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

**小太妹（ 1.9.8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 | 小太妹 |
| 版本 | 1.9.8 |
| 包名 | com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb |
| 域名线索 | 33条 |
| URL线索 | 43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 | wam03df1.apk |
| 文件大小 | 15.52MB |
| MD5值 | df4e3c6a3032d7a621263edb099f2dcf |
| SHA1值 | 34891fabfae997d746471aeaa308810515706316 |
| SHA256值 | 7168cd4edb565f95ee9079b7ac13a6d7d12721293e53e28bb8b4c17e08605d61 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小太妹 |
| 包名 | com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb |
| 主活动Activity | com.limit.cache.ui.page.main.WelComeActivity |
| 安卓版本名称 | 1.9.8 |
| 安卓版本 | 198 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| errnewlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.29.249 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| weibo.com | IP: 116.133.8.18 所属国家: China 地区: Beijing 城市: Beijing  |
| pslog.umeng.com | IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alist.ttpvi.com | IP: 52.139.152.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| plus.google.com | IP: 108.160.162.109 所属国家: United States of America 地区: California 城市: San Francisco  |
| alist.dglago.com | IP: 20.189.74.77 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| 1.1.1.1 | IP: 1.1.1.1 所属国家: United States of America 地区: California 城市: San Jose  |
| alist.6ay26b.com | IP: 154.19.167.111 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| alogsus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xtm99.top | IP: 91.195.240.12 所属国家: Germany 地区: Nordrhein-Westfalen 城市: Koeln  |
| ulogs.umengcloud.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| ucc.umeng.com | IP: 203.119.145.45 所属国家: China 地区: Beijing 城市: Beijing  |
| cnlogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alist.wyx0429.com | IP: 112.28.188.240 所属国家: China 地区: Anhui 城市: Hefei  |
| resolve.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alist.zhwizh.com | IP: 202.79.172.132 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| ns.adobe.com | 没有服务器地理信息.  |
| h5.dev.test.ggbba.top | 没有服务器地理信息.  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| aspect-upush.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| aria.laoyuyu.me | 没有服务器地理信息.  |
| utoken.umeng.com | IP: 223.109.148.139 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| schemas.android.com | 没有服务器地理信息.  |
| errnewlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| errlogos.umeng.com | IP: 47.246.110.96 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.obao22.com | 没有服务器地理信息.  |
| alogus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alist.hbhaojing.com | IP: 218.11.6.230 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| alist.zhangdaer.com | IP: 218.11.6.230 所属国家: China 地区: Hebei 城市: Shijiazhuang  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://aria.laoyuyu.me/aria\_doc/create/any\_java.html  | com/arialyy/aria/core/Aria.java  |
| https://aria.laoyuyu.me/aria\_doc/other/annotaion\_invalid.html  | com/arialyy/aria/core/download/DownloadReceiver.java  |
| https://github.com/AriaLyy/Aria/issues/597  | com/arialyy/aria/core/download/m3u8/M3U8Option.java  |
| https://aria.laoyuyu.me/aria\_doc/other/annotaion\_invalid.html  | com/arialyy/aria/core/upload/UploadReceiver.java  |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errnewlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/d/c.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/f.java  |
| http://schemas.android.com/apk/res/android  | com/limit/cache/widget/MoMoTabLayout.java  |
| https://h5.dev.test.ggbba.top/dd/%E6%97%B6%E9%97%B4%E9%97%AA%E7%83%81%E6%88%90%E5%93%81.png  | com/limit/cache/widget/MoMoTabLayout.java  |
| https://alist.hbhaojing.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.zhangdaer.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.wyx0429.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.6ay26b.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.dglago.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.ttpvi.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://alist.zhwizh.com  | com/limit/cache/ui/page/main/WelComeActivity.java  |
| https://h5.dev.test.ggbba.top/dd/%E4%BB%B7%E6%A0%BC%E6%88%90%E5%93%81.png  | com/limit/cache/ui/page/seckill/SeckillAdapter.java  |
| https://h5.dev.test.ggbba.top/dd/%E4%BB%B7%E6%A0%BC%E6%88%90%E5%93%81.png  | com/limit/cache/ui/page/seckill/SeckillDetailActivity.java  |
| https://www.obao22.com/?i\_code=  | com/limit/cache/ui/fragment/web/AppWebFragment.java  |
| https://1.1.1.1/  | com/limit/cache/apphttp/DNSClient.java  |
| https://aspect-upush.umeng.com/occa/v1/event/report  | com/umeng/analytics/pro/aq.java  |
| https://cnlogs.umeng.com/ext\_event  | com/umeng/analytics/pro/aq.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/l.java  |
| https://resolve.umeng.com/resolve  | com/umeng/analytics/pro/bt.java  |
| https://ucc.umeng.com/v2/inn/fetch  | com/umeng/analytics/pro/ar.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://developer.umeng.com/docs/119267/detail/118637  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrashContent.java  |
| https://developer.umeng.com/docs/193624/detail/194590  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlogos.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlogos.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com/upload  | com/umeng/umcrash/UMCrash.java  |
| https://errnewlog.umeng.com  | com/umeng/umcrash/UMCrash.java  |
| https://utoken.umeng.com  | com/umeng/umzid/ZIDManager.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/c/b.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/c/b.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/alimuzaffar/lib/pin/PinEntryEditText.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | f4/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | f4/h.java  |
| https://github.com/danikula  | f4/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | f4/h.java  |
| http://%s:%d/%s  | f4/k.java  |
| http://%s:%d/%s  | f4/f.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | f4/f.java  |
| https://plus.google.com/  | q5/t0.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | sd/b.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | sd/d.java  |
| https://weibo.com  | y5/a.java  |
| http://schemas.android.com/apk/res/android  | z0/h.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | t1/a.java  |
| https://xtm99.top  | aa/e.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | m5/n.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |
| 17512775099  | p7/a.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=y, ST=y, L=y, O=y, OU=y, CN=y 签名算法: rsassa\_pkcs1v15 有效期自: 2024-02-01 08:03:23+00:00 有效期至: 2124-01-08 08:03:23+00:00 发行人: C=y, ST=y, L=y, O=y, OU=y, CN=y 序列号: 0x24c2cf8c 哈希算法: sha256 md5值: f6d29e95f5ed16c785b4fa8923a6d834 sha1值: adc5f2bc96110a02ed69702b6a09dd9bbf4360fa sha256值: 2a46efa90f56da1c5a73d2fe6e6a9662639e69b0aa9f70b19c5f9a591c1575f4 sha512值: ec719a7c87ba0a3008dc0cb88a901950ac90e81c333d4d4bdf9956b52479e98be91ff0bf0d327aa03a6ce3c23b5ff4253e14705b67993318d2b36106de57b37e 公钥算法: rsa 密钥长度: 2048 指纹: adc2795979ec41e44411ed7f1c496405f05179f5246722108e18bcb32b47c8a9**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "digits\_username" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"  |
| "modify\_pwd" : "修改密码"  |
| "pwd\_inconsistent" : "密码不一致"  |
| "pwd\_not\_rule" : "密码不符合规则"  |

## **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.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| 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 |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| 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 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.ytmomoiw.yrcaodbbvineleiesulibmffipfqdbggxnteb.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**