MoGua

mo.co 1.0.0.APK 分析报告

APP名称: mo.co

包名:	com.tencent.tmgp.supercell.moco
域名线索:	56条
URL线索:	40条
邮箱线索:	0条
分析日期:	2025年8月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 89900051_com.tencent.tmgp.supercell.moco_h3761453_1.0.0_cxyfDn.apk
文件大小: 1076.75MB
MD5值: 5bf89ec51172f1397ac15438b1479c67
SHA1值: 2def5eee199a97c4051e939bbc4a8476def2fed7
SHA256值: 5ab0037c0f4c11ee62c83255187c128a5e5a44d232920638dfefa813a31368b1

APP 信息

App名称: mo.co
包名: com.tencent.tmgp.supercell.moco
主活动Activity: com.supercell.titan.tencent.GameAppTencent
安卓版本名称: 1.0.0
安卓版本: 1000000

域名线索

域名	服务器信息
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
snowflake.qq.com	**IP**: 125.36.181.166 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
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
scdn-stestsettings.s	没有服务器地理信息.
aggregator.service.usercentrics.eu	IP: 34.120.28.121 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
scdn-ssettings.s	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
config.eu.usercentrics.eu	IP: 143.244.50.84 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
sregister.s	没有服务器地理信息.
sdlsdk.s	没有服务器地理信息.
cfg.imtt.qq.com	IP: 60.29.240.17 **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
ssdk-services.s	没有服务器地理信息.
uct.service.usercentrics.eu	**IP**: 34.95.108.180 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
sinapps.s	没有服务器地理信息.
graph.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
consent-rt-ret.service.consent.usercentrics.eu	**IP**: 34.102.167.147 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
consent-rt-ret.service.consent.eu1.usercentrics.eu	**IP**: 143.244.49.177 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904

h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
analy.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
android.crashsight.qq.com	**IP**: 114.222.112.57 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
tbs.imtt.qq.com	**IP**: 124.166.237.202 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
app.usercentrics.eu	**IP**: 35.190.14.188 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
slaunches.s	没有服务器地理信息.
sattr.s	没有服务器地理信息.

uct.eu.usercentrics.eu	**IP**: 143.244.49.178 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
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
sonelink.s	没有服务器地理信息.
sgcdsdk.s	没有服务器地理信息.
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
fusion.qq.com	**IP**: 116.130.228.157 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.usercentrics.eu	**IP**: 35.241.3.184 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568

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
sapp.s	没有服务器地理信息.
usercentricssupport.zendesk.com	**IP**: 216.198.54.6 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
smonitorsdk.s	没有服务器地理信息.
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
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
appact.qzone.qq.com	**IP**: 116.130.224.189 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

tun-cos-1258344701.file.myqcloud.com	**IP**: 123.6.2.137 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
test.snowflake.qq.com	**IP**: 221.198.69.15 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
open.weixin.qq.com	**IP**: 116.128.171.214 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
aggregator.eu.usercentrics.eu	**IP**: 143.244.49.178 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
sadrevenue.s	没有服务器地理信息.
sars.s	没有服务器地理信息.
sconversions.s	没有服务器地理信息.
consent-api.service.consent.usercentrics.eu	**IP**: 35.201.111.240 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731

	经度: -94.578568
imgcache.qq.com	**IP**: 61.163.203.74 **所属国家**: China **地区**: Henan **城市**: Zhumadian **纬度**: 32.979439 **经度**: 114.030144
m.wsq.qq.com	没有服务器地理信息.
webpresence.qq.com	**IP**: 220.194.111.233 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
sviap.s	没有服务器地理信息.
simpression.s	没有服务器地理信息.
consent-api.service.consent.eu1.usercentrics.eu	**IP**: 143.244.49.179 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
mp.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
svalidate.s	没有服务器地理信息.

app.eu.usercentrics.eu	**IP**: 143.244.50.84 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904

URL线索

URL**信息**	Url**所在文件**
https://play.google.com/d?id=	com/supercell/titan/GameApp.java
https://play.google.com/store/apps/details?id=	com/supercell/titan/GameApp.java
https://android.crashsight.qq.com/pb/async	com/supercell/titan/tencent/CrashSightAgent.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&timestamp=%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://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/AuthDialog.java
https://openmobile.qq.com/user/user_login_statis	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://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/j.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://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
http://%s/d?dn=%s&clientip=%s&ttl=%s&id=%s	com/tencent/itop/httpdns/a/a/c.java
https://imgcache.qq.com/open/mobile/rate/sdk_rate.html?	com/tencent/open/SocialApiIml.java
https://appact.qzone.qq.com/appstore_activity_task_pcpush_sdk	com/tencent/open/TaskGuide.java
https://graph.qq.com/org/bind/query?appid=%s&org_id=%s&word_id=%s&openid=%s&openkey=%s	com/tencent/open/GuildApi.java
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/open/utils/ServerSetting.java

https://imgcache.qq.com	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/brag/sdk_brag.html?	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/utils/ServerSetting.java
https://openmobile.qq.com/	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/reactive/sdk_reactive.html?	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/open/mobile/not_support.html?	com/tencent/open/utils/ServerSetting.java
https://imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/open/utils/ServerSetting.java
https://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/open/utils/ServerSetting.java
https://fusion.qq.com/cgi-bin/prize_sharing/exchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
https://fusion.qq.com/cgi-bin/prize_sharing/get_activity_state.cgi	com/tencent/open/utils/ServerSetting.java
https://fusion.qq.com/cgi-bin/prize_sharing/make_share_url.cgi	com/tencent/open/utils/ServerSetting.java
https://fusion.qq.com/cgi-bin/prize_sharing/query_unexchange_prize.cgi	com/tencent/open/utils/ServerSetting.java
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/OpenConfig.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/c/h.java
https://h.trace.qq.com/kv	com/tencent/open/c/b.java

https://analy.qq.com/cgi-bin/mapp_apptrace	com/tencent/open/yyb/a.java
https://imgcache.qq.com/open/mobile/jsbridge/demo.htm	com/tencent/open/yyb/AppbarJsBridge.java
https://m.wsq.qq.com/direct?	com/tencent/open/yyb/AppbarAgent.java
https://webpresence.qq.com/getonline?Type=1&	com/tencent/open/wpa/WPA.java
https://test.snowflake.qq.com/ola/v2	com/tencent/tdm/qimei/x/d.java
https://snowflake.qq.com/ola/v2	com/tencent/tdm/qimei/x/d.java
https://tun-cos-1258344701.file.myqcloud.com/fp.js	com/tencent/tdm/qimei/aw/a.java
https://tun-cos-1258344701.file.myqcloud.com/my.html	com/tencent/tdm/qimei/aw/a.java
https://aggregator.service.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://aggregator.eu.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://uct.service.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://uct.eu.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://app.usercentrics.eu/session/1px.png	com/usercentrics/sdk/BuildKonfig.java
https://app.eu.usercentrics.eu/session/1px.png	com/usercentrics/sdk/BuildKonfig.java
https://consent-rt-ret.service.consent.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://consent-rt-ret.service.consent.eu1.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://consent-api.service.consent.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java
https://consent-api.service.consent.eu1.usercentrics.eu	com/usercentrics/sdk/BuildKonfig.java

https://config.eu.usercentrics.eu	com/usercentrics/sdk/domain/api/ApiEndpointsEurope.java
https://api.usercentrics.eu	com/usercentrics/sdk/domain/api/ApiEndpointsWorld.java
https://usercentricssupport.zendesk.com/hc/en-us/requests/new	com/usercentrics/sdk/mediation/facade/MediationFacade.java

邮箱线索

手机线索

手机号	所在文件
15555215554	com/framgia/android/emulator/EmulatorDetector.java
15555215556	com/framgia/android/emulator/EmulatorDetector.java
15555215558	com/framgia/android/emulator/EmulatorDetector.java
15555215560	com/framgia/android/emulator/EmulatorDetector.java
15555215562	com/framgia/android/emulator/EmulatorDetector.java
15555215564	com/framgia/android/emulator/EmulatorDetector.java
15555215566	com/framgia/android/emulator/EmulatorDetector.java
15555215568	com/framgia/android/emulator/EmulatorDetector.java
15555215570	com/framgia/android/emulator/EmulatorDetector.java

15555215572	com/framgia/android/emulator/EmulatorDetector.java
15555215574	com/framgia/android/emulator/EmulatorDetector.java
15555215576	com/framgia/android/emulator/EmulatorDetector.java
15555215578	com/framgia/android/emulator/EmulatorDetector.java
15555215580	com/framgia/android/emulator/EmulatorDetector.java
15555215582	com/framgia/android/emulator/EmulatorDetector.java
15555215584	com/framgia/android/emulator/EmulatorDetector.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=(GD), L=(Shenzhen), O=(Tencent), OU=(Tencent), CN=(Tencent)
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-16 07:09:31+00:00
有效期至: 2134-07-24 07:09:31+00:00
发行人: C=(CN), ST=(GD), L=(Shenzhen), O=(Tencent), OU=(Tencent), CN=(Tencent)
序列号: 0x63c93455
哈希算法: sha256
md5值: 8f7a1f79b13ac30c17af7767f7937e5f
sha1值: e03c5a80dd0b653a267807526ca82ef2bb79b7b8
sha256值: f1823732e6e386571725b794b17eb951510d5effe61f495fee08dd0f7b184356
sha512值: b6e42ee52f32fbc5b493e54220596a78ebdb086c728fca35a0ccf23cee4248414021abccdc65c22823fa2e2845063cf9ee4c9f3101b090e7b486f95c15ef047c
公钥算法: rsa
密钥长度: 3072
指纹: be44a6e28bc9fbfc4271cc4ae4e049767cf390e76412839c420efec10c35ff3e

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.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.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.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_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
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_BASIC_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.Manifest.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
com.google.android.gms.permission.AD_ID	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_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_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
	危	精细定位	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

android.permission.ACCESS_FINE_LOCATION	险	（GPS）	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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	Unknown permission	Unknown permission from android reference
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。
com.tencent.tmgp.supercell.moco.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.midas.qq.APMidasQQWalletActivity	Schemes: qwallet100703379://,
com.supercell.titan.tencent.GameAppTencent	Schemes: moco-integration://, moco-playable://, moco-branch-integration://, moco://, https://, Hosts: go.mo.co, link-dev.moco.supercell.com, link-staging.moco.supercell.com, joinmoco.onelink.me, play.mo.co, Path Prefixes: /JUhc,
com.tencent.tauth.AuthActivity	Schemes: tencent1112345965://,

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。