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

**一个（ 2.7.0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 | 一个 |
| 版本 | 2.7.0 |
| 包名 | dark.VmIEw.fQvqL |
| 域名线索 | 14条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年6月15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 | one2.7.0.apk |
| 文件大小 | 32.15MB |
| MD5值 | 048d32a3ffb3b2ee08fb33f19180d062 |
| SHA1值 | 7fecd64b2b658a76c33e8db63cea604e5dfb61b5 |
| SHA256值 | 695fc3511fc2561111441e9e5fa1a90e47150ad179fd63c2ecb232a0ff586708 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 一个 |
| 包名 | dark.VmIEw.fQvqL |
| 主活动Activity | com.one.MainActivity |
| 安卓版本名称 | 2.7.0 |
| 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  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.ffmpeg.org | IP: 79.124.17.100 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| ultravideo.cs.tut.fi | IP: 130.230.203.118 所属国家: Finland 地区: Pirkanmaa 城市: Tampere  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| android.googlesource.com | IP: 192.178.163.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| dashif.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| streams.videolan.org | IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| yige.fm | IP: 104.21.3.43 所属国家: United States of America 地区: California 城市: San Francisco  |
| journeyapps.com | IP: 13.35.37.111 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| dartbug.com | IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |

### **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/nodeca/pica  | 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  |
| http://www.smpte-ra.org/schemas/2067-3/2013  | lib/arm64-v8a/libavformat.so  |
| http://%s:%d%s  | lib/arm64-v8a/libavformat.so  |
| http://%s%s  | lib/arm64-v8a/libavformat.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/arm64-v8a/libavformat.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/arm64-v8a/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/arm64-v8a/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/arm64-v8a/libffmpegkit.so  |
| http://ultravideo.cs.tut.fi/  | lib/arm64-v8a/libavcodec.so  |
| https://yige.fm  | lib/arm64-v8a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| ffmpeg-devel@ffmpeg.org  | lib/arm64-v8a/libffmpegkit.so  |
| twolame-discuss@lists.sourceforg  | lib/arm64-v8a/libavcodec.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: 2025-06-09 17:53:08+00:00 有效期至: 2035-06-07 17:53:08+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: 0x4fc7834a 哈希算法: sha256 md5值: 861c966c34b11e20a9314184b0574ee4 sha1值: 123ac294085e54fae488ccd7f3d8575dec6995cc sha256值: f5e1c00596611e622a187cdb061942be780223e86392aad96747d17b7fc6b25d sha512值: ab553edbe451511c0f6c097e5add11f917b3ef090be588d3dc8283ac99a98a70733bad6a03bde6352e5018a9f9277f2eff416ff15035796685ec53a94274e9b2 公钥算法: rsa 密钥长度: 2048 指纹: 24b14c38624ddb592564f38774dca47064744aa8634db27de201579f967683df**

## **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.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.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.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.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\_MEDIA\_IMAGES | 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| dark.VmIEw.fQvqL.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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。**