



MoGua

17麻将 1.2.5.APK 分析报告



APP名称:

17麻将

包名:	com.qiquhuyu.mj17
域名线索:	20条
URL线索:	5条
邮箱线索:	5条
分析日期:	2025年6月15日
分析平台:	摸瓜APK反编译平台

文件名: 1.apk
文件大小: 54.26MB
MD5值: 9403474d6de26e47f3a80589ff600c5b
SHA1值: 58414460bb32818bf47611530eadcd65a9e45fe9
SHA256值: c8afa8999e89190db78c6b33c2eeae72ef5402767768ef7fd262b22d767eb18

i APP 信息

App名称: 17麻将
包名: com.qiquhuyu.mj17
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 1.2.5
安卓版本: 2023111726

🔍 域名线索

域名	服务器信息
harmony.voice.gcloud.qq.com	IP: 153.3.46.72 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.khronos.org	IP: 104.236.24.254 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
dom.spec.whatwg.org	IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey

	城市: Clifton 纬度: 40.858585 经度: -74.163605
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
idcconfig.gcloudsdk.com	IP: 140.207.124.33 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.openssl.org	IP: 34.36.58.177 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
www.mp3dev.org	IP: 142.251.42.243 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
eligrey.com	IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
	IP: 140.207.124.80

tglog.gcloud.qq.com	所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
192.168.2.232	IP: 192.168.2.232 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
heycam.github.io	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.apple.com	IP: 218.58.101.229 所属国家: China 地区: Shandong 城市: Zibo 纬度: 36.790775 经度: 118.063354
www.saxproject.org	IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047

github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.cocos.com	IP: 125.39.165.87 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
cdn.jsdelivr.net	IP: 104.16.89.20 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.translator.voice.gcloud.qq.com	IP: 220.196.141.60 所属国家: China 地区: Jiangsu 城市: Xuzhou 纬度: 34.266666 经度: 117.166664
api.pr.weixin.qq.com	IP: 116.128.184.236 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
purl.eligrey.com	IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco

纬度: 37.774929

经度: -122.419418

 URL线索

URL信息	Url所在文件
http://eligrey.com	Mogua Engine V2
https://github.com/dsamarin	Mogua Engine V2
https://github.com/eligrey/Blob.js/blob/master/LICENSE.md	Mogua Engine V2
http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	Mogua Engine V2
http://www.w3.org/1999/xhtmll	Mogua Engine V2
https://dom.spec.whatwg.org/	Mogua Engine V2
https://heycam.github.io/webidl/	Mogua Engine V2
https://github.com/taylorhakes	Mogua Engine V2
https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE	Mogua Engine V2
https://cdn.jsdelivrivr.net/npm/promise-polyfill@8/dist/polyfill.js	Mogua Engine V2
http://www.cocos.com	Mogua Engine V2
https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB_texture_float.txt	Mogua Engine V2
http://www.w3.org/1999/xhtmll';	Mogua Engine V2

http://www.w3.org/XML/1998/namespace ;	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html	Mogua Engine V2
http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html	Mogua Engine V2
http://www.w3.org/TR/REC-DOM-Level-1/ecma-script-language-binding.html	Mogua Engine V2
http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/ecma-script-binding.html	Mogua Engine V2
http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/core.html	Mogua Engine V2
http://www.w3.org/TR/REC-DOM-Level-1/level-one-core.html	Mogua Engine V2
http://www.w3.org/2000/xmlns/)	Mogua Engine V2
http://www.w3.org/XML/1998/namespace	Mogua Engine V2
http://www.w3.org/1999/xhtml)	Mogua Engine V2
http://www.w3.org/1999/xhtml '	Mogua Engine V2
http://www.w3.org/2000/xmlns/ ;	Mogua Engine V2
http://www.cocos.com	Mogua Engine V2

https://www.cocos.com/	Mogua Engine V2
http://192.168.2.232:81/privacy?projectID=adang01fkc	Mogua Engine V2
https://idconfig.gcloudsdk.com	lib/armeabi-v7a/libGCloudVoice.so
https://api.translator.voice.gcloud.qq.com:443/api/v2/translator/offline	lib/armeabi-v7a/libGCloudVoice.so
https://api.translator.voice.gcloud.qq.com:443/api/v1/tts	lib/armeabi-v7a/libGCloudVoice.so
https://api.translator.voice.gcloud.qq.com:443/api/v1/ttt	lib/armeabi-v7a/libGCloudVoice.so
https://api.translator.voice.gcloud.qq.com:443/api/v1/translator/realtime	lib/armeabi-v7a/libGCloudVoice.so
https://api.translator.voice.gcloud.qq.com/api/v1/r tts	lib/armeabi-v7a/libGCloudVoice.so
https://harmony.voice.gcloud.qq.com:443/report_query	lib/armeabi-v7a/libGCloudVoice.so
https://harmony.voice.gcloud.qq.com:443/report_record	lib/armeabi-v7a/libGCloudVoice.so
https://tglog.gcloud.qq.com/tglog/report	lib/armeabi-v7a/libGCloudVoice.so
http://api.pr.weixin.qq.com/cgi-bin/wxvoicereco	lib/armeabi-v7a/libGCloudVoice.so
http://www.mp3dev.org/	lib/armeabi-v7a/libGCloudVoice.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos2djs.so
https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/libcocos2djs.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libcocos2djs.so

 邮箱线索

邮箱地址	所在文件
j1g@v.ag9	Mogua Engine V2
ᵐ@8.hig 3āzabm6@x.mm ak@ᵒ_.smj	Mogua Engine V2
i@a.fo	Mogua Engine V2
نر@e.bn ov@h.9wzt	Mogua Engine V2
minggo@a03101308207.local	lib/armeabi-v7a/libcocos2djs.so

 手机线索

手机号	所在文件
17357573465	Mogua Engine V2
17357573465	Mogua Engine V2

 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=cn, ST=fujian, L=fuzhou, O=qiquhuyu, OU=qiquhuyu, CN=qiquhuyu
签名算法: rsassa_pkcs1v15
有效期自: 2020-05-13 03:42:26+00:00
有效期至: 2075-02-14 03:42:26+00:00
发行人: C=cn, ST=fujian, L=fuzhou, O=qiquhuyu, OU=qiquhuyu, CN=qiquhuyu
序列号: 0x642c074
哈希算法: sha256
md5值: c4e40321d99d89460c18b833c1861bb8
sha1值: 60babbdf8178f550030eed1cdcd4b97f7feab44
sha256值: 7071d8af928b25a4709536666a4129a73ca4728d704478917c6925a9fd7da14b
sha512值: 9a2f0ecf051621d245e792165fd54db70053b96f8ae0e1d58752611e608efd8eb5aa58c9ec43c56443a2e3c92fde431a92e88808196d799fedcd8306d0dea903

硬编码敏感信息

可能的敏感信息
"BaiduKey" : "17mj"
"apps_flyer_key" : "17mj"
"meizu_key" : "17mj"
"oppo_key" : "17mj"
"oppo_secret" : "17mj"
"vivo_key" : ""
"weixin_key" : "wxd6b2f696f217aabf"
"xiaomi_key" : "17mj"
"yoyo_key" : ""

yaya_key .
"youmeng_key" : "6050273f6ee47d382b842c18"
"youmeng_secret" : "17mj"

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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.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.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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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。
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。

应用内通信

活动(ACTIVITY)	通信(INTENT)
org.cocos2dx.javascript.AppActivity	Schemes: @string/openscheme://,