



MoGua

淘色 1.2.7.APK 分析报告



APP名称:

淘色

包名: com.android.taose2024

域名线索: 48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: com.android.taose2024-1.2.7.apk
文件大小: 14.32MB
MD5值: f0d1770d41b101538bdacb4509582daf
SHA1值: 67ae62bc6ce7552beffa8cb9ee9fc210d1cce101
SHA256值: dd68b450492c9e6bccdff3870ace4c6cce61aeec967d6cbbf22679ef0115a739

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: 1.2.7
安卓版本: 127

🔍 域名线索

域名	服务器信息
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
dashif.org	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
developer.umeng.com	IP: 59.82.31.95 所属国家: China 地区: Zhejiang

	城市: Hangzhou 纬度: 30.293650 经度: 120.161583
api.maiyoux.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
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
publish.twitter.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
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
plbslog.umeng.com	IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
i.lulutv.fun	没有服务器地理信息.

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
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
storage.zhanbowy.com	没有服务器地理信息.
x.ins620.com	IP: 8.210.158.46 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
xiuxiuba.vip	没有服务器地理信息.
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

issuetracker.google.com	IP: 172.253.117.102 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
github.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
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
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
twitter.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: -

	纬度: 0.000000 经度: 0.000000
xiguaule.com	IP: 172.67.188.251 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
i.dfutw.com	没有服务器地理信息.
www.jiuwei.tv	没有服务器地理信息.
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
cfg.imtt.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
mjapp.mjomj.com	没有服务器地理信息.
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
	IP: 203.119.145.40 所属国家: China

cmnsguider.yunos.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
storage.0551pf.com	没有服务器地理信息.
mdc.html5.qq.com	IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
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
api3.sgp1.cc	IP: 104.21.48.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
realm.io	IP: 3.165.75.70 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
platform.twitter.com	IP: 104.244.46.211 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
api.vipmisss.com	IP: 23.186.216.33 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
alogsus.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
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
	IP: 104.21.16.1

api2.sgp1.cc	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
www.youtube.com	IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
storage.dreameragame.com	没有服务器地理信息.
cdnjs.cloudflare.com	IP: 127.0.0.1 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.
i.longzhuzs.com	没有服务器地理信息.

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/utils/d.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.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
https://x.ins620.com/api/party/common/generals/public/getGeneral	g/b/a/j/s/e/a.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
http://45.77.12.142:8080/api/get/	g/b/a/j/p/d/a.java
https://i.dfutw.com/pwa.txt	g/b/a/j/c0/m/b.java

https://i.longzhuzs.com/pwa.txt	g/b/a/j/c0/m/b.java
https://i.lulutv.fun/pwa.txt	g/b/a/j/c0/m/b.java
http://www.jiuwei.tv:81/getTxMediaInfo	g/b/a/j/h/c/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
https://api2.sgp1.cc/api.php/api/narrate/list_post	g/b/a/j/k/b/a.java
https://api3.sgp1.cc/api.php/api/narrate/post_detail	g/b/a/j/k/b/a.java
https://api2.sgp1.cc/api.php/api/narrate/original_detail	g/b/a/j/k/b/a.java
http://dashif.org/guidelines/last-segment-number	g/h/a/a/h1/t0/k/c.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://www.youtube.com/embed/%s	d/a/a/d/h/c/b.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://github.com/L-JINBIN/ApkSignatureKillerEx	bin/mt/signature/KillerApplication.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
14222222222	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=CN
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-12 00:49:21+00:00
有效期至: 2049-04-06 00:49:21+00:00
发行人: C=CN
序列号: 0x583488cd
哈希算法: sha256
md5值: ecdfc654ae638d857d64ccd488db9bcb
sha1值: 8216459ad94fb552d07491ec6a819bf7322c308c
sha256值: df740279934ad9f3032ccf4e31212f93559eac09cd23c2959fbc6fc404950d3a
sha512值: b5471766b9e78f8abc4a5c2dd657304b9d195982e54f502cd6fbef259881126091e1ad4651346c0ce3a2103bd2d55552d4cf5dc261e51c0d7419cc74f264dd7a
公钥算法: rsa
密钥长度: 2048
指纹: bbb32c475b78efc58fa1e901324e3d98f9f41c98e07349694aa6b54276cb911e

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