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

**还呗（ 1.0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 | 还呗 |
| 版本 | 1.0 |
| 包名 | bopaozlbvm.sbfnfh |
| 域名线索 | 15条 |
| URL线索 | 13条 |
| APP图标 |  |
| 分析日期 | 2025年7月4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 | bopaozlbvm.sbfnfh.apk |
| 文件大小 | 1.47MB |
| MD5值 | 7fe3250fa5e7a70e7abcc21bd8109a96 |
| SHA1值 | c2ddf59117c29c947db57cce9e1dc2445efa9e3f |
| SHA256值 | 64c8bb461b474161bba565a5dc2f27c7c98a0f79c75b8fc2164d204f40928138 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 还呗 |
| 包名 | bopaozlbvm.sbfnfh |
| 主活动Activity | tacd.ncte.o8qt.soae |
| 安卓版本名称 | 1.0 |
| 安卓版本 | 1 |

## **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  |
| tbs.imtt.qq.com | IP: 119.176.27.78 所属国家: China 地区: Shandong 城市: Weifang  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| ulogs.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| developer.umeng.com | IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| utoken.umeng.com | IP: 223.109.148.171 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| alogsus.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| schemas.android.com | 没有服务器地理信息.  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| log.tbs.qq.com | IP: 124.95.231.218 所属国家: China 地区: Liaoning 城市: Shenyang  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.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://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://utoken.umeng.com/api/updateZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://utoken.umeng.com/api/postZdata/v4  | com/umeng/umzid/ZIDManager.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | b2/z.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | b2/z.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | b2/z.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | b2/z.java  |
| http://schemas.android.com/apk/res/android  | b2/i.java  |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | b2/m.java  |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties  | l1/q.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | z1/d0.java  |
| https://pms.mb.qq.com/rsp204  | z1/p0.java  |

### **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: True v3 签名: True 找到 1 个唯一证书 主题: C=beijing, ST=beijing, L=beijing, O=mj1724235122214, OU=dc1724235122214, CN=zwcc 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-21 10:12:23+00:00 有效期至: 2074-08-09 10:12:23+00:00 发行人: C=beijing, ST=beijing, L=beijing, O=mj1724235122214, OU=dc1724235122214, CN=zwcc 序列号: 0x55ffd1cc 哈希算法: sha512 md5值: 6e5e0508d14c8192f2b8fbadc600a601 sha1值: 0a9d56b2d291026288ab438eae8159c42ae0ae1a sha256值: 0e6e9e908c03b69e7ef59d942ed2d04f71b862a9821a204729cd5c7eb2fbfb2b sha512值: 5f10dafe14b6deeca66ca2bf38445947bc71c16b58138e763b20d7c98c884cda1765df2a71fdffb470cb718602b036c5f02d4a6825ce50fd2b3e75dc0b748e94 公钥算法: rsa 密钥长度: 4096 指纹: 3cd329c38b0b52af233f6dbe808821211f2bb3f58d6edb0cdbfb1c09f6b3aa0c**

## **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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.MICROPHONE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| tacd.ncte.o8qt.soae | **Schemes**: http://, https://, about://, javascript://, inline://, tbopen://, a://, **Hosts:** tacd.ncte.browser, **Mime Types:** text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml, **Path Prefixes:** /index.html,  |

**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。**