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

**夹米（ 0.0.3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 | 夹米 |
| 版本 | 0.0.3 |
| 包名 | com.jiamiappprovip.app |
| 域名线索 | 6条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | 2\_jiami\_v0.apk |
| 文件大小 | 114.49MB |
| MD5值 | 4ae90d4746bbd94b26373d5840494e9a |
| SHA1值 | 1a9623e6ce6e9ed88502a41d3239d9d2515ab30e |
| SHA256值 | 7ff326db3bf838b488a1e3a50f67e85168887a72f27ffd9e0d2253d929cd5e1c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 夹米 |
| 包名 | com.jiamiappprovip.app |
| 主活动Activity | com.jiamiappprovip.app.ui.activity.SplashActivity |
| 安卓版本名称 | 0.0.3 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin  |
| grs.dbankcloud.cn | IP: 124.70.116.153 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2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  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sw@jiamivip.com kf@jiamivip.com media@jiamivip.com  | 摸瓜V1引擎  |

### **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: False 找到 1 个唯一证书 主题: CN=JiaMi, OU=JiaMi, O=JiaMi, L=WuHan, ST=HuBei, C=cn 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-03 15:02:46+00:00 有效期至: 2050-05-28 15:02:46+00:00 发行人: CN=JiaMi, OU=JiaMi, O=JiaMi, L=WuHan, ST=HuBei, C=cn 序列号: 0x1 哈希算法: sha256 md5值: 31e59900b6b1a9355087cebae1594145 sha1值: dc27dcdb70b5242c73f1f432c8b5e09d1f3001c0 sha256值: c3c7ded23a76aa7a5f2c64efac0111fa594c5339894683dde2b5aff05a57d9f4 sha512值: bb6d6caa8eba85f20817a6da5f3c11a8ed904f7bf2e28d7f1b79925b997c4472514ebf42240db57de5619ec8868a102737a5d4cc0db6a8afc74c59cb64659ed6 公钥算法: rsa 密钥长度: 2048 指纹: 730391aca9a653e64559746d9ac293637d1b9064dd2ff0de0f6013d11a3e0158**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_security\_alipay\_auth" : "支付宝授权"  |
| "account\_security\_alipay\_auth\_tip" : "确定绑定支付宝吗？"  |
| "account\_security\_forget\_pay\_password" : "忘记支付密码"  |
| "account\_security\_password" : "登录密码"  |
| "account\_security\_set\_teen\_mode\_password" : "设置独立密码"  |
| "account\_security\_wx\_auth" : "微信授权"  |
| "account\_security\_wx\_auth\_btn" : "去绑定"  |
| "account\_security\_wx\_auth\_tip" : "确定绑定微信吗？"  |
| "authorization\_for\_use\_personal\_information" : "《个人信息使用授权书》"  |
| "contact\_no\_such\_user" : "该用户不存在"  |
| "http\_token\_refresh" : "Refresh"  |
| "http\_token\_refresh1" : "令牌过期，将自动申请令牌"  |
| "invite\_code\_authentication" : "邀请码认证"  |
| "invite\_code\_authentication\_inviter" : "邀请人："  |
| "invite\_code\_authentication\_inviter\_info" : "邀请人信息"  |
| "invite\_code\_authentication\_inviter\_info\_back" : "返回"  |
| "invite\_code\_authentication\_inviter\_info\_tips" : "一旦绑定，无法更改，请谨慎操作"  |
| "invite\_code\_authentication\_is\_invalid" : "邀请码错误，请重新输入"  |
| "invite\_code\_authentication\_phone" : "手机号："  |
| "invite\_code\_authentication\_tips" : "填写邀请码，享更多权益"  |
| "ksad\_ad\_default\_author" : "@可爱的广告君创造的原声"  |
| "ksad\_ad\_default\_username" : "@可爱的广告君"  |
| "loading\_go\_auth" : "Go to Alipay for authorization"  |
| "make\_sure\_payment\_pwd\_title" : "确认支付密码"  |
| "modify\_login\_password\_origin\_pwd" : "原密码"  |
| "password" : "密码"  |
| "private\_group" : "讨论组"  |
| "real\_authentication\_agree" : "同意认证后，将同意您的个人信息用于认证"  |
| "real\_authentication\_go\_balance" : "去兑换余额"  |
| "real\_authentication\_go\_setup" : "去设置"  |
| "real\_authentication\_id\_card" : "身份证"  |
| "real\_authentication\_id\_card\_tips" : "请输入正确的身份证号"  |
| "real\_authentication\_name" : "姓名"  |
| "real\_authentication\_pay" : "支付￥1.1进行认证"  |
| "real\_authentication\_pay\_btn" : "确认支付"  |
| "real\_authentication\_pay\_failed" : "支付失败"  |
| "real\_authentication\_pay\_success" : "支付成功"  |
| "real\_authentication\_pay\_tips" : "需支付费用"  |
| "real\_authentication\_pay\_tips\_1" : "认证信息错误导致失败，费用概不退回"  |
| "real\_authentication\_pay\_title" : "实名认证支付"  |
| "real\_authentication\_phone" : "手机号"  |
| "real\_authentication\_setup\_success\_tips" : "设置成功"  |
| "real\_authentication\_submit" : "提交认证"  |
| "real\_authentication\_tips" : "请进行实名认证，保护您的账号安全"  |
| "real\_authentication\_tips\_0" : "您尚未进行实名认证"  |
| "real\_authentication\_tips\_1" : "为了您的账号安全，请先进行实名认证"  |
| "real\_authentication\_tips\_2" : "夹米丨信息安全保护中"  |
| "real\_authentication\_title" : "实名认证"  |
| "real\_authentication\_unset\_pay\_pwd\_tips" : "暂未设置支付密码，无法进行支付！ 请先设置支付密码再进行操作"  |
| "setting\_password" : "修改密码"  |
| "setting\_payment\_pwd\_title" : "设置支付密码"  |
| "teenager\_mode\_make\_sure\_pwd\_title" : "确认支付密码"  |
| "teenager\_mode\_pwd\_title" : "设置独立密码"  |
| "loading\_go\_auth" : "去支付宝授权"  |

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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.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\_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\_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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.jiamiappprovip.app.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| android.permissio.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.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.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。 |
| com.jiamiappprovip.app.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| com.jiamiappprovip.app.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa.SECURITY\_ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| oplus.permission.settings.LAUNCH\_FOR\_EXPORT | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.identifier.permission.OAID\_STATE\_DIALOG | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| com.jiamiappprovip.app.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。 |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent102794740://,  |

**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。**