



MoGua

淘色 1.3.4.APK 分析报告



APP名称:

淘色

包名: com.android.taose2024

域名线索: 46条

URL线索: 30条

邮箱线索: 0条

分析日期: 2025年10月3日

分析平台: [摸瓜APK反编译平台](#)

文件名: 淘色.apk
文件大小: 14.13MB
MD5值: 04318b11d8ea16f981bcf65583b0566f
SHA1值: efcf88e3f779186607e5240f5f806565e86bfe85
SHA256值: d45de0ebf4069653909f76da512e9748b0b9d9ace15c25d12ba8d4f8bb6525ef

i APP 信息

App名称: 淘色
包名: com.android.taose2024
主活动Activity: com.android.o.ui.main.LauncherActivity
安卓版本名称: 1.3.4
安卓版本: 134

🔍 域名线索

域名	服务器信息
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
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
xiguaule.com	IP: 0.0.0.0 所属国家: - 地区: -

	城市: - 纬度: 0.000000 经度: 0.000000
plbslog.umeng.com	IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
cmnsguider.yunos.com	IP: 203.119.175.235 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
storage.dreameragame.com	没有服务器地理信息.
bak.sgp1.cc	IP: 104.21.80.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
publish.twitter.com	IP: 104.244.42.195 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968

	经度: -122.410446
soft.tbs.imtt.qq.com	IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
dashif.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
i.lulutv.fun	IP: 143.204.126.94 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
xiuxiuba.vip	没有服务器地理信息.
api.vipmisss.com	IP: 45.88.194.109 所属国家: United States of America 地区: South Dakota 城市: Winner 纬度: 43.376671 经度: -99.859009
45.77.12.142	IP: 45.77.12.142 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322

l.lzpeng.com	IP: 8.219.114.98 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
ouplog.umeng.com	IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
storage.0551pf.com	IP: 18.65.185.35 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
119.28.65.192	IP: 119.28.65.192 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
cdnjs.cloudflare.com	IP: 104.17.25.14 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
realm.io	IP: 13.227.62.2 所属国家: Japan 地区: Tokyo 城市: Tokyo

	纬度: 35.689499 经度: 139.692322
www.jiuwei.tv	没有服务器地理信息.
twitter.com	IP: 104.244.42.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
ulogs.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
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
wup.imtt.qq.com	IP: 125.39.104.63 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
developer.umeng.com	IP: 59.82.31.160 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

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
platform.twitter.com	IP: 151.101.88.157 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
kakzpm.ins164.com	IP: 47.242.156.236 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
radioluntan.space	IP: 172.67.187.92 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
i.573bd.com	IP: 18.65.185.76 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
ulogs.umengcloud.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
storage.zhanbowy.com	没有服务器地理信息.
mjapp.mjomj.com	没有服务器地理信息.
www.youtube.com	IP: 31.13.106.4 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
47.92.103.233	IP: 47.92.103.233 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.maiyoux.com	IP: 172.96.160.41 所属国家: United States of America 地区: Florida 城市: Miami 纬度: 25.811834 经度: -80.236389
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
i.dfutw.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
api.muweifeng.cn	没有服务器地理信息.
alogsus.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
alogus.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
issuetracker.google.com	IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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

URL线索

URL信息	Url所在文件
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/i.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java

http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utls/d.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://storage.0551pf.com/host_f2_2.txt	g/b/a/j/l/h/b.java
https://storage.zhanbowy.com/host_f2_2.txt	g/b/a/j/l/h/b.java
https://storage.dreameragame.com/host_f2_2.txt	g/b/a/j/l/h/b.java
https://api.muweifeng.cn/tl/index/liveList	g/b/a/j/v0/c/a.java
http://119.28.65.192:8090/api/photos/listAll	g/b/a/j/y/g/a.java
http://radioluntan.space/apiv286.php	g/b/a/j/r0/a/a.java
https://i.dfutw.com/web1.txt	g/b/a/j/c0/l/b.java

https://i.573bd.com/web1.txt	g/b/a/j/c0/l/b.java
https://i.lulutv.fun/web1.txt	g/b/a/j/c0/l/b.java
http://www.jiuwei.tv:81/getTxMediaInfo	g/b/a/j/h/c/a.java
http://45.77.12.142:8080/api/get/	g/b/a/j/p/d/a.java
http://kakzpm.ins164.com:29909/party/common/generals/public/getGeneral	g/b/a/j/s/f/a.java
https://bak.sgp1.cc/api.php/api/narrate/post_detail	g/b/a/j/k/b/a.java
https://bak.sgp1.cc/api.php/api/narrate/list_post	g/b/a/j/k/b/a.java
https://bak.sgp1.cc/api.php/api/narrate/original_detail	g/b/a/j/k/b/a.java
https://xiguaule.com/dy/getinfo	g/b/a/j/w0/e/a.java
http://47.92.103.233/	g/b/a/j/w0/e/a.java
https://mjapp.mjomj.com/index.php/app/ios/vod/index	g/b/a/j/l0/h/a.java
https://mjapp.mjomj.com/index.php/app/ios/vod/show	g/b/a/j/l0/h/a.java
http://api.vipmisss.com:81/xcdsw/	g/b/a/j/n0/a.java
http://l.lzpeng.com/api/public/?service=Home.getHot	g/b/a/j/n0/a.java
http://xiuxiuba.vip:82/mobile/live/index	g/b/a/j/n0/a.java
http://xiuxiuba.vip:82/mobile/live/anchors	g/b/a/j/n0/a.java
http://api.maiyoux.com:81/mf/json.txt	g/b/a/j/n0/a.java
http://api.maiyoux.com:81/mf/	g/b/a/j/n0/a.java

http://api.vipmisss.com:81/xcdsw/json.txt	g/b/a/j/n0/a.java
http://dashif.org/guidelines/last-segment-number	g/h/a/a/h1/t0/k/c.java
https://realm.io/docs/java/latest/	h/a/g0.java
https://realm.io/news/android-installation-change/	h/a/b0.java
https://realm.io/docs/java/latest/	h/a/b0.java
https://issuetracker.google.com/issues/36918154	h/a/x.java
https://www.youtube.com/embed/%s	d/a/a/d/h/c/b.java
https://publish.twitter.com/oembed?url=https://twitter.com/twitter/status/%s	d/a/a/d/g/c/b.java
https://publish.twitter.com/oembed?url=https://twitter.com/twitter/status/%s&hide_media=true	d/a/a/d/g/c/b.java
https://twitter.com/%s\	d/a/a/d/g/c/b.java
https://platform.twitter.com/widgets.js\	d/a/a/d/g/c/b.java
https://cdnjs.cloudflare.com/ajax/libs/mathjax/2.7.2/MathJax.js?config=TeX-MML-AM_CHTML	br/tiagohm/markdownview/MarkdownView.java

 邮箱线索

 手机线索

手机号	所在文件

1422222222	com/tencent/smtt/sdk/i.java
------------	-----------------------------

🌟 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

🔑 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.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.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.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

应用内通信

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。