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

**萌正太（ 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 | 萌正太 |
| 版本 | 1.0.0 |
| 包名 | com.android.huawei.mzthmyp |
| 域名线索 | 17条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年9月27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 | 4e43a2f38058230829c061e7e550fcfa.apk |
| 文件大小 | 16.55MB |
| MD5值 | 1bff1b1e23a4cd0dceaeb42bf1eae8b1 |
| SHA1值 | b9e3556f2297ea1c877f9c74731cda5cbc72d26c |
| SHA256值 | 474b5ab2eec1649277e6338acbb2fe9723dbf4390a102c89696e9fdb6c0e53c8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 萌正太 |
| 包名 | com.android.huawei.mzthmyp |
| 主活动Activity | com.android.temp.sam.lolita\_app.MainActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 2001 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.asia | IP: 119.8.176.197 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| aomedia.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| journeyapps.com | IP: 13.225.131.83 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Icheon  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.apple.com | IP: 17.253.85.203 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ns.adobe.com | 没有服务器地理信息.  |
| dashif.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| exoplayer.dev | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| grs.dbankcloud.com | IP: 113.201.107.90 所属国家: China 地区: Shaanxi 城市: Baoji  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.microsoft.com | IP: 13.107.213.74 所属国家: United States of America 地区: Washington 城市: Redmond  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://)([\\s\\S]+)  | com/huawei/hms/scankit/p/C0230bd.java  |
| http://www.w3.org/ns/ttml  | d4/c.java  |
| https://aomedia.org/emsg/ID3  | f3/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | f3/a.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | h4/a0.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/f.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | k2/z0.java  |
| http://schemas.android.com/apk/res/android  | o/k.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | p2/o0.java  |
| https://x</LA\_URL>  | p2/n0.java  |
| https://x  | p2/n0.java  |
| http://dashif.org/guidelines/last-segment-number  | r3/d.java  |
| http://dashif.org/guidelines/trickmode  | r3/d.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | t8/c.java  |
| http://ns.adobe.com/xap/1.0/  | v2/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | v8/c.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | v8/e.java  |
| https://journeyapps.com/  | Mogua Engine V1  |
| https://github.com/journeyapps/zxing-android-embedded  | Mogua Engine V1  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/libflutter.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/libflutter.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | o4/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=oauyds, ST=oaisydh, L=oayisd, O=oauydsh, OU=apisodu, CN=owiu 签名算法: rsassa\_pkcs1v15 有效期自: 2023-10-27 15:31:22+00:00 有效期至: 2078-07-30 15:31:22+00:00 发行人: C=oauyds, ST=oaisydh, L=oayisd, O=oauydsh, OU=apisodu, CN=owiu 序列号: 0x1bf19974563c9858 哈希算法: sha256 md5值: 9cfd62229253d5b9baa2b1168044e00a sha1值: e89b3c4d4bef498ad7cde9c3feb0e0b23a54cb22 sha256值: d613b66256e61a0d5ac4b9b5e2d0809e8387f0b625c2adc862a695b754fd8090 sha512值: f68aab33112d08abe072a05b6411779e2afe4e1857eaecb0dda26064adb8b4db12989abbb30262ea0d8192278f77ecca8dabacd001b0f27d032ff80514ab63f6 公钥算法: rsa 密钥长度: 2048 指纹: a75dc61439a5957355c53408397c5806a2619f53747e4f52d8f91277acb9ca88**

## **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.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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |

## **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。**