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

**淘色（ 1.3.4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 | 淘色 |
| 版本 | 1.3.4 |
| 包名 | com.android.taose2024 |
| 域名线索 | 46条 |
| URL线索 | 30条 |
| APP图标 |  |
| 分析日期 | 2025年10月3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 | 淘色.apk |
| 文件大小 | 14.13MB |
| MD5值 | 04318b11d8ea16f981bcf65583b0566f |
| SHA1值 | efcf88e3f779186607e5240f5f806565e86bfe85 |
| SHA256值 | d45de0ebf4069653909f76da512e9748b0b9d9ace15c25d12ba8d4f8bb6525ef |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| xiguaule.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| plbslog.umeng.com | IP: 36.156.202.68  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| cmnsguider.yunos.com | IP: 203.119.175.235  所属国家: China  地区: Beijing  城市: Beijing |
| 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 |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| publish.twitter.com | IP: 104.244.42.195  所属国家: United States of America  地区: California  城市: San Francisco |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| dashif.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| i.lulutv.fun | IP: 143.204.126.94  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 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 |
| 45.77.12.142 | IP: 45.77.12.142  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| l.lzpeng.com | IP: 8.219.114.98  所属国家: Singapore  地区: Singapore  城市: Singapore |
| ouplog.umeng.com | IP: 47.246.110.94  所属国家: Singapore  地区: Singapore  城市: Singapore |
| storage.0551pf.com | IP: 18.65.185.35  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 119.28.65.192 | IP: 119.28.65.192  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| cdnjs.cloudflare.com | IP: 104.17.25.14  所属国家: United States of America  地区: California  城市: San Francisco |
| realm.io | IP: 13.227.62.2  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 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 |
| ulogs.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| wup.imtt.qq.com | IP: 125.39.104.63  所属国家: China  地区: Tianjin  城市: Tianjin |
| developer.umeng.com | IP: 59.82.31.160  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cfg.imtt.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| platform.twitter.com | IP: 151.101.88.157  所属国家: United States of America  地区: California  城市: San Francisco |
| kakzpm.ins164.com | IP: 47.242.156.236  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| radioluntan.space | IP: 172.67.187.92  所属国家: United States of America  地区: California  城市: San Francisco |
| i.573bd.com | IP: 18.65.185.76  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| ulogs.umengcloud.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| 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 |
| 47.92.103.233 | IP: 47.92.103.233  所属国家: China  地区: Beijing  城市: Beijing |
| api.maiyoux.com | IP: 172.96.160.41  所属国家: United States of America  地区: Florida  城市: Miami |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| mdc.html5.qq.com | IP: 125.39.196.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| i.dfutw.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| 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 |
| alogus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Jiangsu  城市: Nanjing |
| issuetracker.google.com | IP: 142.251.211.238  所属国家: United States of America  地区: California  城市: Mountain View |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |

### **4.2 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://mqqad.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 |
| 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 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14222222222 | com/tencent/smtt/sdk/i.java |

## **5. 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**

## **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.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 |

## **10. 应用内通信**

**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。**