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

**淘色（ 1.2.0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 | 淘色 |
| 版本 | 1.2.0 |
| 包名 | com.android.taose2024 |
| 域名线索 | 45条 |
| URL线索 | 31条 |
| APP图标 |  |
| 分析日期 | 2025年10月9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v1.2.0.apk |
| 文件大小 | 13.24MB |
| MD5值 | 9d2e1a2751b5600949ecca8e10fb44b2 |
| SHA1值 | 2d537215cb6fe99138ef430784ede12cf50b93e2 |
| SHA256值 | ad18c8ba511bc1e9ec104a6f5ec8bbeff279a40b9f6d40d428b9c76e4aeb3173 |

## **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 | 1.2.0 |
| 安卓版本 | 120 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| i.longzhuzs.com | 没有服务器地理信息.  |
| i.lulutv.fun | IP: 143.204.126.39 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| developer.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| twitter.com | IP: 162.125.80.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.maiyoux.com | IP: 23.225.198.194 所属国家: United States of America 地区: California 城市: Los Angeles  |
| 45.77.12.142 | IP: 45.77.12.142 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| mdc.html5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| storage.aweiya.net | IP: 154.12.30.213 所属国家: United States of America 地区: California 城市: Pasadena  |
| radioluntan.space | IP: 172.67.187.92 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  |
| platform.twitter.com | IP: 67.230.169.182 所属国家: United States of America 地区: California 城市: Los Angeles  |
| ulogs.umengcloud.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| 119.28.65.192 | IP: 119.28.65.192 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| alogsus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| xiguaule.com | IP: 172.67.188.251 所属国家: United States of America 地区: California 城市: San Francisco  |
| dashif.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| realm.io | IP: 3.165.21.63 所属国家: United States of America 地区: Washington 城市: Seattle  |
| wup.imtt.qq.com | IP: 116.130.230.62 所属国家: China 地区: Beijing 城市: Beijing  |
| mjapp.mjomj.com | 没有服务器地理信息.  |
| cdnjs.cloudflare.com | IP: 104.17.24.14 所属国家: United States of America 地区: California 城市: San Francisco  |
| x.ins620.com | IP: 8.210.158.46 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cmnsguider.yunos.com | IP: 203.119.175.203 所属国家: China 地区: Beijing 城市: Beijing  |
| l.lzpeng.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| storage.0551pf.com | IP: 65.9.42.112 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| api.vipmisss.com | IP: 23.225.198.198 所属国家: United States of America 地区: California 城市: Los Angeles  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.muweifeng.cn | 没有服务器地理信息.  |
| issuetracker.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.youtube.com | IP: 199.96.58.85 所属国家: United States of America 地区: California 城市: San Francisco  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| 47.92.103.233 | IP: 47.92.103.233 所属国家: China 地区: Beijing 城市: Beijing  |
| storage.pinyingkeji.com | 没有服务器地理信息.  |
| i.dfutw.com | IP: 18.65.168.35 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xiuxiuba.vip | IP: 23.225.178.90 所属国家: United States of America 地区: California 城市: Los Angeles  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| publish.twitter.com | IP: 128.121.243.107 所属国家: United States of America 地区: Washington 城市: Redmond  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.jiuwei.tv | 没有服务器地理信息.  |

### **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  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/h.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.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://cdnjs.cloudflare.com/ajax/libs/mathjax/2.7.2/MathJax.js?config=TeX-MML-AM\_CHTML  | br/tiagohm/markdownview/MarkdownView.java  |
| http://www.w3.org/2000/svg'  | br/tiagohm/markdownview/MarkdownView.java  |
| http://www.w3.org/1999/xlink'  | br/tiagohm/markdownview/MarkdownView.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://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://mjapp.mjomj.com/index.php/app/ios/vod/index  | g/b/a/j/j0/h/a.java  |
| https://mjapp.mjomj.com/index.php/app/ios/vod/show  | g/b/a/j/j0/h/a.java  |
| https://storage.aweiya.net/host\_f2\_2.txt  | g/b/a/j/l/h/b.java  |
| https://storage.0551pf.com/host\_f2\_2.txt  | g/b/a/j/l/h/b.java  |
| https://storage.pinyingkeji.com/host\_f2\_2.txt  | g/b/a/j/l/h/b.java  |
| http://api.vipmisss.com:81/xcdsw/  | g/b/a/j/l0/a.java  |
| http://l.lzpeng.com/api/public/?service=Home.getHot  | g/b/a/j/l0/a.java  |
| http://xiuxiuba.vip:82/mobile/live/index  | g/b/a/j/l0/a.java  |
| http://xiuxiuba.vip:82/mobile/live/anchors  | g/b/a/j/l0/a.java  |
| http://api.maiyoux.com:81/mf/json.txt  | g/b/a/j/l0/a.java  |
| http://api.maiyoux.com:81/mf/  | g/b/a/j/l0/a.java  |
| http://api.vipmisss.com:81/xcdsw/json.txt  | g/b/a/j/l0/a.java  |
| http://45.77.12.142:8080/api/get/  | g/b/a/j/p/d/a.java  |
| http://radioluntan.space/apiv286.php  | g/b/a/j/p0/a/a.java  |
| https://x.ins620.com/api/party/common/generals/public/getGeneral  | g/b/a/j/s/e/a.java  |
| https://api.muweifeng.cn/tl/index/liveList  | g/b/a/j/s0/c/a.java  |
| https://xiguaule.com/dy/getinfo  | g/b/a/j/t0/e/a.java  |
| http://47.92.103.233/  | g/b/a/j/t0/e/a.java  |
| http://119.28.65.192:8090/api/photos/listAll  | g/b/a/j/y/g/a.java  |
| http://dashif.org/guidelines/last-segment-number  | g/h/a/a/h1/t0/k/c.java  |
| http://www.w3.org/ns/ttml  | g/h/a/a/i1/r/a.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://realm.io/docs/java/latest/  | h/a/g0.java  |
| http://www.w3.org/1999/xhtml  | Mogua Engine V2  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=1r, ST=123, L=13e, O=14d, OU=1da, CN=1c 签名算法: rsassa\_pkcs1v15 有效期自: 2024-01-18 13:28:58+00:00 有效期至: 2049-01-11 13:28:58+00:00 发行人: C=1r, ST=123, L=13e, O=14d, OU=1da, CN=1c 序列号: 0x35eeee85 哈希算法: sha256 md5值: c6c88bfbfde1eac1b62fef07f18423c8 sha1值: 7da8d8a03f427f497963768c6aa3b6a5e983ee89 sha256值: e6b6d339de7795e0ba316d1401a91821dbc61cfe649658c7ffd96d7b3fef1075 sha512值: dce699050981529daa2aa7e3ada252ae95c95019ec9df03e1c5bc080c19a744454e050d45746902722bd589b7a562cac13f6d7d783a345477fc994a7f78669cd**

## **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。**