



MoGua

潮玩鲨 5.0.00.APK 分析报告



APP名称:

潮玩鲨

包名:	uni.UNI896ED8E
域名线索:	27条
URL线索:	31条
邮箱线索:	0条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件名: 潮玩鲨_（游戏）.apk
文件大小: 20.77MB
MD5值: 9e2ca3c082373dc135d6d7fb9ac5a19f
SHA1值: f675591cc32ec5784cc481391e0beb0849fbdfbd
SHA256值: a17a70477f4859bddbe386fa693f733263f5fd07fa0211127e36ac8a5bd3f3a6

i APP 信息

App名称: 潮玩鲨
包名: uni.UNI896ED8E
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 5.0.00
安卓版本: 5000

🔍 域名线索

域名	服务器信息
m3w.cn	IP: 221.204.15.84 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
open.weixin.qq.com	IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
debugx5.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin

	城市: Tianjin 纬度: 39.142181 经度: 117.176102
long.open.weixin.qq.com	IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
ns.adobe.com	没有服务器地理信息.
mclient.alipay.com	IP: 218.24.90.223 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
pms.mb.qq.com	IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
wappaygw.alipay.com	IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.weixin.qq.com	IP: 112.65.193.153 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333

	经度: 121.468948
log.tbs.qq.com	IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
tbs.imtt.qq.com	IP: 218.29.50.184 所属国家: China 地区: Henan 城市: Xinxiang 纬度: 35.308777 经度: 113.867203
loggw-exsdk.alipay.com	IP: 119.42.231.59 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
h5.m.taobao.com	IP: 125.38.11.131 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
mdc.html5.qq.com	IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
	IP: 110.75.138.35 所属国家: China 地区: Zhejiang

mobilegwpre.alipay.com	城市: Hangzhou 纬度: 30.293650 经度: 120.161583
mcgw.alipay.com	IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
render.alipay.com	IP: 27.221.79.105 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
schemas.android.com	没有服务器地理信息.
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
er.dcloud.io	没有服务器地理信息.
	IP: 60.28.172.238 所属国家: China

cfg.imtt.qq.com	地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
tbsrecovery.imtt.qq.com	IP: 61.181.204.91 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobilegw.alipay.com	IP: 203.209.247.65 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
debugtbs.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/l/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/l/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/m/a.java
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java

https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.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://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.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=11047&is64=0	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047&is64=1	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041&is64=0	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041&is64=1	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java

https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/o.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java

https://api.weixin.qq.com/sns/oauth2/access_token? appid=%s&secret=%s&code=%s&grant_type=authorization_code	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/283	j/b.java

 邮箱线索

 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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, ST=, L=, O=Android, OU=Android, CN=LRnMyZC2h2m4DSRUahqzXTWb6O58Pu0l4c1R1jUu9NGquKFuAg4v1FjDxd6%2FR3ofd8uBE94TJ7bRrRKorCP8fw%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-05 04:16:09+00:00
有效期至: 2124-11-11 04:16:09+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=LRnMyZC2h2m4DSRUahqzXTWb6O58Pu0l4c1R1jUu9NGquKFuAg4v1FjDxd6%2FR3ofd8uBE94TJ7bRrRKorCP8fw%3D%3D
序列号: 0x5654c371
哈希算法: sha256
md5值: f545736012de31977a8a7c1a4c5ea92b
sha1值: b1f64bbd89775a53e2a0d07200d5e77c44bcd4f
sha256值: b86a7031ea5b187ac5c5a15082eef01ab4686df59f7b61600f33da96c21315da
sha512值: 4c6629fcd83bf3c027da00b70a5ce03d555a84b1661b5e6ea4ad8ba7fc44fa9fd477f0a57195fbee8b31d347693e61e3b4bbc651cb2f864771514598d4c72fd7
公钥算法: rsa
密钥长度: 2048
指纹: 075ed8c6634bbd0d4cf4cc127d63ebd47c3d83a85b443999ad02f66ca096a4c2

硬编码敏感信息

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.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_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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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_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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: huw2u2://,