



MoGua

趣闲赚 2.2.5.APK 分析报告



APP名称:

趣闲赚

包名:	com.quxianzhuan.wap
域名线索:	70条
URL线索:	60条
邮箱线索:	0条
分析日期:	2025年4月23日
分析平台:	摸瓜APK反编译平台

文件名: qxz_225.apk
文件大小: 10.44MB
MD5值: a21a3db0ed823a0f21114c202cbe32ac
SHA1值: 7885c4e5f3735507ed02a5f2b5d4dcde77671063
SHA256值: f86156a4e6530539f9bd4956cc09c3d9f882fd174f0bc4f5cd672e890a596ad7

i APP 信息

App名称: 趣闲赚
包名: com.quxianzhuan.wap
主活动Activity: com.lt.app.MainActivity
安卓版本名称: 2.2.5
安卓版本: 225

🔍 域名线索

域名	服务器信息
aspect-upush.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
appsupport.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
	IP: 101.69.207.68 所属国家: China 地区: Zhejiang

zxid-m.mobileservice.cn	城市: Hangzhou 纬度: 30.293650 经度: 120.161583
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
api-push.meizu.com	IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan 纬度: 23.026770 经度: 113.131477
ulogs.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
ucc.umeng.com	IP: 203.119.169.175 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
10.38.162.35	IP: 10.38.162.35 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

b-gtc.getui.net	IP: 101.68.218.171 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
b-gtc.getui.nethttps	没有服务器地理信息.
imgcache.qq.com	IP: 61.54.91.204 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683289 经度: 112.453911
ulogs.umengcloud.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.baidu.com	IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
open.weixin.qq.com	IP: 116.128.169.212 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
	IP: 59.82.29.248 所属国家: China

pslog.umeng.com	地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
resolve.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
gtc.getui.net	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
metrics2.data.hicloud.com	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
store-at-dre.hispace.dbankcloud.com	没有服务器地理信息.
xmlpull.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California

	纬度: 40.065647 经度: -79.891724
gcc.gnu.org	IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh 纬度: 35.773994 经度: -78.632759
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
h.trace.qq.com	IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
nisportal.10010.com	IP: 124.64.196.20 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 59.82.112.112

developer.umeng.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api-push.in.meizu.com	IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon 纬度: 38.978210 经度: -77.386993
gtc.getui.nethttps	没有服务器地理信息.
b-gtc.gepush.com	IP: 101.68.218.169 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
mp.weixin.qq.com	IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
store3.hispace.hicloud.com	IP: 23.210.26.177 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
	IP: 3.166.228.36 所属国家: United States of America 地区: Washington

store2.hispace.hicloud.com	城市: Seattle 纬度: 47.627499 经度: -122.346199
1.12.12.12	IP: 1.12.12.12 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
cgi.qplus.com	没有服务器地理信息.
grs.dbankcloud.asia	IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
metrics.dt.dbankcloud.ru	IP: 159.138.204.140 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
resolver.msg.xiaomi.net	IP: 123.125.102.69 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
alogus.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668

	经度: 118.777992
sdk-open-phone.getui.com	IP: 124.160.155.44 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
c-hzgt2.getui.com	IP: 124.160.155.61 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
store-drru.hispac.hicloud.com	IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
store1.hispac.hicloud.com	IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
dns.alidns.com	IP: 223.5.5.5 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
	IP: 60.28.193.195 所属国家: China

grs.dbankcloud.com	地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
c-gtc.getui.nethttps	没有服务器地理信息.
utoken.umeng.com	IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
data-dra.push.dbankcloud.com	IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
crl.securetrust.com	IP: 23.210.26.156 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
cgi.connect.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
grs.platform.dbankcloud.ru	没有服务器地理信息.
	IP: 121.36.117.149

grs.dbankcloud.cn	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
d-gt.getui.com	没有服务器地理信息.
play.google.com	IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam 纬度: 37.420624 经度: 127.126717
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
openmobile.qq.com	IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
data-drcn.push.dbankcloud.com	IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 49.4.47.241 所属国家: China 地区: Guangdong

store.hispace.hicloud.com	城市: Guangzhou 纬度: 23.127361 经度: 113.264572
norma-external-collect.meizu.com	IP: 183.60.176.112 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
appgallery.cloud.huawei.com	IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.eu	没有服务器地理信息.
gtc.gepush.com	IP: 43.231.145.96 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
aid.mobileservice.cn	IP: 101.69.207.68 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
c-gtc.gepush.com	IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199

	经度: 120.750000
alogsus.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
cn.register.xmpush.xiaomi.com	IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
cnlogs.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
	IP: 124.160.155.57 所属国家: China

c-gtc.getui.net	地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
-----------------	--

 URL线索

URL信息	Url所在文件
https://c-gtc.getui.net,https://c-gtc.gepush.com	com/getui/gtc/c/b.java
https://gtc.getui.net,https://gtc.gepush.com	com/getui/gtc/c/b.java
https://b-gtc.getui.net,https://b-gtc.gepush.com	com/getui/gtc/c/b.java
https://sdk-open-phone.getui.com/	com/getui/gtc/i/d/b.java
https://([\s\S]+)	com/huawei/hms/scankit/p/t3.java
https://sdk-open-phone.getui.com/api.php	com/igexin/push/a.java
https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
https://bi.	com/igexin/push/config/b.java
https://config.	com/igexin/push/config/b.java
https://bi.	com/igexin/push/config/h.java
https://config.	com/igexin/push/config/h.java

https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/server/getPushConf	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.in.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/c/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/c/a.java
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/cloud/pushsdk/platform/c/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%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
https://mp.weixin.qq.com/publicpoc/opensdkconf? action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s	com/tencent/mm/opensdk/openapi/WXAPISecurityHelper.java
https://imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApilml.java
https://imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApilml.java
https://imgcache.qq.com	com/tencent/open/SocialApilml.java
https://imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApilml.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java

https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/b/h.java
https://h.trace.qq.com/kv	com/tencent/open/b/b.java
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utis/j.java
https://openmobile.qq.com/	com/tencent/open/utis/HttpUtils.java
https://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
https://cgi.qplus.com/report/report	com/tencent/connect/avatar/ImageActivity.java
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/l.java
https://aspect-upush.umeng.com/occa/v1/event/report	com/umeng/analytics/pro/aq.java
https://cnlogs.umeng.com/ext_event	com/umeng/analytics/pro/aq.java
https://resolve.umeng.com/resolve	com/umeng/analytics/pro/bt.java

https://ucc.umeng.com/v2/inn/fetch	com/umeng/analytics/pro/ar.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://developer.umeng.com/docs/119267/detail/118637	com/umeng/commonsdk/debug/UMLogCommon.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://alogus.umeng.com	com/umeng/commonsdk/stateless/a.java
https://utoken.umeng.com	com/umeng/umzid/ZIDManager.java
http://xmllpull.org/v1/doc/features.html	com/xiaomi/push/hh.java
http://xmllpull.org/v1/doc/features.html	com/xiaomi/push/hz.java
https://%1\$s/gslb/?ver=5.0	com/xiaomi/push/dd.java
http://xmllpull.org/v1/doc/features.html	com/xiaomi/push/ia.java

http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/gv.java
http://10.38.162.35:9085	com/xiaomi/push/service/v.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/v.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bx.java
https://aid.mobileservice.cn/	com/zx/a/l8b7/j3.java
https://zxid-m.mobileservice.cn/sdk/config/v2/init	com/zx/a/l8b7/n.java
https://nisportal.10010.com:9001	com/zx/a/l8b7/f1.java
https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/l8b7/l.java
https://zxid-m.mobileservice.cn/sdk/app/depAnalysis	com/zx/a/l8b7/d1.java
https://zxid-m.mobileservice.cn/sdk/module/getCoreModule	com/zx/a/l8b7/f0.java
https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken	com/zx/a/l8b7/v1.java
https://zxid-m.mobileservice.cn/sdk/extend/tag	com/zx/a/l8b7/b2.java
https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/l8b7/w1.java
https://zxid-m.mobileservice.cn/sdk/ext/pconfig	com/zx/a/l8b7/f.java
https://zxid-m.mobileservice.cn/sdk/channel/report	com/zx/a/l8b7/p1.java
https://www.baidu.com/favicon.ico?\	j5/w0.java
https://dns.alidns.com/dns-query	l5/q.java
https://1.12.12.12/dns-query	l5/q.java

https://play.google.com/store/apps/details?id=	摸瓜V1引擎
https://appgallery.cloud.huawei.com	摸瓜V1引擎
https://store.hispace.hicloud.com/hwmarket/api/	摸瓜V1引擎
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics.dt.dbankcloud.ru	摸瓜V2引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎
https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://store1.hispace.hicloud.com/hwmarket/api/	摸瓜V2引擎

https://store2.hispace.hicloud.com/hwmarket/api/	摸瓜V2引擎
https://store3.hispace.hicloud.com/hwmarket/api/	摸瓜V2引擎
https://store-drru.hispace.hicloud.com/hwmarket/api/	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://c-gtc.getui.net	摸瓜V3引擎
http://developer.umeng.com/docs/66650/cate/66650	摸瓜V3引擎
https://openmobile.qq.com/oauth2.0/m_authorize?	摸瓜V3引擎
http://10.38.162.35:9085	摸瓜V3引擎
https://resolve.umeng.com/resolve	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/ext/pconfig	摸瓜V3引擎
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	摸瓜V3引擎
https://imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	摸瓜V3引擎
https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎

https://imgcache.qq.com/ptlogin/static/qzsjump.html?	摸瓜V3引擎
https://ucc.umeng.com/v2/inn/fetch	摸瓜V3引擎
https://api-push.in.meizu.com/garcia/api/client/	摸瓜V3引擎
https://1.12.12.12/dns-query	摸瓜V3引擎
https://ulogs.umeng.com	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/uaid/get	摸瓜V3引擎
https://www.baidu.com/favicon.ico?	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/extend/tag	摸瓜V3引擎
https://c-gtc.gepush.com	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	摸瓜V3引擎
http://gcc.gnu.org/bugs.html):	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/config/init	摸瓜V3引擎
https://open.weixin.qq.com/connect/sdk/qconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signatur	摸瓜V3引擎
https://developer.umeng.com/docs/119267/detail/118637#3091c7c11fx3q	摸瓜V3引擎
https://h.trace.qq.com/kv	摸瓜V3引擎

https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	摸瓜V3引擎
https://imgcache.qq.com/open/mobile/request/sdk_request.html?	摸瓜V3引擎
https://sdk-open-phone.getui.com/	摸瓜V3引擎
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	摸瓜V3引擎
https://openmobile.qq.com/v3/user/get_info	摸瓜V3引擎
https://c-hzgt2.getui.com/api.php	摸瓜V3引擎
https://nisportal.10010.com:9001	摸瓜V3引擎
https://cn.register.xmpush.xiaomi.com	摸瓜V3引擎
https://utoken.umeng.com	摸瓜V3引擎
https://imgcache.qq.com/open/mobile/invite/sdk_invite.html?	摸瓜V3引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V3引擎
https://developer.umeng.com/docs/66632/detail/	摸瓜V3引擎
https://aspect-upush.umeng.com/occa/v1/event/report	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/config/v2/init	摸瓜V3引擎
https://api-push.meizu.com/garcia/api/server/getPushConf	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/module/getCoreModule	摸瓜V3引擎
https://api-push.meizu.com/garcia/api/client/	摸瓜V3引擎
https://mp.weixin.qq.com/publicpoc/opensdkconf?	摸瓜V3引擎

action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s	
https://b-gtc.gepush.com	摸瓜V3引擎
https://alogus.umeng.com	摸瓜V3引擎
https://openmobile.qq.com/oauth2.0/me	摸瓜V3引擎
https://openmobile.qq.com/	摸瓜V3引擎
http://xmlpull.org/v1/doc/features.html#process-namespaces	摸瓜V3引擎
https://cnlogs.umeng.com/ext_event	摸瓜V3引擎
https://resolver.msg.xiaomi.net/psc/?t=a	摸瓜V3引擎
https://norma-external-collect.meizu.com/push/android/external/add.do	摸瓜V3引擎
https://openmobile.qq.com/user/user_login_statis	摸瓜V3引擎
https://cgi.qplus.com/report/report	摸瓜V3引擎
https://%1\$s/gslb/?ver=5.0	摸瓜V3引擎
https://api-push.meizu.com/garcia/api/client/log/upload	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/app/depAnalysis	摸瓜V3引擎
https://b-gtc.getui.net	摸瓜V3引擎
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	摸瓜V3引擎
https://api-push.meizu.com/garcia/api/server/getPublicKey	摸瓜V3引擎
https://imgcache.qq.com	摸瓜V3引擎

https://d-gt.getui.com/api.htm	摸瓜V3引擎
https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
https://aid.mobileservice.cn/	摸瓜V3引擎
https://zxid-m.mobileservice.cn/sdk/channel/report	摸瓜V3引擎
https://gtc.gepush.com	摸瓜V3引擎
https://sdk-open-phone.getui.com/api.php	摸瓜V3引擎
https://dns.alidns.com/dns-query	摸瓜V3引擎
http://crl.securetrust.com/STCA.crl0	摸瓜V3引擎
https://developer.umeng.com/docs/119267/detail/182050	摸瓜V3引擎
https://gtc.getui.net	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	摸瓜V3引擎

 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=CN, ST=SC, L=CD, O=local, OU=LTAPP, CN=local

签名算法: rsassa_pkcs1v15

有效期自: 2018-12-24 14:34:14+00:00

有效期至: 2118-11-30 14:34:14+00:00

发行人: C=CN, ST=SC, L=CD, O=local, OU=LTAPP, CN=local

序列号: 0xe49d712

哈希算法: sha256

md5值: aa8716ead898b4d55520615c3fdc62c6

sha1值: dfc5284f63c6df8d712af20a043d2796832afb7

sha256值: 9cbb47f103cdfe6cd23115d1debcd1f90a19a3d992edd0ce59b076d20e292d4a

sha512值: 2028110f4d88e81fb5aa39b35778e0b25314f1a3126c5a84baed2a382c363b7eb52cdb1dedb7f00e4d6cbd416cbf48a48717718b5c62d7d86af86e67e78f92bb

公钥算法: rsa

密钥长度: 2048

指纹: 6e41f8086c3896774512c947769f5ec9087b6a06485ab5d1fbdd8e83a75ed133

🔑 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" : "fa2c714cf6bf427bbc9216060f97a765"
"p_rcpush_opAppKey" : "a3f303389cef4800972fd94c91fd2a05"

"p_rcpush_opAppSecret" : "845ca84c5eff4249994fd92a31f9b9f0"
"p_rcpush_vvAppKey" : "e0cde6e8d306b6451b94315d178416ca"
"p_rcpush_xmAppKey" : "5972011053512"
"p_u_appkey" : "606d8d7018b72d2d2449a9dd"
"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"

 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.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。
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.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_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.POST_NOTIFICATIONS	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。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.quxianzhuan.wap.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
com.quxianzhuan.wap.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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_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
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
oplus.permission.settings.LAUNCH_FOR_EXPORT	未知	Unknown permission	Unknown permission from android reference
com.vivo.identifier.permission.OAID_STATE_DIALOG	未知	Unknown permission	Unknown permission from android reference
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。
com.quxianzhuan.wap.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference

com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.quxianzhuan.wap.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.quxianzhuan.wap.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
getui.permission.GetuiService.com.quxianzhuan.wap	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
com.quxianzhuan.wap.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.quxianzhuan.wap.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

com.meizu.flyme.permission.PUSH	知	permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp124758://, @string/p_u_scheme://,
com.tencent.tauth.AuthActivity	Schemes: tencent1107977175://,

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