Evaluation Warning: The document was created with Spire.Doc for Python.

**国窖传奇（ 1.0.3版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 国窖传奇 |
| 版本 | 1.0.3 |
| 包名 | x83.x17.x124.x27 |
| 域名线索 | 3条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2024年11月7日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

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

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| 1.12.12.12 | IP: 1.12.12.12 所属国家: China 地区: Beijing 城市: Beijing  |
| www.baidu.com | IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding  |

### **4.2 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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 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**

## **6. 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"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |

## **10. 应用内通信**

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

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**