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

**腾讯成人版（ 1.0.0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 | 腾讯成人版 |
| 版本 | 1.0.0 |
| 包名 | dark.CZlhw.BjMUE |
| 域名线索 | 7条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年6月21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 | 腾讯成人版.apk |
| 文件大小 | 23.58MB |
| MD5值 | 7f0dcebfcce2e9d4b94065d85178a990 |
| SHA1值 | 6bb4e9568ba0cfbb1504b3618c697daa891e9527 |
| SHA256值 | 30609ea9bfc7db242fdcc550cfe878f194009a15dbb8cb991225085125738453 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 腾讯成人版 |
| 包名 | dark.CZlhw.BjMUE |
| 主活动Activity | dark.CZlhw.BjMUE.MainActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| journeyapps.com | IP: 18.65.168.3 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| dartbug.com | IP: 216.239.38.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://journeyapps.com/  | 摸瓜V1引擎  |
| https://github.com/journeyapps/zxing-android-embedded  | 摸瓜V1引擎  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| https://github.com/apvarun/toastify-js  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://github.com/nodeca/pica  | 摸瓜V2引擎  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| android-sdk-releaser@odhe6.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |

### **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='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国' 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-07 02:31:06+00:00 有效期至: 2035-05-05 02:31:06+00:00 发行人: C='中国', ST='北京', L='北京', O='北京', OU='北京', CN='中国' 序列号: 0x881ef176793a993b 哈希算法: sha256 md5值: fe96e6c35679c4a62dc2303cc29311ac sha1值: a1ee64ef03accaab4b4e8ae496fe15a062ae26cd sha256值: 4e20362116cd6f85e30b8cc8c1bab1c3a17f846183b8498430e4d0c4b287f1b5 sha512值: 940d09e29768f8852f2a565cd592c6909a70a24c07cdfdc66332f5498cb9e2680487733967c0b52ec7a9242284af206de37a06e50a1cb407b4c4153d534fbb1e 公钥算法: rsa 密钥长度: 2048 指纹: a2cc8e51475604b0bd56af746c010f5cdff1b08bb6dc7fa32633f3328dedfb91**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.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\_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\_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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.POST\_NOTIFICATIONS | 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| dark.CZlhw.BjMUE.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**