Evaluation Warning: The document was created with Spire.Doc for Python.

**mo.co（ 1.0.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | mo.co |
| 版本 | 1.0.0 |
| 包名 | com.tencent.tmgp.supercell.moco |
| 域名线索 | 56条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年8月4日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| snowflake.qq.com | IP: 125.36.181.166 所属国家: China 地区: Tianjin 城市: Tianjin  |
| openmobile.qq.com | IP: 60.28.215.27 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 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  |
| 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  |
| config.eu.usercentrics.eu | IP: 143.244.50.84 所属国家: United States of America 地区: California 城市: Los Angeles  |
| 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  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 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  |
| 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  |
| 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  |
| 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  |
| h.trace.qq.com | IP: 113.56.189.162 所属国家: China 地区: Hubei 城市: Huangshi  |
| analy.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| android.crashsight.qq.com | IP: 114.222.112.57 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| tbs.imtt.qq.com | IP: 124.166.237.202 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| app.usercentrics.eu | IP: 35.190.14.188 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| 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  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 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  |
| fusion.qq.com | IP: 116.130.228.157 所属国家: China 地区: Beijing 城市: Beijing  |
| api.usercentrics.eu | IP: 35.241.3.184 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| 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  |
| 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  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| appact.qzone.qq.com | IP: 116.130.224.189 所属国家: China 地区: Beijing 城市: Beijing  |
| tun-cos-1258344701.file.myqcloud.com | IP: 123.6.2.137 所属国家: China 地区: Henan 城市: Zhengzhou  |
| test.snowflake.qq.com | IP: 221.198.69.15 所属国家: China 地区: Tianjin 城市: Tianjin  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| aggregator.eu.usercentrics.eu | IP: 143.244.49.178 所属国家: United States of America 地区: California 城市: Los Angeles  |
| 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  |
| imgcache.qq.com | IP: 61.163.203.74 所属国家: China 地区: Henan 城市: Zhumadian  |
| 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  |
| 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  |
| mp.weixin.qq.com | IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 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  |

### **4.2 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  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 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  |

## **5. 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**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |
| 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 |
| 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 |

## **10. 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**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**