2024年11月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 国窖传奇(2).apk
文件大小: 3.57MB
MD5值: ce5b70f1a4de4a7141a0de1930d83f3a
SHA1值: cc5ba5481f5da960703afab0933b8ae153621d2a
SHA256值: efc723aacd461c8785755859f23cc2f551fc915acefeef73a7e0bb42a159272f

APP 信息

App名称: 国窖传奇
包名: x83.x17.x124.x27
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 1.0.3
安卓版本: 103

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
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**: 110.242.68.4 **所属国家**: China

www.baidu.com	**地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280

URL线索

URL信息	Url所在文件
https://dns.alidns.com/dns-query	h4/q.java
https://1.12.12.12/dns-query	h4/q.java
https://www.baidu.com/favicon.ico?\	g4/f1.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=RPWC
签名算法: rsassa_pkcs1v15
有效期自: 2024-09-16 06:32:38+00:00
有效期至: 2124-08-23 06:32:38+00:00

发行人: C=CN, O=COM, OU=IT, CN=RPWC
序列号: 0x4021850
哈希算法: sha256
md5值: a421900c6a8f678953068e8be6dd71bd
sha1值: 540944f8a88dc3db1f6958a79effb301d9bafd7a
sha256值: 84df06e807833d21786b5b230f147218636a769b072a9096edf09b44afc93af2
sha512值: f7f42373db8588a327860e2e496a49be7daed06c88f6530c2d126a2e0a2270c294b1f397c87ae8be7fa0d0500ed92c35f3cc4bfd15803389fe3b2fa59b19e02c
公钥算法: rsa
密钥长度: 2048
指纹: b521d80e3c0516bea09a88356cd42c23f26694399ef8fa247dfeebd1f296d3f6

🔑 硬编码敏感信息

可能的敏感信息
"http_auth" : "HTTP Authentication"
"http_auth_p" : "Password"
"http_auth_u" : "User Name"
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""
"p_rcpush_xmAppKey" : ""
"p_weibo_appkey" : ""
"http_auth" : "HTTP 身份驗證"

"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"
"http_auth" : "HTTP 身份驗證"
"http_auth_p" : "密碼"
"http_auth_u" : "用戶名"
"http_auth" : "HTTP 身份验证"
"http_auth_p" : "密码"
"http_auth_u" : "用户名"

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。
x83.x17.x124.x27.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
x83.x17.x124.x27.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
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference

android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp428389://,
