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

**通城麻将（ 1.0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 | 通城麻将 |
| 版本 | 1.0 |
| 包名 | com.tongcheng.yule |
| 域名线索 | 11条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年4月3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 | 通城麻将.apk |
| 文件大小 | 43.3MB |
| MD5值 | 55b8c73647092a56b8414d4ae9a71273 |
| SHA1值 | e05ea555dd456fba3008522af2485b204deb3326 |
| SHA256值 | df99974e06b41694172648ad7152ba29d86298fbbfbae137a7ca4f46ea7d9d3e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 通城麻将 |
| 包名 | com.tongcheng.yule |
| 主活动Activity | org.cocos2dx.cpp.AppActivity |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.mch.weixin.qq.com | IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| open.weixin.qq.com | IP: 220.196.132.78 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api.weixin.qq.com | IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.baidu.com | IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding  |
| pay.heepay.com | IP: 115.182.244.184 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apple.com | IP: 2.16.184.197 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Dusseldorf  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/sdk/diffdev/a/f.java  |
| http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/sdk/diffdev/a/d.java  |
| http://mta.qq.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://mta.oa.com/  | com/tencent/wxop/stat/StatServiceImpl.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/wxop/stat/common/StatConstants.java  |
| https://api.weixin.qq.com/sns/userinfo?  | lib/armeabi/libcocos2dcpp.so  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?  | lib/armeabi/libcocos2dcpp.so  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?  | lib/armeabi/libcocos2dcpp.so  |
| https://api.mch.weixin.qq.com/pay/unifiedorder  | lib/armeabi/libcocos2dcpp.so  |
| https://pay.heepay.com/Phone/SDK/PayInit.aspx?  | lib/armeabi/libcocos2dcpp.so  |
| http://www.baidu.com  | lib/armeabi/libcocos2dcpp.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/armeabi/libcocos2dcpp.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi/libcocos2dcpp.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/armeabi/libcocos2dcpp.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2008-02-29 01:33:46+00:00 有效期至: 2035-07-17 01:33:46+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0x936eacbe07f201df 哈希算法: sha1 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569**

## **6. 硬编码敏感信息**

## **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.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.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |

## **10. 应用内通信**

**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。**