MoGua

789娱乐城 1.1.APK 分析报告

APP名称: 789娱乐城

包名:	com.arDf8g2vRHGpRWjv5Va_nPvPTqF72ZxiIIOVcU_iV440XHBm
域名线索:	46条
URL线索:	50条
邮箱线索:	0条
分析日期:	2025年7月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 1667314815768.apk
文件大小: 40.52MB
MD5值: 63d75f78dd936f4823a9b1e193914774
SHA1值: 0593c409575155ac42e0ae74a40110cc1baf4041
SHA256值: b06ac5b23e61dff36c095336c1af2a2b8e18af0e73b4eaec9754d1cf4f62b554

APP 信息

App名称: 789娱乐城
包名: com.arDf8g2vRHGpRWjv5Va_nPvPTqF72ZxiIIOVcU_iV440XHBm
主活动Activity: com.mb.rn.activity.ReactMainActivity
安卓版本名称: 1.1
安卓版本: 2

域名线索

域名	服务器信息
spxw.mop.com	没有服务器地理信息.
mobilegw.aaa.alipay.net	没有服务器地理信息.
config.shareinstall.com.cn	**IP**: 120.46.79.149 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
ns.adobe.com	没有服务器地理信息.
oss-cn-.aliyuncs.comor	没有服务器地理信息.
	IP: 108.160.163.106

www.facebook.com	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
loggw-exsdk.alipay.com	IP: 110.76.3.1 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
plus.google.com	IP: 64.13.192.76 **所属国家**: United States of America **地区**: Arizona **城市**: Tempe **纬度**: 33.336079 **经度**: -111.922157
check.shareinstall.com.cn	IP: 120.46.79.149 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
pv.sohu.com	IP: 42.81.26.128 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
mobilegw-1-64.test.alipay.net	没有服务器地理信息.
	IP: 69.50.221.20 **所属国家**: United States of America **地区**: Arizona

codepush.azurewebsites.net	**城市**: Phoenix **纬度**: 33.682438 **经度**: -112.107254
bjuser.jpush.cn	IP: 122.9.9.237 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
mqqad.html5.qq.com	IP: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
iploc.market.alicloudapi.com	IP: 112.74.96.187 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
mobilegw.stable.alipay.net	没有服务器地理信息.
twitter.com	IP: 108.160.165.173 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
soft.tbs.imtt.qq.com	IP: 121.51.175.60 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673

	经度: 114.068108
www.pgyer.com	**IP**: 203.107.44.30 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
adsbrefrigerator.tt.cn	**IP**: 152.136.6.37 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
3.136.99.112	**IP**: 3.136.99.112 **所属国家**: United States of America **地区**: Ohio **城市**: Columbus **纬度**: 39.961380 **经度**: -82.997749
log.tbs.qq.com	**IP**: 109.244.244.32 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mobilegw.alipaydev.com	**IP**: 110.75.132.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 182.92.20.189 **所属国家**: China

182.92.20.189	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
d.alipay.com	IP: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
mobilegw.alipay.com	IP: 203.209.243.98 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
123.59.60.170	IP: 123.59.60.170 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mclient.alipay.com	IP: 27.128.221.244 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
debugtbs.qq.com	IP: 175.27.9.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

image.cnamedomain.com	没有服务器地理信息.
tsis.jpush.cn	**IP**: 121.36.74.75 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ce3e75d5.jpush.cn	**IP**: 120.233.50.73 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
pms.mb.qq.com	**IP**: 175.27.12.246 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
task.shareinstall.com.cn	**IP**: 120.46.79.149 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
wappaygw.alipay.com	**IP**: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
	IP: 175.27.9.46

debugx5.qq.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.sharetrace.com	IP: 39.98.67.122 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
h5.m.taobao.com	IP: 220.181.135.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
tbsrecovery.imtt.qq.com	IP: 109.244.244.237 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
m.alipay.com	IP: 203.209.245.74 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
statlog.shareinstall.com.cn	IP: 119.3.169.231 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572

pinterest.com	**IP**: 69.171.224.36 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604
cfg.imtt.qq.com	**IP**: 109.244.173.227 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mcgw.alipay.com	**IP**: 124.239.239.237 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
mdc.html5.qq.com	**IP**: 175.27.9.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
s.sharetrace.com	**IP**: 39.98.67.122 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL信息	Url所在文件
https://api.sharetrace.com	a/a/a/a/c/d.java
https://twitter.com/intent/tweet?text=	cl/json/social/TwitterShare.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookPagesManagerShare.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookShare.java
https://plus.google.com/share?url=	cl/json/social/GooglePlusShare.java
https://pinterest.com/pin/create/button/?url=	cl/json/social/PinterestShare.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/aj/d.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ai/b.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java
https://tsis.jpush.cn	cn/jiguang/ao/i.java
https://www.pgyer.com/apiv1/crash/add	com/pgyersdk/crash/PgyCrashManager.java
https://www.pgyer.com/apiv1/crash/add	com/pgyersdk/crash/a.java
https://www.pgyer.com/apiv1/feedback/add	com/pgyersdk/feedback/PgyFeedback.java
https://www.pgyer.com/apiv1/update/check	com/pgyersdk/f/a.java
https://www.pgyer.com/apiv1/sdkstat/launch	com/pgyersdk/a/a.java
http://pv.sohu.com/cityjson?ie=utf-8	com/sh/sdk/shareinstall/c/a/g.java

http://iploc.market.alicloudapi.com/v3/ip	com/sh/sdk/shareinstall/c/a/f.java
http://123.59.60.170/shareinstall_log/register	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_log/register	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/shareinstall_log/install	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_log/install	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/shareinstall_log/active	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_log/active	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/shareinstall_log/online	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_log/online	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/sdkinfoscollection/startover	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/sdkinfoscollection/startover	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/shareinstall_logs_act/activity	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_logs_act/activity	com/sh/sdk/shareinstall/c/g/f.java
http://123.59.60.170/shareinstall_log/openapplist	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_log/openapplist	com/sh/sdk/shareinstall/c/g/f.java
https://statlog.shareinstall.com.cn/shareinstall_logs_act/activity	com/sh/sdk/shareinstall/business/a/a/a/b.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/business/a/a/a/b.java
https://task.shareinstall.com.cn/hike/excepush	com/sh/sdk/shareinstall/business/helper/h.java

https://statlog.shareinstall.com.cn/shareinstall_log/task	com/sh/sdk/shareinstall/business/helper/n.java
https://statlog.shareinstall.com.cn/shareinstall_log/si	com/sh/sdk/shareinstall/business/helper/k.java
https://config.shareinstall.com.cn/signal/config	com/sh/sdk/shareinstall/business/helper/b.java
https://statlog.shareinstall.com.cn/shareinstall_log/noticeup	com/sh/sdk/shareinstall/business/helper/l.java
https://check.shareinstall.com.cn/wwwroot	com/sh/sdk/shareinstall/business/helper/d.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/util/n.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/util/m.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/packet/impl/e.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/d.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://3.136.99.112:3000/	com/mb/rn/activity/MainApplication.java
https://d.alipay.com	com/mb/rn/webview/XJsInterface.java
https://codepush.azurewebsites.net/	com/microsoft/codepush/react/CodePush.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/m.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java

https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://adsbrefrigerator.tt.cn/export/VSqqAf.api	com/lockscreen/news/b/a.java
https://spxw.mop.com/NewsCenter/locksc	com/lockscreen/news/b/b.java
http://ns.adobe.com/xap/1.0/	lib/armeabi/libimagepipeline.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so

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=ijz, ST=wjijxzioj, L=sjiodjFOIJoqj, O=ylcaaa, OU=JOIoijsoia, CN=ASDIO1JOI
签名算法: rsassa_pkcs1v15

有效期自: 2022-10-20 09:28:14+00:00
有效期至: 2047-10-14 09:28:14+00:00
发行人: C=ijz, ST=wjijxzioj, L=sjiodjFOIJoqj, O=ylcaaa, OU=JOIoijsoia, CN=ASDIO1JOI
序列号: 0x3c5f08a
哈希算法: sha256
md5值: 05c29b286bc7d5ed8f406d9f92e34166
sha1值: 01f86041dde5cfa0890f51f5c1161a78cf7746c9
sha256值: 5feb372e48a08e0c3bbb7e45d3550a27f0ba60ac6d1b897f2a045d39169c7214
sha512值: 0f2a363fa0dde60da8b9c985f1a193261dc70222a8266e5741332cebe19704446bb76f1e39d01e62796548f7b8088000bd6e5a46bb5f9f6680ca52fc6ffa2991
公钥算法: rsa
密钥长度: 2048
指纹: 20dcfc3b18c779b77b535df1db94d0972e476d3e9035ce3de3c4798df930f20f

硬编码敏感信息

可能的敏感信息
"CfgKey" : "Num2Tid1ylc"
"VersionKey" : "fT6phq0wkOPRlAoyToidAnkogUV7ttGo"

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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息

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.MONUN_UNMOUNT_FILESYSTEMS	未知	Unknown permission	Unknown permission from android reference
android.permission.JPUSH_MESSAGE	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
com.arDf8g2vRHGpRWjv5Va_nPvPTqF72ZxiIIOVcU_iV440XHBm.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.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
			访问精细位置源,例如手机上的全球定位系统,如果可用。

android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	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_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.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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC

android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.mb.rn.activity.ReactMainActivity	Schemes: myNative://, NULL://, stbcb156e84c54e55d://,

---